

## Call-Off Schedule 6 (ICT Services)

### 1. Definitions

- 1.1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

<b>"Buyer Property"</b>	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
<b>"Buyer Software"</b>	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
<b>"Buyer System"</b>	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
<b>"Commercial off the shelf Software" or "COTS Software"</b>	Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms
<b>"Core Network"</b>	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract;
<b>"Defect"</b>	any of the following: <ul style="list-style-type: none"><li>a) any error, damage or defect in the manufacturing of a Deliverable; or</li><li>b) any error or failure of code within the Software which causes a Deliverable to</li></ul>

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

malfunction or to produce unintelligible or incorrect results; or

- c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or
- d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;

### **"Emergency Maintenance"**

ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;

### **"ICT Environment"**

the Buyer System and the Supplier System;

### **"Licensed Software"**

all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;

### **"Maintenance Schedule"**

has the meaning given to it in paragraph 8 of this Schedule;

### **"Malicious Software"**

any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious

software is introduced wilfully, negligently or without knowledge of its existence;

**"New Release"**

an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;

**"Open Source Software"**

computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;

**"Operating Environment"**

means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:

- a) the Deliverables are (or are to be) provided; or
- b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or
- c) where any part of the Supplier System is situated;

**"Permitted Maintenance"**

has the meaning given to it in paragraph 8.2 of this Schedule;

**"Quality Plans"**

has the meaning given to it in paragraph 6.1 of this Schedule;

**"Sites"**

has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;

**"Software"**

Specially Written Software COTS Software and non-COTS Supplier and third party Software;

**"Software Supporting Materials"**

has the meaning given to it in paragraph 9.1 of this Schedule;

**"Source Code"**

computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;

**"Specially Written Software"**

any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;

**"Supplier System"**

the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

**2. When this Schedule should be used**

- 2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

**3. Buyer due diligence requirements**

- 3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
- 3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
  - 3.1.2. operating processes and procedures and the working methods of the Buyer;

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
  - 3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.
- 3.2. The Supplier confirms that it has advised the Buyer in writing of:
- 3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
  - 3.2.2. the actions needed to remedy each such unsuitable aspect; and
  - 3.2.3. a timetable for and the costs of those actions.

## **4. Licensed software warranty**

- 4.1. The Supplier represents and warrants that:
- 4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;
  - 4.1.2. all components of the Specially Written Software shall:
    - 4.1.2.1. be free from material design and programming errors;
    - 4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
    - 4.1.2.3. not infringe any IPR.

## **5. Provision of ICT Services**

- 5.1. The Supplier shall:
- 5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
- 5.1.3. ensure that the Supplier System will be free of all encumbrances;
- 5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
- 5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

## **6. Standards and Quality Requirements**

- 6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").
- 6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
- 6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
  - 6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
  - 6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
  - 6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

## **7. ICT Audit**

- 7.1. The Supplier shall allow any auditor access to the Supplier premises to:
  - 7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
- 7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

## 8. Maintenance of the ICT Environment

- 8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
- 8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (other than to the Core Network) (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
- 8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance, including to the Core Network.
- 8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

## 9. Intellectual Property Rights in ICT

### 9.1. Assignments granted by the Supplier: Specially Written Software

- 9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:
  - 9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
  - 9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

- 9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
- 9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
- 9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

- 9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

**9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer**

- 9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:
- a) of its own Existing IPR that is not COTS Software;
  - b) third party software that is not COTS Software
- 9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution,

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

- 9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

- 9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

- 9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

### **9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer**

- 9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

- 9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

- 9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1. will no longer be maintained or supported by the developer;  
or

9.3.4.2. will no longer be made commercially available

### **9.4. Buyer's right to assign/novate licences**

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

### **9.5. Licence granted by the Buyer**

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

### **9.6. Open Source Publication**

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation,

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

running or security of the Specially Written Software, New IPRs or the Buyer System;

- 9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
  - 9.6.2.3. do not contain any material which would bring the Buyer into disrepute;
  - 9.6.2.4. can be published as Open Source without breaching the rights of any third party;
  - 9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and
  - 9.6.2.6. do not contain any Malicious Software.
- 9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:
- 9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
  - 9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

## 9.7. Malicious Software

- 9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.
- 9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

## **10. Supplier-Furnished Terms**

### **10.1. Software Licence Terms**

10.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Annex A of this Call Off Schedule 6.

10.1.2. Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Annex B of this Call Off Schedule 6.

### **10.2. Software Support & Maintenance Terms**

10.2.1. Additional terms for provision of Software Support & Maintenance Services are detailed in Annex C of this Call Off Schedule 6.

### **10.3. Software as a Service Terms**

10.3.1. Additional terms for provision of a Software as a Service solution are detailed in Annex D of this Call Off Schedule 6.

### **10.4. As a Service Terms**

10.4.1. Additional terms for provision of a devices, utility and consumption models for technology infrastructure generally described as "As a Service" solutions are detailed in Annex E to this Call-Off Schedule 6.

## **ANNEX A**

### **Non-COTS Third Party Software Licensing Terms**

**Not Used**

## **ANNEX B**

### **COTS Licensing Terms**

#### **Entrust - General Terms and Conditions**

These general terms and conditions (“General Terms”) apply to a purchase of one or more Offerings (as defined in Section 1 below) and are made part of a legally binding agreement by and between Entrust Corporation or other affiliate company (“Entrust”) identified in the Order (as defined in Section 1 below) and the purchaser identified on the Order (“Customer”). When purchasing through Entrust’s online portal, you, as the individual making the purchase, represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example the company or organization you work for, you represent to Entrust that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS, USE, DOWNLOAD, AND/OR INSTALL THE ENTRUST OFFERING. THE CONTINUED RIGHT TO ACCESS AND USE THE ENTRUST OFFERING IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (AND BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

#### **1. Contract Structure and Parties.**

- 1.1. These General Terms govern purchase of, access to, and use of any one or more of the following Entrust products and services (each, an “Offering”): (a) one or more executable software modules and associated deployment tools in machine-readable form (“Software”); (b) managed or cloud services hosted by Entrust or its hosting providers (“Hosted Service”); (c) technical support, training and Software maintenance (“Support”); (d) consulting and other professional services (“Professional Services”); (e) hardware, equipment and supplies (together, “Hardware and Supplies”). Each Offering consists of the features, and is further subject to the offering-specific terms and conditions, set out in the applicable terms of use or schedule attached hereto, provided with the Offering, available on Entrust’s website at <https://www.entrust.com/legal-compliance/terms-conditions> (each set of terms of use and

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

each schedule, a “Offering Schedule”), or as otherwise set forth herein. Without limiting the foregoing:

- 1.1.1. If an Order calls for any Software (whether or not as part of or in connection with another Offering), and no more specific Schedule is provided with the Software, the Schedule for the Software is the end user license available at <https://www.entrust.com/end-user-license.pdf>.
  - 1.1.2. If an Order calls for any Hardware and Supplies to be provided by Entrust as part of an Offering then the Hardware and Supplies Schedule, available at <https://www.entrust.com/hardware-suppliesschedule.pdf>, shall apply to that portion of the Offering.
  - 1.1.3. If an Order calls for Support to be provided by Entrust for an Offering, any such support will be provided pursuant to the then-current Support Schedule for the applicable Offering as referenced within the applicable Offering Schedule or available at <https://www.entrust.com/legalcompliance/terms-conditions>.
- 1.2. An “Order” for one or more Offering(s) means a document, such as a quote, sales order, price list, invoice, or statement of work, issued by Entrust offering to provide the Offering(s) to Customer directly, through an Entrust-authorized reseller (“Partner”), or via an online purchase portal.
- 1.3. Each Order, together with these General Terms, the applicable Schedule(s) for the Offering(s) listed on the Order, and, in the case of Professional Services Offerings through a Partner, a statement of work duly signed by Entrust and Customer, constitute the sole and entire “Agreement” between Customer and Entrust for the Offering(s). Entrust’s assent to the Agreement and to provide any Offering is expressly conditional on Customer’s acceptance of the terms and conditions of the Agreement, which acceptance Customer indicates by providing or authorizing payment or using the Offering. Any terms and conditions on any printed form of Customer are hereby expressly rejected by Entrust.
- 1.4. In the Agreement, “Affiliate” means, with respect to Entrust, any subsidiary of Entrust Corporation, and, with respect to Customer, any corporation or other entity that is directly or indirectly controlled by Customer either through ownership of fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control.

## 2. **Fees and Taxes.**

- 2.1. Customer will pay to Entrust the amounts set forth in the Order(s) (including where overages are applicable, any overage fees). All amounts due under the Agreement to Entrust must be paid to the Entrust Affiliate that issued the applicable invoice. Except as otherwise stated in the applicable Order, fees will be invoiced before the beginning of the Offering Term, and Customer will pay all amounts payable under the Agreement within thirty (30) days of the date of the invoice, without setoff or counterclaim, and without any deduction or withholding. Entrust may elect to charge Customer interest for late fees at the lesser of 1.5% per month or the maximum rate permitted by law. In addition, if payment is not received within fifteen (15) business days of written notice that a payment is delinquent, Entrust may suspend provision of all or part of a product or service, may refuse any additional Orders, and may require a fee to reinstate the product or service.
- 2.2. Customer will be responsible for any taxes (other than taxes based on Entrust’s net income), fees, duties, or other similar governmental charge. Should any taxes be due, Customer will

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

pay such taxes. Sales and use taxes can be reduced if Customer provides Entrust with an exemption certificate or document acceptable to the appropriate authorities exempting Customer from payment of these taxes. Entrust, for its part, will provide Customer with applicable certificates, forms, or other information as Customer reasonably requests to document exemption or reduction of withholding tax, which is the liability of the Customer.

- 2.3. Notwithstanding any of the foregoing, if Customer has purchased any Offering through a Partner then the terms relating to fees and taxes will be those terms established between the Customer and such Partner instead of those set out above.

### 3. **Term and Termination.**

- 3.1. The General Terms and Schedules shall be in effect commencing on the date of the first Order is accepted and will remain effective for a period of three (3) years and shall automatically renew for one year periods thereafter unless written notice of non-renewal is provided by a party to the other party no less than sixty (60) days prior to the end of the initial period or renewal period, as applicable, unless terminated sooner in accordance with this Agreement.
- 3.2. The obligations with respect to each Offering will commence on the date that the Order for the Offering is accepted by Entrust, unless otherwise specified in the Order or in the applicable Offering Schedule, and will remain effective for the period specified in the Order for the specific Offering, or in the applicable Offering Schedule, unless terminated earlier in accordance with this Agreement ("Offering Term").
- 3.3. For Offerings purchased on a subscription basis, including Support, the subscription shall automatically renew for a subsequent Offering Term ("Renewal Term") at the end of the then-current Offering Term, unless notice of cancellation is provided by a party to the other party at least sixty (60) days prior to the end of the then-current Offering Term. Notice of subscription cancellation may be provided by either party in writing in accordance with Section 21 (Notices), or, in the case of Customer, by such other mechanism provided by Entrust to facilitate such cancellations. The Renewal Term duration and fees will be as set out in Entrust's renewal reminder notice or in a separate renewal quote, or, if no notice or quote is provided, the fees will be Entrust's then-current list price and the renewal Offering Term will be one (1) year. Fees for any Renewal Term(s) will be charged using the method of payment on Entrust's file for the Customer's account. The Agreement for the Offering for the Renewal Term will be deemed to be updated with the Renewal Term fees and duration, but will otherwise remain the same unless amended by the parties in accordance with Section 29 (Amendment).
- 3.4. Either party may terminate the Agreement by giving notice to the other party: (i) if the other party commits a material breach of the Agreement and fails to remedy such material breach within thirty (30) days after delivery of notice by the non-breaching party of the occurrence or existence of such breach or such longer period as may be agreed to in writing by the non-breaching party; (ii) if the other party (A) applies for or consents to the appointment of a receiver, trustee, or liquidator for substantially all of its assets or such a receiver, trustee, or liquidator is appointed, (B) has filed against it an involuntary petition of bankruptcy that has not been dismissed within thirty (30) days thereof, (C) files a voluntary petition of bankruptcy, or a petition or answer seeking reorganization, or an arrangement with creditors, or (D) seeks to take advantage of any other law relating to relief of debtors, or makes an assignment for the benefit of creditors; or (iii) with respect to a particular Offering, as otherwise provided in the applicable Schedule.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

### 3.5. Effects of Termination and Expiration.

3.5.1. Termination of Agreement for Offerings. Upon termination of the Agreement for any Offering, Entrust will have no further obligation to provide the Offering, Customer will immediately cease all use of the Offering, and Customer will destroy any copies of documentation and delete any software Offering in its possession or control.

3.5.2. General. Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Any provision of this Agreement which contemplates or requires performance after the termination of this Agreement or that must survive to fulfill its essential purpose, including the terms of this Section (Term and Termination), confidentiality, disclaimers, limitations and exclusions of liability, and any payment obligations, will survive the termination and continue in full force and effect until completely performed.

3.5.3. Termination Fees. In the event of any termination by Customer, Customer is required to pay to Entrust any unpaid fees for any terminated Offerings in accordance with Section 2 (Fees and Taxes). Entrust will not be required to refund the Customer any fees paid in advance. For clarity, all fees are noncancellable and non-refundable notwithstanding any termination of this Agreement.

4. **Confidentiality.** In this Section (Confidentiality), “Discloser” means the party that discloses Confidential Information (defined below), and “Recipient” means the party that receives it. If Confidential Information is disclosed or received by an Affiliate of a party, it is deemed to have been disclosed or received by the party itself. The Recipient will use all Confidential Information it receives only for the purpose of exercising its rights and fulfilling its obligations under the Agreement. Recipient will treat such Confidential Information with the same degree of care against unauthorized use or disclosure that it affords to its own information of a similar nature, but no less than reasonable degree of care. Recipient will not remove or destroy any proprietary or confidential legends or markings placed upon any documents or other materials. Recipient will only disclose Discloser’s Confidential Information to Recipient’s and its Affiliates’ personnel and agents with a need to know (“Recipient Agents”). Recipient shall be responsible for ensuring Recipient Agents comply with the confidentiality obligations of this Section (Confidentiality) and any acts or omissions of a Recipient Agent in breach of the terms and conditions of this Section (Confidentiality) shall be considered the acts or omissions of the Recipient. “Confidential Information” means any business, technical, financial, or other information, however conveyed or presented to the Recipient, that is clearly designated by the Discloser as being confidential or that ought reasonably to be considered confidential by the Recipient, including all information derived by the Recipient from any such information. Confidential Information does not include any information that: (i) is expressly excluded from the definition of Confidential Information in an applicable Schedule; (ii) was lawfully known by Recipient prior to disclosure; (iii) was lawfully in the public domain prior to its disclosure, or becomes publicly available other than through a breach of the Agreement; (iv) was disclosed to Recipient by a third party without a duty of confidentiality to the Discloser; (v) is independently developed by Recipient without reference to Discloser’s Confidential Information; or (vi) is Feedback (as defined below). If Recipient is compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law, to disclose Confidential Information of the Discloser, Recipient will use reasonable efforts to seek confidential treatment for such Confidential Information, and, if and as permitted by law, will provide prior notice to the Discloser to allow the Discloser to seek protective or other court orders. Recipient agrees that its breach of this Section (Confidentiality) may cause Discloser irreparable injury, for

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

which monetary damages may not provide adequate compensation, and that in addition to any other remedy, Discloser may be entitled to injunctive relief against such breach or threatened breach. Personal Data and Excluded Data (each as defined in Section 5 (Data Protection) below) are excluded from the general definition of “Confidential Information” and the application of this Section (Confidentiality) but are subject to the specific confidentiality and other provisions of Section 5 (Data Protection).

### 5. **Data Protection.**

- 5.1. To the extent that Entrust processes any Customer Personal Data (as defined in the latest version of Entrust’s customer data processing agreement (“DPA”), which is available at <https://www.entrust.com/legalcompliance/data-privacy>) on Customer’s behalf and in performance of the Agreement, the terms of the DPA, which are hereby incorporated by reference, shall apply and the parties agree to comply with such terms. Customer’s acceptance of this Agreement shall be treated as acceptance and signing of the DPA (including the Standard Contractual Clauses attached to the DPA). Entrust reserves the right to update the DPA from time to time to comply with legal and regulatory requirements, and to keep current with upgrades and enhancements to its products and services. The latest version posted on Entrust’s website shall always apply and upon request Customer may receive update notifications.
- 5.2. Customer represents and warrants that it will not provide or transfer or cause to be provided or transferred to Entrust any Excluded Data, except if and as the provision or transfer of Excluded Data is expressly required and addressed in a Schedule. “Excluded Data” means: (i) social security numbers or their equivalent (e.g., social insurance numbers), driver license numbers, and health card numbers; (ii) other personal data that would be considered sensitive in nature including information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation; (iii) data falling into a "special category of data" under EU General Data Protection Regulation; (iv) “cardholder data” as defined by the Payment Card Industry Data Security Standards; (v) data regulated under the Health Insurance Portability and Accountability Act or the Gramm-Leach-Bliley Act or similar laws or regulations in place now or in the future in the applicable jurisdiction (collectively, the “Excluded Data Laws”). Customer recognizes and agrees that, except to the extent specified in a Schedule: (i) Entrust has no liability for any failure to provide protections set forth in the Excluded Data Laws or otherwise to protect Excluded Data; and (ii) Entrust’s Offerings are not intended for management or protection of Excluded Data and may not provide adequate or legally required security for Excluded Data. To the extent that Entrust obtains data, including Excluded Data, that is not necessary for Entrust to provide its Offerings or which Entrust reasonably considers unlawful, harmful or inappropriate, or infringes third party rights, Entrust shall have the right to delete such data without further notice or obligation to the Customer.

### 6. **Customer’s Responsibilities.**

- 6.1. Customer’s Users. Customer is responsible for the use of the Offering by any individual, organization or legal entity, including Customer’s Affiliates (each, a “Person”) who directly or indirectly receives access to, or the ability to use, the Offering or any component thereof through the Customer, including any such Persons more specifically described in the user guide, manual, technical specifications or release notes for the applicable Offering provided

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

by Entrust, all as may be updated from time to time ("Documentation") or described in the applicable Schedule (each such Person, a "User"). Any act or omission of a User with respect to an Offering is deemed to be the act or omission of Customer.

- 6.2. General Restrictions. Customer will not: (a) host, time-share, rent, lease, sell, license, sublicense, assign, distribute or otherwise transfer or allow third parties to exploit any component of any Offering, except as provided in the Agreement; (b) copy, modify, translate, reverse engineer, de-compile or disassemble, or create derivative works from any Offering except to the extent that law explicitly prohibits this restriction notwithstanding a contractual restriction to the contrary; (c) attempt to find, circumvent, bypass, exploit, defeat, or disable any limitations, restrictions, security vulnerabilities, security mechanisms, filtering capabilities, or entitlement mechanisms that are present or embedded in any Offering or any component thereof; (d) provide any passwords or other log-in information provided by Entrust as part of any Offering to any third party; (e) share non-public features or content of any Offering with any third party; (f) access any Offering in order to build or benchmark against a competitive product or service, or to build a product or service using similar ideas, features, or functions of any Offering; (g) use any Offering to transmit or store content or communications (commercial or otherwise) that is infringing, illegal, harmful, unwanted, inappropriate, objectionable, confirmed to be criminal misinformation or that otherwise poses a threat to the public, or viruses, malware, worms, time bombs, Trojan horses and other harmful or malicious codes, files, scripts, agents or programs; (h) attempt to gain unauthorized access to any Offering, or to gain access by any means, including automated means (e.g. bots) other than those set out in the Documentation; (i) use any Offering bundled with or provided for use with another Offering independently of the applicable bundle or Offering with which it is intended to be used; (j) use any Offering other than in compliance with all applicable laws and regulations (k) sell or resell the Offering or any component thereof to any third-party, including but not limited to Customer's distribution partners, resellers, or end-customer(s), unless otherwise explicitly permitted by Entrust in the Agreement.
- 6.3. Hosted Services Restrictions. Customer will not: (a) attempt or make any denial of service (DoS) attack on any Offering or any other conduct that attempts to disrupt, disable, or overload any Offering; (b) distribute, publish, send, or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations (or "spam") using any Offering; (c) violate the security, integrity, or availability of any user, network, computer or communications system, software application, or network or computing device using any Offering; (d) use any Offering to engage in or encourage any activity that is illegal, fraudulent, deceptive, harmful, violating others' rights, or harmful to Entrust's business operations or reputation; (e) interfere with or otherwise negatively impact any aspect of an Offering or any third-party components linked to any Offering; (f) create a false identity or any attempt to mislead others as to the identity of the sender or the origin of any data or communications.
- 6.4. High Risk Applications. Customer may not use, or authorize others to use, any part of any Offering in any application in which the failure of the Offering could lead to death, personal injury or severe physical or property damage ("High-Risk Applications"), including the monitoring, operation or control of nuclear facilities, mass transit systems, aircraft navigation or aircraft communication systems, air traffic control, weapon systems and direct

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

life support machines. Entrust expressly disclaims any express or implied warranty of fitness for High Risk Applications.

7. **Professional Services.** If Entrust provides any consulting or other professional services and any related deliverables (“Professional Services”) with respect to any Offering, the following provisions shall apply with respect to such Professional Services, unless a separate professional services agreement has been entered by the parties (e.g. Letter of Engagement).

- 7.1. An Order (or in the case of purchases of Professional Services Offerings through a Partner, a statement of work duly signed by Entrust and Customer) will further set out the scope and details of any Professional Services, including, if and as applicable, resource specialist(s), milestones, delivery dates, acceptance criteria, payment terms and any other information and terms related to the Professional Services.
- 7.2. Background and Professional Services IP. Any intellectual property rights of a party or its Affiliates conceived, created, developed, or reduced to practice prior to, or independently of, any Professional Services provided under the Agreement (“Background IP”) shall remain the exclusive property of such party or its Affiliate. Customer grants Entrust a non-exclusive, non-transferable, royalty-free, worldwide license for the term of the applicable Order to make, use and copy any Customer Background IP that it discloses to Entrust, but solely to the extent necessary for Entrust to provide the Professional Services to the Customer pursuant to the Order. The Professional Services, including all deliverables, are not “works for hire”, and the intellectual property embodied therein is owned by Entrust (“Professional Services IP”). Entrust grants Customer a nonexclusive, non-transferable, royalty-free, worldwide, perpetual license to any Professional Services IP incorporated into a deliverable, but solely to the extent necessary to use and exploit the deliverable as contemplated in the applicable Order and only so long as such Professional Services IP is embedded in the deliverable and not separated therefrom.

## 8. **Compliance with Applicable Laws.**

- 8.1. In the Agreement, the following terms have the following definitions:
- 8.1.1. “Denied Parties” means a Person that is subject to trade sanctions, embargoes, or other restrictions imposed by a relevant government or an international organization, including (i) a Person to whom the export of any product, software, or technology licensed or purchased under the Agreement, or related information, would be prohibited by the laws of the United States (“U.S.”), Canada, United Kingdom (“U.K.”), United Nations (“U.N.”), European Union (“E.U.”), or other applicable jurisdiction; or (ii) a Person listed on, or directly or indirectly owned or controlled by a Person listed on, or acting on behalf of a Person listed on, any U.S, Canadian, E.U., U.K., or U.N. sanctions list, including the list of Specially Designated Nationals maintained by the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”), and the U.S. Department of Commerce Entities List (“Entities List”).
- 8.1.2. “Restricted Country” means a country where Entrust prohibits all business due to the imposition of comprehensive sanctions by a relevant government or international organization or the presence of other higher sanctions risk, including (i) any country to which the export of any product, software, or technology licensed or purchased under the Agreement, or related information, would be prohibited by the applicable laws, rules or regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (ii) any of the countries listed at <https://www.entrust.com/legal-compliance/sanctioned-countries>.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 8.2. Customer will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection with Customer's exercise of its rights and obligations under any part of the Agreement, including use or access by Users. Entrust will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations that may be required in connection with Entrust's provision of the Offerings in the normal course of its business (for clarity, laws applicable to Customer shall not be deemed applicable to Entrust merely because of Customer's use of Entrust's Offerings). Without limiting the foregoing, each party will comply with all applicable trade control laws, including any sanctions or trade controls of the E.U., Canada, the U.K., and the U.N.; the Export Administration Regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security; U.S. sanctions regulations administered by OFAC; or on the Entities List; and any import or export licenses required pursuant to any of the foregoing; and all applicable anti-money laundering laws, including the U.S. Bank Secrecy Act, Money Laundering Control Act, and Patriot Act, the Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the U.K. Proceeds of Crime Act, and legislation implementing the International Convention on the Suppression of the Financing of Terrorism or the money laundering provisions of the U.N. transnational Organized Crime Convention.
- 8.3. Customer represents and warrants that: (a) neither Customer nor any User is located in, under the control of, or a national or resident of any Restricted Country; (b) neither Customer nor any User is a Denied Party; (c) Customer and each User has and will comply with applicable laws, rules and regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction(s) and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust; (d) Customer and all Users will not use any Offering for any purposes prohibited by applicable laws, rules or regulations on trade controls, including related to nuclear, chemical, or biological weapons proliferation, arms trading, or in furtherance of terrorist financing; (e) neither Customer nor any User nor any of its affiliates, officers, directors, or employees is a Denied Party or directly or indirectly owned or controlled by a Denied Party; or (ii) located in, incorporated under the laws of, or owned (meaning 50% or greater ownership interest) or otherwise, directly or indirectly, controlled by, or acting on behalf of, a person located in, residing in, or organized under the laws of any Restricted Country; and (f) Customer and each of its Users is legally distinct from, and not an agent of any Denied Party. Entrust represents and warrants that neither Entrust, nor any of its affiliates, officers, directors, or employees is a Denied Party or an agent of any Denied Party. In the event any of the above representations and warranties is incorrect or a party or any of the Customer's Users engages in any conduct that is contrary to sanctions or trade controls or other applicable laws, regulations, or rules, any Agreements, purchase orders, performance of services, or other contractual obligations of the other party are immediately terminated.
- 8.4. Where Customer is provisioning services to Users using Entrust Offerings, it shall have and enforce appropriate procedures and controls to ensure services are not provisioned to a Denied Party or a User in a Restricted Country. Entrust further reserves the right to implement geo-blocking, require Users undergo Entrust's due diligence review, or such other measures as it deems necessary to ensure that the Offerings are not provided to a Denied Party or User in a Restricted Country or otherwise in violation of applicable export control, trade or financial sanctions laws, regulations, orders, directives, licenses and requirements of any governmental or relevant authority with jurisdiction over activities undertaken in connection with this Agreement. In the event that Entrust reasonably determines that a User may be a Denied Party

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

or in a Restricted Country, Entrust may restrict access to said User without any further liability to Customer.

- 8.5. Customer shall immediately notify Entrust if, during the Term, it has breached the terms of this Section (Compliance with Applicable Laws) of the Agreement. If Entrust has reason to believe that a breach of this Section (Compliance with Applicable Laws) has occurred or may occur, Entrust shall have the right, in its sole discretion, to audit at its own expense Customer's business records, data, and other such documents and information that Entrust may deem relevant in order to satisfy itself that no such breach has occurred or will occur. Customer agrees in the context of any audit undertaken pursuant to this paragraph to use its best efforts to make or cause to be made available relevant individuals and/or information. Any breach of this Section (Compliance with Applicable Laws) shall be considered a material breach of the Agreement.
- 8.6. Customer understands and agrees that Entrust is not responsible for service interruptions or blocks that may be experienced by Users using third party devices (e.g. Huawei mobile phones) that may interoperate with an Entrust Offering, to the extent that trade compliance restrictions, legal obligations, or information security requirements applicable to Entrust do not allow for compliance with third party device requirements.

### **9. Disclaimer of Warranties.**

**Except as may be so expressly stated elsewhere in the Agreement, each Offering is provided "as is", and Entrust and its Affiliates, licensors and suppliers disclaim any and all representations, conditions or warranties of any kind, express or implied, including warranties of non-infringement, title, merchantability or fitness for a purpose, satisfactory quality, or any representations, conditions or warranties implied by statute, course of dealing, course of performance, or usage or trade. Entrust makes no representations, conditions or warranties regarding any third party product or service, with which any Offering may interoperate. Entrust makes no representations, conditions or warranties that any Software will perform without interruption or error.**

### **10. Indemnities.**

#### **10.1. Intellectual Property Claims.**

**10.1.1. Intellectual Property Indemnity. Entrust shall defend at its expense (including, for clarity, bearing court costs and reasonable attorney's fees) Customer against any claims by third parties that the Software, Hosted Service, or Hardware and Supplies furnished and used within the scope of the Agreement infringes upon or misappropriates a patent, trademark, copyright, trade secret or other intellectual or proprietary right (an "IP Claim"), and will pay any (i) amounts finally awarded against Customer by a court or arbitrator in any proceeding related to such IP Claim or (ii) settlement amounts approved in accordance with this Section (Indemnities).**

**10.1.2. Mitigation by Entrust. If Entrust becomes aware of an actual or potential IP Claim, or if Customer provides Entrust with notice of an actual or**

potential IP Claim, Entrust may (or in the case of an injunction against Customer, shall), at Entrust's sole option and expense: (i) procure for Customer the right to continue to use the affected portion of the Software, Hosted Service, or Hardware and Supplies; (ii) modify or replace the affected portion of the Software, Hosted Service, or Hardware and Supplies with functionally equivalent or superior software or products so that Customer's use is non-infringing; or (iii) if (i) or (ii) are not commercially reasonable, terminate the Agreement with respect to the affected Software, Hosted Service, or Hardware and Supplies and refund to the Customer, as applicable, either (A) any perpetual purchase price paid for the affected Software or Hardware and Supplies depreciated over a three (3) year period from the date of delivery on a straight line basis less any outstanding moneys owed on such affected portion of the Software or Hardware and Supplies; or (B) any prepaid and unused subscription fees for the affected Software, Hosted Service or Hardware and Supplies for the terminated portion of the applicable Offering Term.

10.1.3. **Exceptions to Indemnity.** Entrust shall have no liability for any IP Claim in respect of any Software, Hosted Service, or Hardware and Supplies to the extent that: (i) such Software, Hosted Service, or Hardware and Supplies is used by Customer outside the scope of the rights granted in the Agreement or in a manner or for a purpose other than that for which it was supplied, as contemplated by the Documentation; (ii) such Software, Hosted Service, or Hardware and Supplies is modified by Customer; (iii) such Software, Hosted Service, or Hardware and Supplies is used by Customer in combination with other software, services, or equipment not provided by Entrust and the infringement arises from such combination or the use thereof; (iv) the IP Claim arises from information, data or specifications provided by Customer; (v) the Software, Hosted Service, or Hardware and Supplies was provided on a beta testing, proof of concept, evaluation or "not for resale" basis; or (vi) the IP Claim relates to the use of any version of the Software other than the current, unaltered release, if such IP Claim would have been avoided by the use of a current unaltered release of the Software.

10.1.4. **THE PROVISIONS OF THIS SECTION 10.1 (INTELLECTUAL PROPERTY CLAIMS) ARE SUBJECT TO SECTION 11 (LIABILITY) AND STATE THE SOLE AND EXCLUSIVE LIABILITY OF ENTRUST AND ITS AFFILIATES AND THE SOLE AND EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO ANY CLAIM OF THE NATURE HEREIN.**

10.2. **Customer Data and Use Claims.** Customer agrees to defend, indemnify and hold harmless Entrust, its Affiliates and licensors, and each of their respective employees, officers, directors, and representatives against any and all third party claims, demands, suits or proceedings, fines, costs, damages, losses, settlement fees, and expenses (including investigation costs and attorney fees and disbursements) arising out of or related to: (a) Customer's breach of, or errors in providing, the representations and warranties set out in Section 5 (Data Protection) or Section 8 (Compliance with Applicable Laws), (b) the Personal Data or Excluded Data provided by the Customer or its Users (c) any inaccuracies in any data provided by Customer or Users to Entrust,

and (d) the misuse or misconfiguration of any Software or Hosted Service by the Customer or any of its Users (each of (a)-(d), a “Customer Indemnified Claim”).

- 10.3. **Conditions.** The obligations in this Section (Indemnities) will apply only if indemnified party: (i) provides the indemnifying party prompt written notice of the IP Claim or Customer Indemnified Claim (“Claim”), provided that failure by the indemnified party to provide prompt notice will relieve the indemnifying party of its obligations only to the extent that the indemnifying party was actually and materially prejudiced by such failure; (ii) gives the indemnifying party the exclusive right to control and direct the investigation and defense of such Claim, including appeals, negotiations, and any settlement or compromise thereof, provided that the indemnified party will have the right to reject any settlement or compromise that requires that it or they admit wrongdoing or liability or that subjects it or them to any ongoing affirmative obligations; (iii) has not compromised or settled the Claim; and (iv) agrees to cooperate and provide reasonable assistance (at indemnifying party’s sole expense) in the defense.

**11. Liability.**

- 11.1. In this Section (Liability), “Entrust” will be deemed to mean Entrust Corporation, its Affiliates, and their respective suppliers, licensors, resellers, distributors, subcontractors, directors, officers, and personnel.
- 11.2. In no event will Entrust be liable for, and Customer waives any right it may have to, any consequential, indirect, special, incidental, punitive or exemplary damages or for any loss of business, opportunities, revenues, profits, savings, goodwill, reputation, customers, use, or data, or costs of procurement or business interruption.
- 11.3. For any given Offering, in no event will Entrust’s total aggregate liability arising out of or related to the Agreement or the use and performance of the Offering exceed the fees paid to Entrust for the specific Offering for the twelve months prior to the first event giving rise to liability, less any refunds, service credits or deductions.
- 11.4. The exclusions and limits in this Section (Liability) apply: (a) regardless of the form of action, whether in contract (including fundamental breach), tort (including negligence), warranty, indemnity, breach of statutory duty, misrepresentation, strict liability, strict product liability, or otherwise; (b) on an aggregate basis, regardless of the number of claims, transactions, digital signatures or certificates; (c) even if the possibility of the damages in question was known or communicated in advance and even if such damages were foreseeable; and (d) even if the remedies fail of their essential purpose. Customer acknowledges that Entrust has set its prices and entered into the Agreement in reliance on the limitations and exclusions in this Section (Liability), which form an essential basis of the Agreement.
- 11.5. Notwithstanding anything to the contrary in this Section (Liability) or elsewhere in the Agreement, to the extent required by applicable law Entrust neither excludes nor limits its liability for: (i) death or bodily injury caused by its own negligence; (ii) its own fraud or fraudulent misrepresentation; or (iii)

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

**other matters for which liability cannot be excluded or limited under applicable law.**

12. **Nature of Relationship.** Nothing contained in the Agreement will be deemed to constitute either party or any of its employees, the partner, agent, franchisee, or legal representative of the other party or to create any fiduciary relationship for any purpose whatsoever. Except as otherwise specifically provided in the Agreement, nothing in the Agreement will confer on either party or any of its employees any authority to act for, bind, or create or assume any obligation or responsibility on behalf of the other party. The parties agree that no Entrust personnel is or will be considered the personnel of Customer.
13. **Affiliates.** Entrust may use one or more Affiliate(s) or subcontractors to perform its obligations under the Agreement, provided that such use will not affect Entrust's obligations under the Agreement.
14. **Non-Solicitation.** Customer acknowledges that Entrust has specially trained personnel and agrees that during the term of this Agreement and for one (1) year following the term Customer will not solicit or otherwise attempt to employ any such personnel who have been engaged in the performance of the Agreement and/or with whom Customer has contact by virtue of the Agreement, without the prior written consent of Entrust; provided that such restriction does not apply to the hiring of employees who respond without solicitation by Customer to Internet or other advertisements of general circulation not specifically targeted to such employees.
15. **Third Party Beneficiaries.** Except as expressly stated in the Agreement, the Agreement is made solely for the benefit of the parties hereto and their respective successors and permitted assigns, and no other person or entity will have or acquire any right or benefit under the Agreement, including under the UK Contracts (Rights of Third Parties) Act 1999.
16. **No Exclusivity.** Nothing in the Agreement shall prevent Entrust or its Affiliates from providing to a third party the same or similar products, services or deliverables as those provided to the Customer pursuant to the Agreement.
17. **Notices.** In any case where any notice or other communication is required or permitted to be given, such notice or communication will be in writing and (a) personally delivered, in which case it is deemed given and received upon receipt or (b) sent by international air courier service with confirmation of delivery to the addresses stated below, in which case it is deemed given and received when delivery is confirmed.

Notices to Customer: the address stipulated in the Order.

Notices to Entrust: 1187 Park Pl., Shakopee, MN 55379-3817, USA

18. **Choice of Law.** Any disputes related to the products and services offered under the Agreement, as well as the construction, validity, interpretation, enforceability and performance of the Agreement, and all claims arising out of or related to the Agreement, including tort claims, shall, (i) if Customer is located in Canada, be governed by the laws of the Province of Ontario, Canada, and shall be brought in the provincial or federal courts sitting in Ottawa, Ontario; (ii) if Customer is located in Europe, the Middle East, or Africa, be governed by the laws of England and Wales and shall be brought in the courts sitting in London, England; and (iii) if Customer is located anywhere else in the world, be governed by the laws of the State of Minnesota, United States, and shall be brought in the federal and state courts located in Hennepin County, Minnesota. Each party hereby agrees that the applicable courts identified in this Section (Choice of Law) shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial,

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

state or federal court each party waives any right that such party may have to a jury trial. To the maximum extent permitted by applicable law, the parties agree that the provisions of the United Nations Convention on Contracts for the International Sale of Goods, as amended, shall not apply to the Agreement.

19. **Force Majeure**. “Force Majeure Event” means any event or circumstance beyond Entrust’s reasonable control, including floods, fires, hurricanes, earthquakes, tornados, epidemics, pandemics, other acts of God or nature, strikes and other labor disputes, failure of utility, transportation or communications infrastructures, riots or other acts of civil disorder, acts of war, terrorism (including cyber terrorism), malicious damage, judicial action, lack of or inability to obtain export permits or approvals, acts of government such as expropriation, condemnation, embargo, designation as a Restricted Country, changes in applicable laws or regulations, and shelter-in-place or similar orders, and acts or defaults of third party suppliers or service providers. In the event that a Force Majeure Event directly or indirectly causes a failure or delay in Entrust’s performance of its obligations under this Agreement, Entrust shall not be in default or liable for any loss or damages where performance is impossible or commercially impracticable.
20. **No Waiver**. No failure to exercise, no delay in exercising, and no statement or representation other than by any authorized representative in an explicit written waiver, of any right, remedy, or power will operate as a waiver thereof, nor will single or partial exercise of any right, remedy, or power under the Agreement preclude any other or further exercise thereof or the exercise of any other right, remedy, or power provided in the Agreement, in law, or in equity. The waiver of the time for performance of any act or condition under the Agreement does not constitute a waiver of the act or condition itself.
21. **Successors; Assignment**. Each party agrees that it will not (and neither party has any right to) assign, sell, transfer, or otherwise dispose of, whether voluntarily, involuntarily, by operation of law, or otherwise, the Agreement or any right or obligation under the Agreement without the prior written consent of the other party. Any purported assignment, sale, transfer, delegation or other disposition in violation of this Section (Successors; Assignment) will be null and void. Notwithstanding the foregoing, Entrust may, without the consent of Customer, assign the Agreement together with all of its rights and obligations under the Agreement (i) to an Affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets of the business to which the Agreement relates. Subject to the foregoing limits on assignment and delegation, the Agreement will be binding upon and will inure to the benefit of the parties and their respective successors and permitted assigns.
22. **No Other Rights Granted**. The rights granted under the Agreement are only as expressly set forth in the Agreement. No other right or interest is or will be deemed to be granted, whether by implication, estoppel, inference or otherwise, by or as a result of the Agreement or any conduct of either party under the Agreement. Entrust and its licensors expressly retain all ownership rights, title, and interest in the products and services provided by Entrust (including any modifications, enhancements and derivative works thereof). Any permitted copy of all or part of any item provided to Customer must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust to Customer.
23. **Feedback**. “Feedback” refers to Customer’s and Users’ suggestions, comments, or other feedback pertaining to Entrust’s Offerings. Customer agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust all of Customer’s (and Users’) right, title, and interest thereto, including without limitation intellectual property rights.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

24. **Order of Precedence.** A provision in an Order executed by both parties will prevail over any conflicting provision elsewhere in the Agreement, and, subject to the foregoing, a provision in a Schedule will prevail with respect to the applicable Offering over any conflicting provision in the Agreement.
25. **Entire Agreement.** The Agreement (as defined in Section 1 (Contract Structure and Parties)) and items expressly incorporated into any part of the Agreement form the entire agreement of the parties. All terms and conditions on any purchase orders, supplier registration forms, supplier code of conduct, or similar document issued by Customer shall not amend the terms of the Agreement and will be of no force or effect notwithstanding any term or statement to the contrary made in such document. Neither party has entered into the Agreement in reliance upon any representation, warranty, condition or undertaking of the other party that is not set out or referred to in the Agreement.
26. **Amendment.** The Agreement may not be modified except by formal agreement in writing executed by both parties.
27. **Severability.** To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any provision of the Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of the Agreement is held to be invalid or otherwise unenforceable in application to particular facts or circumstances: (a) such provision will be interpreted and amended to the extent necessary to fulfill its intended purpose to the maximum extent permitted by applicable law and its validity and enforceability as applied to any other facts or circumstances will not be affected or impaired; and (b) the remaining provisions of the Agreement will continue in full force and effect. For greater certainty, it is expressly understood and intended that each provision that deals with limitations and exclusions of liability, disclaimers of representations, warranties and conditions, or indemnification is severable from any other provisions.
28. **Language.** The definitive version of this Agreement is written in English. If this Agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls. If Customer is located in Quebec, the parties hereby confirm that they have requested that this Agreement and all related documents be drafted in English; les parties ont exigé que le présent contrat et tous les documents connexes soient rédigés en anglais. Some versions of the Offerings which have been designated as localized or country-specific may nonetheless contain certain components and/or interfaces that are in the English language only.
29. **Interpretation.** The parties agree that the Agreement will be fairly interpreted in accordance with its terms without any strict construction in favor of or against either party, and that ambiguities will not be interpreted against the party that drafted the relevant language. In the Agreement, the words “including”, “include” and “includes” will each be deemed to be followed by the phrase “without limitation”. The section or other headings in the Agreement are inserted only for convenience and ease of reference and are not to be considered in the construction or interpretation of any provision of the Agreement. Any exhibit, document or schedule referred to in the Agreement means such exhibit or schedule as amended, supplemented and modified from time to time to the extent permitted by the applicable provisions thereof and by the Agreement. References to any statute or regulation mean such statute or regulation as amended at the time and includes any successor statute or regulation. Unless otherwise stated, references to recitals, sections, subsections, paragraphs, schedules and exhibits will be references to recitals, sections, subsections, paragraphs, schedules

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

and exhibits of the Agreement. All dollar amounts in the Agreement are in U.S. currency unless otherwise indicated.



Entrust  
general-terms 2025.p

### Entrust Managed Root CA Schedule

The Agreement for Entrust's Managed Root CA Offering is made up of this Schedule, the Entrust General Terms and Conditions at <https://www.entrust.com/general-terms.pdf> ("General Terms"), and an Order for the Managed Root CA Offering.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE HOSTED SERVICE. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICE IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

#### 1. **Definitions.**

Capitalized terms not defined in this Schedule have the meanings given to them in the General Terms.

- 1.1. "Certificate" means a digital document issued by the certification authority ("CA") that, at a minimum: (a) identifies the CA issuing it, (b) names or otherwise identifies a subject, (c) contains a public key of a key pair, (d) identifies its operational period, (e) contains a serial number and (f) is digitally signed by the CA.
- 1.2. "Root CA" means the CA that acts as the trust anchor at the top of a particular public key infrastructure (PKI) certification hierarchy. Standard PKI practice is that the Root CA be kept offline while not in use, to protect against compromise and assure the trust of the entire PKI hierarchy which is bound to the Root CA.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

2. **Service Details.** Subject to the Agreement, Entrust will provide the following as part of the Managed Root CA Offering:
  - 2.1. One of Entrust's technical experts to serve as the overall primary contact for Customer in order to ensure a successful Managed Root CA experience.
  - 2.2. High level design document and build as detailed in Section 3 (Included Onboarding/Setup Services) below, including implementation and configuration for one high assurance Root CA for Customer's PKI.
  - 2.3. Customer's Root CA will have the following characteristics:
    - 2.3.1. standalone and offline (no external interfaces).
    - 2.3.2. hosted in Entrust's ISO 27001 compliant data centers on a FIPS 140-2 level 3 hardware security module (HSM).
    - 2.3.3. HSM credentials will be issued during the key ceremony and provided to the designated Entrust and Customer custodians such that controlling quorum of credentials remains in Customer's possession.
3. **Included Onboarding/Setup Services.** Subject to the Agreement, Entrust will provide the following Professional Services as part of the Managed Root CA Offering:
  - 3.1. Discovery & Design Review
    - 3.1.1. Collaborative discovery process with Entrust technical staff and Customer's technical point of contact and other representatives as appropriate to determine and document Customer's business and technical requirements.
    - 3.1.2. Review solution design and determine required configuration of the Root CA (with HSM-protected key store) to meet Customer's requirements.
  - 3.2. Production Build
    - 3.2.1. Installation and configuration of Root CA as detailed during the design review.
  - 3.3. Formal key ceremonies as detailed below, including documented processes and procedures to perform signing operations for Certificates and revocation lists. The key ceremonies are designed to ensure that the chain of custody for the Root CA key is maintained and documented.
    - 3.3.1. Root CA implementation key ceremony, including:
      - creation of Root CA keys;
      - signing of one subordinate CA(s) if required;
      - creation of Root CA revocation list. The Offering includes one annual (1 time per year) support for the creation and signing of a revocation list.
    - 3.3.2. During the key creation ceremony, Customer's HSM physical credentials will be issued and assigned to Entrust and Customer representatives as determined by their assigned roles as specified in the solution design. Each party is responsible for the secure storage and handling of the HSM credentials assigned to its representatives.
    - 3.3.3. As the party who controls the quorum of HSM credentials, Customer is required to be present, either physically or virtually, during the key ceremonies to make up the quorum of HSM credentials. If Customer attends virtually, the physical credentials

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

containing Customer keys will be securely transferred between the parties in a manner mutually agreed by the parties.

- 3.3.4. The key ceremonies will be undertaken in accordance with standard industry practices and Entrust's standard key ceremony policy.

No travel by Entrust or per diems are required or included for the above Professional Services.

Any other Professional Services beyond the scope of this Section (Included Onboarding/Setup Services) may be provided pursuant to a separate statement of work agreed by the Parties.

4. **Assumptions and Limitations.** The Managed Root CA Offering is subject to the following assumptions and limitations:

- 4.1. The Customer's Root CA is not initialized on hardware dedicated to the customer. All Root CAs managed by Entrust (i.e. for different customers) use the same shared hardware and HSM infrastructure. Root CA and CA keys are provided on dedicated virtual images which are initialized onto the shared hardware under audit, these are removed to back up after use and the HSM zeroized.
- 4.2. The Root CA is not subject to any specific regulatory or industry compliance requirements (e.g. public trust/WebTrust audit criteria).
- 4.3. Root CAs hosted anywhere other than in Entrust data centers are outside the scope of the Managed Root CA Offering.
- 4.4. Since access to the Root CA is limited to the physically secured CA, logical security will be implemented only at the system and application layers and not at a network layer.
- 4.5. All access to the operating system will be controlled through administrative accounts with access to these accounts limited to assigned individuals (role holders).
- 4.6. Any variations in policy and procedures to address customized requirements for Customer are outside the scope of the Managed Root CA Offering.

5. **Customer Roles and Responsibilities.** Customer will be responsible for the following:

- 5.1. Identifying a primary technical point of contact within Customers' organization with respect to the Offering.
- 5.2. Providing assistance in identifying representatives from Customer's various internal and external stakeholders who have an interest or are affected by the Offering.
- 5.3. Facilitating scheduling of stakeholder representatives to participate in the exchange of information with Entrust.
- 5.4. Responding in a timely fashion to questions posed by Entrust regarding the Offering.
- 5.5. Attendance at all key ceremonies, with quorum of credentials.
- 5.6. Ensuring that Customer's credentials are stored in a secure location and protected from environmental threats.
- 5.7. Ensuring that Customer's credentials are used in accordance with the detailed design.
- 5.8. Reporting actual and/or suspected loss or damage of credentials or any other factor that may threaten the HSM or Root CA security.

6. **Policy and Compliance.** Entrust will operate the Managed Root CA Offering in ISO 27001 compliant facilities according to the operational standards and procedures laid down in accordance

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

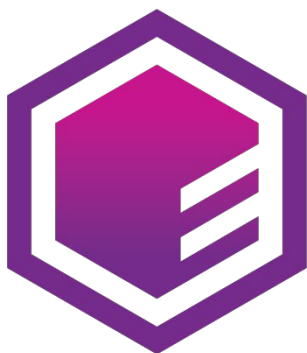
with Entrust's corporate security policies and standard operational practices for PKI administration and management.

7. **Term.** The Managed Root CA Offering is offered on a subscription basis for the Offering Term set out on the Order.
8. **Warranty.** Entrust warrants that the Professional Services it provides in connection with the Managed Root CA Offering shall be performed in a professional manner in keeping with reasonable industry practice.
9. **Support.** Entrust provides the support commitments for the Managed Root CA Offering set out at <https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf>.
10. **Fees.** Customer will pay the costs and fees for the Managed Root CA Offering as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

Template version: December 14 2022



managed-root-ca-sch  
edule.pdf



# ENTRUST

## GLOBAL PERSONAL DATA PROTECTION POLICY

Document Version	1.7
Date	17-Oct-2024

### Contents

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

1. Introduction .....	4	2.
Purpose .....	4	
3. Definitions .....	4	
4. Personal Data Processing Core Principles .....	5	
5. Data Classification .....	6	
6. Lawfulness and Adequacy .....	6	
6.1 Legal Bases for Processing Personal Data .....	6	
6.2 Privacy Assessments .....	7	
6.2.1 Privacy by Design Assessment .....	7	
6.2.2 Data Protection Impact Assessment (DPIA) .....	7	
6.2.3 Data Transfer Impact Assessment (DTIA) .....	7	6.2.4
Legitimate Interest Impact Assessment (LIIA) .....	7	
6.2.5 Standards for Handling Sensitive and Special Category Data .....	8	
6.3 Contractual Protections .....	8	
6.3.1 Intra-Group Data Transfer Agreement (IGDTA).....	8	
6.3.2 Data Processing Agreement (DPA) .....	8	
6.3.3 General Privacy Provisions.....	8	
7. Accuracy and Retention .....	8	
7.1 Records Management .....	8	
7.2 Storage and Backup of Personal Data .....	8	
7.3 Erasure or Destruction of Personal Data .....	9	
8. Confidentiality and Integrity .....	9	
8.1 Information Security .....	9	
8.2 Testing .....	10	
8.3 Reporting a Personal Data Incident .....	10	
8.4 Personal Data Incident Response .....	11	
9. Transparency .....	11	
9.1 Privacy Notices .....	11	
9.2 Training .....	12	
9.3 Data Subject Rights .....	12	
9.4 Supervisory Authorities .....	13	
9.5 Data Protection Officer .....	13	
10. Compliance .....	13	
11. Exceptions .....	13	
12. Ownership and Review .....	13	

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

12.1 Contact Information .....	13
--------------------------------	----

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

### d) 1. Introduction

Entrust Corporation and its subsidiaries (collectively, “Entrust” or the “Company”) process Personal Data relating to our colleagues and to business contacts at our sales partners, suppliers, and customers in our role as a data controller. Entrust also Processes Personal Data relating to our customers’ employees and end users in our role as a Data Processor. Where Entrust processes Personal Data, we do so in compliance with our legal and contractual obligations and with full transparency.

### e) 2. Purpose

This policy sets forth the requirements and elements of our global data privacy program which Entrust has established to ensure we comply with relevant legal and contractual obligations as well as certification and audit requirements. This policy applies globally to all Personal Data Processing performed by Entrust.

### f) 3. Definitions

**“Data Controller”** means the entity that determines the purpose and means of Processing Personal Data and has the same meaning ascribed to “PII Controller” under ISO 27701.

**“Data Processor”** means the entity that processes Personal Data on behalf of the data controller and has the same meaning ascribed to “PII Processor” under ISO 27701.

**“Data Protection Impact Assessment”** refers to a documented analysis by a data controller or data processor assessing privacy risks where Processing is likely to result in a high risk to the rights and freedoms of the data subject.

**“Data Protection Laws”** refers to all Personal Data protection and privacy laws and regulations applicable to Entrust, including, but not limited to, the EU General Data Protection Regulation (GDPR), UK General Data Protection Regulation (UK GDPR), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), and US state privacy laws, in each case as may be amended, superseded, or replaced.

**“Data Subject”** means the identified or identifiable person or household to whom Personal Data relates and has the same meaning ascribed to “PII Principal” under ISO 27701.

**“Data Transfer Impact Assessment”** refers to a documented analysis by a data controller or data processor of the impact and security implications of a transfer of Personal Data from inside the EEA or UK to a country outside the EEA/UK that does not have an adequacy finding by the European Commission or Information Commissioner's Office.

**“Legitimate Interest Impact Assessment”** refers to a documented analysis by a data controller or data processor as to whether legitimate interest can be used as the legal basis for Processing Personal Data. The assessment includes a three-prong test analyzing whether the Personal Data Processing is in pursuit of a legitimate interest, whether it is necessary for that pursuit, and whether the data subject’s interests override the legitimate interest.

**“Personal Data” or “PII”** has the meaning ascribed to “personally identifiable information,” “personal information,” or equivalent terms as such terms are defined under data protection laws.

**“Personal Data Incident”** has the meaning ascribed to “security incident,” “security breach” or “Personal Data breach” or equivalent terms as such terms are defined under data protection laws and includes any situation in which Entrust becomes aware that Personal Data has been accessed, disclosed, altered, lost, destroyed, or used by unauthorized persons, in an unauthorized manner.

**“Processing”** means any operation or set of operations that is performed on Personal Data, whether by automatic means, such as collection, recording, organization structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring or disclosing Personal Data to third parties.

**“Sensitive Personal Data”** is a subset of Personal Data and refers to information about a data subject that if lost, compromised, accessed, or improperly disclosed could result in harm, embarrassment, inconvenience, or unfairness to the data subject and is therefore subject to heightened protection.

**“Special Category Data”** is a subset of Personal Data and refers to information about an individual’s race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

g) 4. Personal Data Processing Core Principles

Entrust adheres to the following core principles when Processing Personal Data as a Data Controller:

- **Lawfulness and Adequacy:** We ensure Personal Data is collected for a lawful purpose and limited to what is relevant and necessary for that purpose.
- **Accuracy and Retention:** We keep our systems up to date, provide mechanisms to update inaccurate Personal Data and do not retain Personal Data longer than necessary to fulfill the lawful purpose for Processing.
- **Confidentiality and Integrity:** We ensure Personal Data remains secure and protected during Processing but respond swiftly and appropriately to Personal Data Incidents if they do occur, including providing timely notifications as required.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- **Fairness and Transparency:** We adequately inform data subjects when we process their Personal Data. We are clear about why we need it, how we will use it and how it will be handled and protected.

All Entrust colleagues are responsible for appropriately Processing and safeguarding Personal Data and understand that failure to do so has the potential not only to undermine customer confidence in Entrust, but to result in significant fines and penalties for the Company.

### h) 5. Data Classification

Entrust maintains a central record of its Processing activities. All Personal Data is classified into one of the following categories:

- 1 NO PII**  
Some technology solutions do not require Entrust to process/store personal data or pass any personal data to Vendors to process/store. The most common types of technology solutions that would not share data are desktop, firmware, on-premise, and operating system technology solutions.
- 2 LOGIN PII**  
Some technology solutions are not used for a purpose that requires processing personal data as part of the offering but because the technology solutions are cloud-hosted Vendor solutions, they may require a user's name, email, username, or password to access the technology solution. These are typically software as a service (SaaS) solutions.
- 3 PUBLICLY AVAILABLE PII**  
Publicly available PII is personal data that is accessible to anyone in the general public without the need for special qualifications, permissions, or privileges. Examples of this type of PII can include name, business mailing address, business email, business phone number, title/business function, and IP address.
- 4 NON-PUBLICLY AVAILABLE PII**  
This category is comprised of many types of personal data including but not limited to personal mailing address, personal email, personal phone number, date of birth, marital status, employment history, education history, employee identification number, salary/wage information, beneficiaries, work schedule or leave history (where access allows for aggregate information about an individual), and geo-location data. If any of this information is passed to or stored by a Vendor, or a Vendor has the ability to access this data, the Vendor is processing Entrust's non-publicly available personal data.
- 5 SENSITIVE PII**  
There are certain types of personal data that are more sensitive than others but do not qualify under the GDPR's definition of special category data. This data can still require special protections under other data privacy laws. This PII can include criminal records, financial data, tax information, bank account information, credit card information, and national ID/social security number.
- 6 SPECIAL CATEGORY PII**  
Special category PII is personal data that requires extra protection under GDPR and includes genetic data, biometric data, fingerprints, medical history, philosophical beliefs, political opinions, photo (where used for identification/verification), race/ethnicity, religious beliefs, sexual orientation, and union membership.

## 6. Lawfulness and Adequacy

### 6.1 Legal Bases for Processing Personal Data

When acting as a Data Controller, the Company only processes Personal Data as legally permitted.

Entrust principally relies on the following legal bases for Processing:

- Performance of a contract;
- Compliance with legal obligations, including but not limited to, lawful requests from law enforcement;

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- Legitimate interest, except where such interest is overridden by the interests or fundamental rights and freedoms of the data subject; and
- Consent.

Where consent is the legal basis for Processing, Entrust ensures that consent is freely given, specific, informed and an unambiguous indication of the data subject's wishes. The data subject has the right to withdraw consent at any time for any reason.

## 6.2 Privacy Assessments

### 6.2.1 Privacy by Design Assessment

Entrust evaluates Personal Data Processing against the core principles described in Section 4 above as part of its design and development of new or substantially modified product offerings and when onboarding vendor solutions where PII will be processed, including licensed in third party software applications. This "Privacy by Design" assessment is embedded in Entrust's development and vendor onboarding processes. Completion of the assessment requires review and approval by Entrust's Privacy and Information Security teams. Development may not move forward without approval.

#### i) 6.2.2 Data Protection Impact Assessment (DPIA)

When contemplated Personal Data Processing poses a high risk to an individual's rights and freedoms, Entrust completes a DPIA to document and assess the purpose for the Processing, how Entrust will comply with relevant Data Protection Laws and how the Company will mitigate potential risks to the Data Subject. Where a DPIA relates to Processing where Entrust is the

Data Controller, it is reviewed by Entrust's Data Protection Officer who must approve the proposed Processing before it commences.

#### ii) 6.2.3 Data Transfer Impact Assessment (DTIA)

Where Entrust intends to transfer Personal Data from inside the European Economic Area (EEA) or United Kingdom (UK) to a country outside of the EEA or UK that does not benefit from an adequacy finding by the European Commission or UK Information Commissioner's Office, Entrust completes a formal DTIA to analyze the impact and security implications of the transfer, particularly where the laws of the receiving country could allow its government access to the Personal Data being transferred. Entrust will only proceed with the transfer where it concludes the risk posed by the transfer is acceptable.

#### iii) 6.2.4 Legitimate Interest Impact Assessment (LIIA)

Where Entrust acts as a Data Controller and relies on legitimate interest as the legal basis for Processing Personal Data, the Company completes a formal LIIA to document and assess the

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

legitimate interest, determine whether the Processing is necessary, and evaluating whether the Data Subject's interests, rights and freedoms outweigh or override the legitimate interest. Entrust will only proceed with the Processing on the basis of legitimate interest where the LIIA concludes that the legitimate interest is not so overridden.

### iv) 6.2.5 Standards for Handling Sensitive and Special Category Data

In its role as a Data Controller, Entrust processes Sensitive Personal Data relating to colleagues across various business systems and some limited Special Category Data on a voluntary basis and as permitted by local law. Appropriate controls are in place and outlined in applicable DPIAs, the [Access Control Standard for Sensitive and Special Category Data](#), and enhanced privacy training mandated for colleagues handling this Sensitive and Special Category Data.

## 6.3 Contractual Protections

### 6.3.1 Intra-Group Data Transfer Agreement (IGDTA)

Entrust Corporation and its subsidiaries enter into the Intra-Group Data Transfer Agreement to ensure that where Personal Data is shared within the Entrust group, this is covered by appropriate data sharing clauses (including controller – processor clauses as required by GDPR). The IGDTA also ensures there are appropriate safeguards in place (i.e. standard contractual clauses) for when the sharing of Personal Data within the Entrust group involves the transfer of Personal Data from inside the EEA/UK to a country outside of the EEA/UK that does not benefit from an adequacy finding by the European Commission or Information Commissioner's Office.

### v) 6.3.2 Data Processing Agreement (DPA)

Companies outside of the Entrust group who process Personal Data for or on behalf of Entrust are required to enter into a Data Processing Agreement with Entrust to ensure the third party (e.g., vendor, supplier, channel partner) has appropriate technical and organizational measures in place to comply with relevant data protection laws. Entrust makes equivalent commitments to its customers where it acts as a Data Processor through a standard customer DPA.

### vi) 6.3.3 General Privacy Provisions

Contractual language around privacy is also built into standard agreements with customers, suppliers, and partners as well as in Entrust's standard Non-Disclosure Agreement (NDA).

## 7. Accuracy and Retention

### 7.1 Records Management

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

The global records management program ensures that a retention period is formally defined for Processing Personal Data to ensure it is kept only for as long as it is needed, and that Personal Data is erased, destroyed, or anonymized at the end of the assigned retention period. The [Global Records Management Policy](#) sets forth handling requirements for all records, not just those containing Personal Data, and the accompanying [Records Retention Schedule](#) defines the retention period for each type of record maintained by the Company.

### vii) 7.2 Storage and Backup of Personal Data

Entrust stores and backs up Personal Data across multiple server locations directly and indirectly managed by the Company. IT and relevant vendors (for non-IT managed, cloud-hosted applications) are provided with standard guidance around the proper handling of Personal Data on these servers, including with respect to storage and backups.

Entrust does not remove copies of Personal Data from its backup media and servers at the end of the retention period when doing so would be commercially impracticable; however, Personal Data retained by Entrust in this manner is protected by the same security standards protecting the Personal Data while in use and the Personal Data remains subject to confidentiality and may not be accessed except as required by applicable law.

### viii) 7.3 Erasure or Destruction of Personal Data

The [Global Records Management Policy](#) and [Information Classification Handling Standard](#) set forth the requirements for appropriately handling records of all types at the end of their prescribed retention period. In particular, the following principles apply with respect to records containing Personal Data:

- Personal Data should not be copied except as necessary to accomplish the specified purpose for Processing and any copies made should retain any original confidential or proprietary markings.
- Paper records must be shredded and disposed of securely when there is no longer a need to retain them and may not be disposed of in any other manner.
- Personal Data in electronic format should be deleted or anonymized once it is no longer needed.
- IT is responsible for destroying or erasing electronic equipment that contains Personal Data (e.g., laptops, desktops, company-owned mobile devices, and work data on Bring Your Own Device (BYOD) devices) in accordance with relevant Information Security policies and standards.

## 8. Confidentiality and Integrity

### 8.1 Information Security

Where the Company processes Personal Data, it takes appropriate measures to ensure the Personal Data remains secure and is protected against unauthorized or unlawful Processing, accidental loss, destruction, or damage. Entrust does this by:

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- Encrypting Personal Data at rest and in transit where required by law or contract and additionally as commercially practicable;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services used to process Personal Data through formalized business recovery and disaster recovery plans that are routinely tested or exercised;
- Ensuring the restoration of access to Personal Data in a timely manner in the event of a physical or technical incident;
- Periodically testing, assessing, and evaluating the effectiveness of technical and organizational measures in place to secure Personal Data;
- Enforcing physical security standards are in place requiring that desks and cupboards be kept locked if they hold Personal Data, individual monitors/screens not allow for Personal Data to be visible to passers-by and electronic devices (e.g., computers, tablets) are locked or logged off the Company's systems when left unattended.

In assessing appropriate security controls, Entrust considers the risks associated with the Processing, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data that is processed.

Where Entrust engages third parties to process Personal Data on its behalf, such parties do so based on written instructions from Entrust and subject to contractual provisions (e.g., DPA) to appropriately handle the Personal Data and implement appropriate technical and organizational measures that are at least equivalent to Entrust's own security requirements. Personal Data is not shared outside of Entrust without these mechanisms in place. Various security tools (e.g., DLP) are in place to ensure Personal Data does not leave the organization without authorization.

### ix) 8.2 Testing

Personal Data may not be used in any Entrust testing environments without a formal [security exception](#) approved in advance. All testing environments must adhere to the current standards and controls in place for production environments and all Personal Data approved for use in testing environments must be removed without delay once testing has been completed. Further details are outlined in the Secure-Software Development Life Cycle (S-SDLC).

### x) 8.3 Reporting a Personal Data Incident

A Personal Data incident can take many forms including, but not limited to:

- Loss of a mobile device or hard copy file containing Personal Data (e.g., accidentally leaving a device behind on public transportation);
- Theft of a mobile device or hard copy file containing Personal Data;
- Human error (e.g., a colleague accidentally sending an email containing Personal Data to an unintended recipient, or accidentally altering or deleting Personal Data);

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- Cyber-attack (e.g., opening an attachment to an email from an unknown third party that contains ransomware or other malware);
- Allowing unauthorized use/access (e.g., permitting an unauthorized third party to access secure areas of Entrust offices or systems);
- Physical destruction and loss (e.g., fire or flood); or
- Information is obtained from Entrust by a third party through deception (e.g., phishing or smishing attacks).

A Personal Data incident may have occurred if there is:

- Unusual log-in and/or excessive system activity with respect to active user accounts; • Unusual remote access activity;
- The presence of spoof wireless (Wi-Fi) networks visible or accessible from Entrust's working environment;
- Equipment failure; or
- Hardware or software key-loggers connected to or installed on Entrust systems.

Colleagues who become aware of or have any reason to suspect that a Personal Data incident may have occurred or is about to occur must immediately contact Entrust's Security Operations Center at [SOC@entrust.com](mailto:SOC@entrust.com).

### xi) 8.4 Personal Data Incident Response

In the event of an actual or imminent Personal Data incident, Entrust will implement its incident response and handling procedures maintained by Information Security to minimize the impact of the incident and notify regulators, data subjects and/or other parties as legally and/or contractually required. A response will typically involve the following:

- Investigating the incident to determine the nature, cause and extent of the damage or harm that has or may result;
- Implementing necessary steps to stop the incident from continuing or recurring, and limiting the harm to affected data subjects;
- Assessing whether there is an obligation to notify other parties (e.g., national data protection authorities, affected data subjects, contractual parties) and making those notifications in a timely manner; and
- Recording information about the Personal Data incident and steps taken in response, including documenting decisions to notify or not notify regulators or affected parties.

### i) 9. Transparency

Entrust provides transparency with respect to its global data privacy program through robust [internal](#) and [external](#) landing pages.

### i) 9.1 Privacy Notices

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

Entrust provides notice to data subjects about the Processing of their Personal Data in its role as both a data controller and data processor. This information is available through Entrust's various privacy notices for web users, job applicants and colleagues as well as through its individual product privacy notices available [here](#). Such notices provide information about:

- The types of Personal Data Entrust processes;
- The purpose and legal basis for the Processing;
- Third parties used for Processing, if applicable;
- Location and duration of Processing;
- Any cross-border transfers of Personal Data;
- Duration of Processing;
- Data subject rights; and
- Details of any artificial intelligence/automated decision-making processes

### ii) 9.2 Training

Entrust provides colleagues with mandatory, annual training about data protection responsibilities. The Introduction to Data Privacy Training occurs at onboarding and annually thereafter. In addition to the all-colleague Introduction to Data Privacy Training, Entrust mandates annual completion of the Enhanced Data Privacy Training by colleagues who handle sensitive and special category data as well as the Privacy by Design Training by colleagues who play a role in the development and design of software product and service offerings. Entrust continues to develop and deploy additional function-specific privacy trainings as needed.

### iii) 9.3 Data Subject Rights

Where Entrust processes Personal Data, data subjects have certain rights under data protection laws. Although these rights vary by jurisdiction, data subjects generally have the right to:

- Request information about the Personal Data held with respect to them;
- Have any inaccurate Personal Data about them corrected and incomplete Personal Data completed;
- Object to Entrust's Processing their Personal Data where the Company is doing so in pursuit of its own legitimate interests. Entrust can continue Processing the Personal Data notwithstanding an objection if the Company's legitimate interests outweigh those of the data subject, or if Entrust needs to do so for legal reasons;
- Ask Entrust to destroy Personal Data held with respect to the data subject. The Company can refuse this request if the Personal Data is still necessary for the purposes for which it is being processed and there is a legal basis for Entrust to continue Processing;
- Ask Entrust to restrict the Processing of their Personal Data to storage under certain circumstances.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

Entrust will assess a data subject's rights under data protection laws on a case-by-case basis and follow the [Data Subject Request Procedure](#) in determining how to fulfill a request. In general,

Entrust will use a data subject's rights under the EU GDPR as a baseline for fulfilling all requests and apply additional rights available under data protection laws applicable to the data subject to the extent those are more favorable to the data subject. If a data subject exercises these rights and Entrust has disclosed the Personal Data in question to a third party, the Company will do its best to ensure that the third party also complies with the wishes of the data subject.

Data subjects who wish to request information about the Personal Data Entrust holds about them should do so through submission of a formal [Data Subject Request \(DSR\)](#). If colleagues receive a request directly (whether verbally or in writing), the request should immediately be forwarded to [privacy@entrust.com](mailto:privacy@entrust.com).

### iv) 9.4 Supervisory Authorities

Contact information for relevant data supervisory authorities varies by location. The list of European Data Protection Board authorities can be found [here](#). The United Kingdom (UK) Information Commissioner's Office (ICO) can be found [here](#). The Office of the Privacy Commissioner of Canada can be found [here](#).

### v) 9.5 Data Protection Officer

Unless otherwise indicated, Entrust's Data Protection Officer is:

Jenny Carmichael

VP, Compliance

1187 Park Place

Shakopee, MN

55379

[privacy@entrust.com](mailto:privacy@entrust.com)

Entrust Deutschland GmbH's assigned Data Protection Officer is Mr. Niels Kill of Althammer & Kill GmbH & Co. KG ([kontakt-dsb@althammer-kill.de](mailto:kontakt-dsb@althammer-kill.de)).

Onfido's assigned Data Protection Officer is Dyann Heward-Mills at Heward Mills ([dyann@hewardmills.com](mailto:dyann@hewardmills.com)).

### j) 10. Compliance

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

All colleagues and contingent workers are expected to comply with this policy. Additionally, all business units must ensure they have appropriate local standards and procedures in place to comply with this policy and applicable data privacy legislation in their jurisdiction. Breaches of this policy will be taken seriously and may result in disciplinary action, up to and including termination. This policy may be updated or amended at any time.

## 11. Exceptions

There are no exceptions to this policy.

### k) 12. Ownership and Review

This policy is owned by the Chief Legal and Compliance Officer and shall be reviewed on an annual basis.

### i) 12.1 Contact Information

Questions about this policy or Entrust's handling of Personal Data can be directed to [privacy@entrust.com](mailto:privacy@entrust.com).



global-personal-data  
-protection-policy.pdf

Version: 2 April 2025



## **THALES CYBER SECURITY PRODUCTS END USER AGREEMENT**

### **PART 1: GENERAL TERMS AND CONDITIONS**

#### **1. ORDERS.**

##### **1.1 Ordering process.**

- 1.1.1 Products and Services shall be procured by End User pursuant to an Order, either directly from Thales or through an Authorized Third Party.
- 1.1.2 Except as may be set out in the Product Specific Terms, each Order shall correspond to a Quote and shall set out the relevant SKUs and Licensed Volume, where each SKU represents a separate contractual entitlement to a Product or Service.
- 1.1.3 Thales shall be free to accept or reject an Order in its absolute discretion, without liability of any kind. An Order shall only become legally binding on Thales when it has been accepted in writing by Thales.
- 1.1.4 Each Order, together with the corresponding Quote, shall form a part of, be incorporated by reference into, and be subject to, this Agreement. To the extent there is any inconsistency between this Agreement and a provision in an Order, this Agreement shall prevail, except where the relevant provision(s) explicitly and expressly refers to and states that such provision(s) of the Order shall override the conflicting provision(s) of this Agreement and the Order has been signed by a duly authorized representative of Thales and End User.
- 1.1.5 All Orders are non-cancellable and non-refundable. Any amendment, cancellation or other change to an Order is only binding on Thales if signed by an authorized representative of Thales. End User acknowledges that administrative fees may apply to any such change, such as restocking fees.
- 1.1.6 Thales may in its sole discretion agree in writing to be bound by Quote-specific terms and conditions. Any Quotespecific terms which purport to amend this Agreement must be signed by an authorized representative of Thales.
- 1.1.7 Thales shall retain a purchase money security interest in all Appliances or Hardware delivered hereunder until all associated invoices therefor are paid in full. End User shall execute any documentation reasonably requested to enforce such security interest.
- 1.1.8 End User acknowledges that Products may be subject to a stop-ship restriction. Thales will provide reasonable notice to End User of such restriction; however, Thales does not guarantee the resolution of the restriction, nor that the Order will be fulfilled. Any Order for Products subject to a restriction will be fulfilled subject to availability in spite of the day and time of the Order. Any dates

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

provided by Thales in connection with the restriction or shipment status are subject to change at any time by Thales. In no event will Thales be liable for any damages whatsoever related to Product availability, shortages or shipment delays in connection with the fulfilment of the Order.

### 1.2 Direct Orders.

For Orders issued to Thales directly by End User ("**Direct Orders**"), End User shall pay the applicable fees directly to Thales in accordance with Section 2 of Part 1 of this Agreement.

### 1.3 Ordering via an Authorized Third Party.

- 1.3.1 For Orders issued to Thales through an Authorized Third Party, End User shall pay the Authorized Third Party the applicable fees in accordance with the terms agreed between End User and the Authorized Third Party (and not in accordance with Section 2 of Part 1 of this Agreement).
- 1.3.2 The terms governing the use of Product and Services ordered through an Authorized Third Party shall be those set out in this Agreement.
- 1.3.3 Authorized Third Parties are not permitted to bind Thales to any terms other than those expressly set out in this Agreement. Any term, representation, warranty or other statement communicated to End User by an Authorized Third Party as part of the procurement of the Products or Services, and that is not expressly set out in this Agreement, shall not be binding upon Thales.
- 1.3.4 In the event of a conflict between this Agreement and the terms agreed between End User and the Authorized Third Party, as between Thales and the End User, this Agreement shall take precedence.
- 1.3.5 Should a service credit, refund or other payment become due to End User pursuant to this Agreement in respect of an Order issued through an Authorized Third Party, End User acknowledges and agrees that unless the Authorized Third Party agrees otherwise:
  - (a) such service credit, refund or other payment shall be provided by Thales to the relevant Authorized Third Party; and
  - (b) End User may only obtain such service credit, refund or other payment from that Authorized Third Party.
- 1.3.6 Should an End User fail to pay any amount to an Authorized Third Party in respect of an Order, End User agrees that Thales may suspend or terminate an Order.

### 1.4 Exceeding the Licensed Volume.

If End User exceeds the Licensed Volume set out in the Order for any applicable SKU, End User shall pay Thales, or the relevant Authorized Third Party if applicable, the additional fees set out in this Agreement, the Order, or the Documentation. In the absence of a documented

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

rule specifying a rate for additional fees, the End User shall pay any additional fees at Thales' then-current rate.

## **2 PAYMENTS TO THALES.**

### **2.1 Payment terms.**

- 2.1.1 Any fees payable to Thales under this Agreement are non-refundable.
- 2.1.2 All fees shall be payable in the currency specified in the Quote.
- 2.1.3 All payments from End User to Thales shall be payable by End User net thirty (30) days after the date of invoice.
- 2.1.4 If End User is thirty (30) days or more overdue on any payment owed to Thales pursuant to this Agreement, in addition to any of its other rights or remedies, Thales reserves the right to charge a late fee on any overdue amounts at a rate equal to 1.5% per year or the highest rate permitted by applicable law or regulation, whichever is lower. End User shall reimburse Thales for all reasonable costs and expenses incurred (including reasonable attorneys' fees) in collecting overdue amounts pursuant to this Agreement.
- 2.1.5 Upon termination or expiry of End User's rights with respect to a particular Product or Service pursuant to this Agreement, any amounts owed to Thales under the Agreement prior to such termination or expiry will be immediately due and payable.

### **2.2 Taxes.**

- 2.2.1 End User shall pay all sales, use, value-added and other taxes, tariffs and duties of any type and any other governmental charges assessed against End User. Fees are exclusive of all taxes and do not include freight, insurance costs or shipping handling fees.
- 2.2.2 Should End User be required under any law or regulation of any governmental entity or authority to withhold or deduct any portion of the payments due to Thales, then End User shall increase the sum payable to Thales by the amount necessary to yield to Thales an amount equal to the sum it would have received had no withholdings or deductions been made.

### **2.3 Invoicing.**

Thales may invoice all fees for Products and Services in full upon Thales' acceptance of an Order, unless the applicable Quote states otherwise. Fees where the Licensed Volume has been exceeded shall be invoiced in accordance with Thales' then-current policy.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **2.4 No set-off.**

Neither party shall have any right to set off, discount or otherwise reduce or refuse to pay any amounts due to the other party under this Agreement for any reason.

## **3 TERM; TERMINATION.**

### **3.1 Term.**

3.1.1 The term of each Order shall commence on the date the Order is accepted by Thales and shall continue in effect for such time as End User continues to have the right to use the Products and / or receive the Services.

3.1.2 The term of this Agreement shall commence upon the Effective Date and shall continue in effect until this Agreement is terminated in accordance with its terms.

### **3.2 Termination.**

3.2.1 Either party shall be entitled to terminate this Agreement at any time upon notice in writing to the other if the other party:

- (a) commits a material breach of this Agreement which is not capable of remedy;
- (b) commits a material breach of this Agreement that is capable of remedy but which remains un-remedied for more than thirty (30) days after such notice; or
- (c) makes an arrangement with or enters into a compromise with its creditors, becomes the subject of a voluntary arrangement, receivership, administration, liquidation or winding up, is unable to pay its debts or otherwise becomes insolvent or suffers or is the subject of any distraint, execution, event of insolvency or event of bankruptcy or any other similar process or event.

### **3.3 Consequences of termination.**

3.3.1 Upon termination or expiration of this Agreement: (a) Thales shall cease to provide the Products and Services, (b) the rights and licenses granted to End User under this Agreement shall terminate, (c) End User shall, within thirty (30) days, ship to Thales, or, where intangible, destroy (including purging from any system or storage media), all items in its possession which are proprietary to Thales, and (d) each party shall promptly return or destroy the other party's Confidential Information in accordance with the provisions of Section 4.2.3 of Part 1 of this Agreement.

3.3.2 Unless expressly stated in this Agreement or agreed to in writing by the parties, termination of any Order shall not affect any other Order. Upon termination of this Agreement, however, all Orders shall automatically terminate.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 3.3.3 Upon termination or expiration of End User's rights with respect to a particular Product or Service pursuant to this Agreement, Thales shall cease to provide such Product or Service, and the applicable rights and licenses granted

to End User with respect to such Product or Service under this Agreement shall automatically and immediately terminate.

- 3.3.4 Termination shall not relieve End User of the obligation to pay any fees accrued or payable to Thales or an Authorized Third Party prior to the effective date of expiration or termination.

- 3.3.5 The following sections shall survive any termination or expiration of this Agreement: Sections 2, 3.3, 4, 5 (for one year after termination of the Agreement), 6, 7, 8, 9 and 10 of this Part 1; Section 1.2, of Sub-part 2.1; Sections 1.2 and 2 of Sub-part 2.2; Section 2.4 of Sub-part 2.3; Sections 3.2 and 5 of Sub-part 2.4; Sections 2.1 and 5 of Subpart 3.1, Sections 1.2 and 5.2.2 of Sub-part 3.2, Sections 4.2 and 6 of Sub-part 3.3; Section 2.1 and 5 of Sub-part 4.1; Sections 1.2 and [4]of Sub-part 4.2; Sections 3.2 and 5 of Sub-part 4.3.

### **3.4 Temporary suspension and delay.**

- 3.4.1 Thales has the right, without liability to End User, to suspend in whole or in part End User's rights to access or use any Products or Services immediately upon notice if:

- (a) End User is in breach of its payment obligations to Thales, or to an Authorized Third Party, in respect of any Order until any overdue amounts are paid in full; or
- (b) End User makes an arrangement with or enters into a compromise with its creditors, becomes the subject of a voluntary arrangement, receivership, administration, liquidation or winding up, is unable to pay its debts or otherwise becomes insolvent or suffers or is the subject of any distraint, execution, event of insolvency or event of bankruptcy or any other similar process or event.

- 3.4.2 If Thales suspends access or use pursuant to Section 3.4.1 of Part 1 of this Agreement, End User shall:

- (a) remain responsible for all fees (to Thales and/or an Authorized Third Party) during the period of suspension; and
- (b) not be entitled to any service credits for any period of suspension.

- 3.4.3 Without liability to End User or any other person and without prejudice to any other remedy, Thales may withhold or delay Delivery of any Order if End User is late in performing any payment obligation pursuant to this Agreement or is otherwise in default under this Agreement.

## **4 CONFIDENTIALITY.**

### **4.1 Confidential Information.**

4.1.1 As used in this Agreement, “**Confidential Information**” means all confidential and proprietary information of a party (“**Disclosing Party**”) disclosed to the other party (“**Receiving Party**”), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure.

4.1.2 Thales’ Confidential Information includes, without limitation, the Products and Services, their performance (including any benchmarking information), any compliance certifications or attestation reports in respect of the Products and Services and Thales’ pricing of the Products and Services. The source code of any Software is a confidential trade secret of Thales.

4.1.3 Confidential Information shall not include any information that:

- (a) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party;
- (b) was rightfully known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party (as can be demonstrated by reasonable supporting evidence);
- (c) was independently developed by the Receiving Party without access of or reference to the Disclosing Party’s Confidential Information or any breach of any obligation owed to the Disclosing Party (as can be demonstrated by reasonable supporting evidence); or
- (d) is received from a third party which is not under an obligation of confidence or non-use with respect to such information and without breach of any obligation owed to the Disclosing Party (as can be demonstrated by reasonable supporting evidence).

### **4.2 Treatment of Confidential Information.**

4.2.1 The Receiving Party agrees that it shall:

- (a) use Confidential Information for the sole purpose of exercising or enforcing its rights and performing its obligations under this Agreement;
- (b) divulge and allow access to Confidential Information only to those of its employees, directors, independent consultants or agents who have a need to know such Confidential Information and who are bound by professional duty or in writing (in advance) to confidentiality and non-use obligations at least as protective of such information as this Agreement;

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- (c) not disclose any Confidential Information to any third party except as described in Section 4.2.1(b) of Part 1 of this Agreement; and
- (d) use at least the same degree of care in protecting the Disclosing Party's Confidential Information as the Receiving Party uses to preserve and safeguard its own valuable proprietary information, but in any event, no less than a reasonable standard of care.

4.2.2 The Receiving Party shall notify and cooperate with the Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information of the Disclosing Party. The Receiving Party may disclose Confidential Information to comply with an order from a court of competent jurisdiction or with a mandatory requirement of a governing regulatory body, provided such party, to the extent permitted by law and as soon as reasonably practicable under the circumstances, informs the Disclosing Party and allows the Disclosing Party the opportunity to object to the disclosure order or to take action to preserve the confidentiality of the information. The Receiving Party shall cooperate with the Disclosing Party in such party's reasonable efforts to limit the disclosure of the information.

4.2.3 Upon termination of this Agreement, the Receiving Party shall:

- (a) immediately cease all use of the Disclosing Party's Confidential Information; and
- (b) if requested by the Disclosing Party, either promptly destroy (and permanently erase all Confidential Information from its computer systems) or return all Confidential Information of the Disclosing Party; and
- (c) provided, that the Receiving Party may retain a reasonable number of copies of the Confidential Information (and any materials embedding the same) for the sole purposes of satisfying legal or regulatory requirements regarding record and data retention that the Receiving Party is obligated to comply with, enforcing this Agreement and/or archiving consistent with good business practices. Retained copies of Confidential Information remain subject to the confidentiality and restricted use provisions of this Agreement.

4.2.4 If the Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the Disclosing Party in breach of this Section 4, the Disclosing Party may have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts.

## **5 AUDIT.**

### **5.1 Thales right to audit.**

5.1.1 Thales shall have the right during the term of this Agreement, and for one year thereafter, to audit and/or inspect End User's systems and records to:

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- (a) verify End User's use of the Products and Services; and/or
- (b) otherwise validate compliance with this Agreement.

5.1.2 Audits shall be carried out on reasonable notice by Thales and/or its selected external auditor. End User shall provide Thales and/or its selected external auditor with access to its relevant systems and records. Thales shall pay the expenses of the audit, unless such audit reveals an underpayment of five percent (5%) or more or any other material breach of this Agreement, in which case End User shall promptly pay Thales the reasonable fees and expenses incurred by Thales for such audit. End User shall promptly pay Thales or an Authorized Third Party, as applicable, the amount of any underpayment (and correct any other non-compliance) revealed by such audit.

### 5.1.3 Audits of Thales.

Thales will audit the security of the computers and computing environment that it uses to provide the relevant Products and Services. Where Thales is auditing to a standard or framework which provides for audits, an audit will be performed at least annually. Each audit will be performed according to the requirements of the regulatory or accreditation body governing the control standard or framework and will be performed by qualified, independent, third party auditors selected by Thales at Thales' expense. End User shall be entitled to request a copy of the audit reports products by such third party auditors. Thales may redact certain parts of an audit report at its discretion. All information provided or otherwise accessed pursuant to an audit or an audit report shall be deemed Confidential Information. Where a customer is subject to jurisdiction of a governmental regulator, and it is a requirement pursuant to the governing law of this Agreement that Thales cooperates with the requests of such governmental regulator directly, at End User's cost, Thales shall cooperate with the requests of such governmental regulator.

## 6 DISCLAIMER OF WARRANTIES.

**EXCEPT AS EXPRESSLY SET OUT IN THIS AGREEMENT, THE PRODUCTS AND SERVICES ARE PROVIDED AND/OR LICENSED "AS-IS" AND THALES MAKES NO ADDITIONAL WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. THALES MAKES NO WARRANTY THAT USE OF THE PRODUCTS OR SERVICES SHALL BE UNINTERRUPTED, ERROR-FREE OR DEFECTFREE, OR AVAILABLE AT ALL TIMES. THALES SPECIFICALLY DISCLAIMS, ON BEHALF OF ITSELF AND ITS PARTNERS AND SUPPLIERS, ALL IMPLIED WARRANTIES AND CONDITIONS, INCLUDING ANY WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.**

## **7 LIMITATION OF LIABILITY.**

- 7.1 **SUBJECT TO SECTION 7.6, IN NO EVENT SHALL THALES' (AND ITS AUTHORIZED THIRD PARTIES' OR SUPPLIERS') TOTAL AND AGGREGATE LIABILITY ARISING FROM ALL CLAIMS UNDER OR RELATED TO THIS AGREEMENT (INCLUDING ALL PRODUCTS AND SERVICES HEREUNDER) EXCEED THE TOTAL AMOUNTS PAID BY END USER TO THALES OR AUTHORIZED THIRD PARTY (IF APPLICABLE) FOR THE PRODUCTS OR SERVICES IN RESPECT OF THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO THE APPLICABLE CLAIM, LESS ALL AMOUNTS PAID BY THALES TO CUSTOMER FOR ALL PAST CLAIMS OF ANY KIND ARISING UNDER THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THALES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**
- 7.2 **SUBJECT TO SECTION 7.6, IN NO EVENT SHALL THALES (OR ITS AUTHORIZED THIRD PARTIES' OR SUPPLIERS') HAVE ANY LIABILITY IN CONNECTION WITH THE PRODUCTS, SERVICES OR THIS AGREEMENT FOR ANY LOST PROFITS OR REVENUES, LOSS OF DATA OR USE OF THE PRODUCT(S) OR SERVICE(S), GOODWILL, REPUTATION, INTERRUPTION OF THE SERVICES, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**
- 7.3 **END USER ACKNOWLEDGES AND AGREES THAT THALES HAS OFFERED THE PRODUCTS AND SERVICES, AND SET PRICES IN RELIANCE UPON THE WARRANTY DISCLAIMERS AND THE LIMITATIONS OF LIABILITY SET OUT IN THIS AGREEMENT, THAT THE WARRANTY DISCLAIMERS AND THE LIMITATIONS OF LIABILITY SET OUT IN THIS AGREEMENT REFLECT A REASONABLE AND FAIR ALLOCATION OF RISK, AND THAT THE WARRANTY DISCLAIMERS AND THE LIMITATIONS OF LIABILITY SET OUT IN THIS AGREEMENT FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN END USER AND THALES. THALES WOULD NOT BE ABLE TO PROVIDE THE PRODUCTS OR SERVICES ON AN ECONOMICALLY REASONABLE BASIS WITHOUT THESE LIMITATIONS.**
- 7.4 **SUBJECT TO SECTION 7.6, EXCEPT FOR: (I) END USER'S BREACH OF ITS PAYMENT OBLIGATIONS TO THALES OR ANY AUTHORIZED THIRD PARTIES, AND/OR (II) END USER'S BREACH OF SECTION 8.2 (LICENSES AND USE RESTRICTIONS) OR SECTION 10.1 (EXPORT), IN NO EVENT SHALL END USER'S TOTAL AND AGGREGATE LIABILITY ARISING FROM ALL CLAIMS UNDER OR RELATED TO THIS AGREEMENT (INCLUDING ALL PRODUCTS AND SERVICES HEREUNDER) EXCEED THE TOTAL**

AMOUNTS PAID BY END USER TO THALES FOR THE PRODUCTS OR SERVICES IN RESPECT OF THE **TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO THE APPLICABLE CLAIM, LESS ALL AMOUNTS PAID BY THALES TO CUSTOMER FOR ALL PAST CLAIMS OF ANY KIND ARISING UNDER THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

**7.5 SUBJECT TO SECTION 7.6, EXCEPT FOR: (I) END USER'S BREACH OF ITS PAYMENT OBLIGATIONS TO THALES OR ANY AUTHORIZED THIRD PARTIES, AND/OR (II) END USER'S BREACH OF SECTION 8.2 (LICENSES AND USE RESTRICTIONS) OR SECTION 10.1 (EXPORT), IN NO EVENT SHALL END USER HAVE ANY LIABILITY IN CONNECTION WITH THIS AGREEMENT TO THALES FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

**7.6 NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS EITHER PARTY'S LIABILITY:**

**7.6.1 FOR FRAUD OR FRAUDULENT MISREPRESENTATION;**

**7.6.2 FOR DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE OR THAT OF ITS EMPLOYEES OR AGENTS OR SUBCONTRACTORS; OR**

**7.6.3 TO THE EXTENT SUCH LIABILITY CANNOT BE EXCLUDED OR LIMITED BY LAW.**

## **8 PROPRIETARY RIGHTS.**

### **8.1 Reservation of Rights.**

Subject to the limited rights expressly granted to End User under this Agreement, Thales reserves and, as between the parties, shall solely own all rights, title and interest in and to the Products (excluding any Appliances or Hardware sold to End User pursuant to the terms of this Agreement) and Services, including all improvements, modifications or enhancements to, or derivative works of, the foregoing (regardless of inventorship or authorship), and all Intellectual Property Rights in and to any of the foregoing, and to the extent any such rights vest in End User, End User shall automatically and irrevocably assign such rights to Thales. No rights are granted to End User hereunder (whether by implication, estoppel, exhaustion or otherwise) other than as expressly set out in this Agreement.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

### 8.2 License and use restrictions.

End User may not (and may not permit any third party to) directly or indirectly:

- (a) modify, adapt, incorporate or use in any other works, translate, reverse engineer (except to the limited extent applicable statutory law expressly prohibits reverse engineering restrictions), decompile, disassemble, or otherwise attempt to derive source code from or create derivative works based on the Products or Services;
- (b) make unauthorized copies of the Products or Services;
- (c) disclose, distribute, transfer or market the Products or any material associated with the Product or Services to third parties;
- (d) remove or modify any proprietary notices, labels, or marks on or in any copy of the Products or any material associated with the Product or Services;
- (e) distribute, sell, sublicense, rent, lease or use the Products or Services (or any portion) for time sharing, hosting, service provider or other computer services to third parties or otherwise make the functionality of the Products or Services available to third parties;
- (f) publicly disseminate reports generated by the Products / Services or Product / Service performance information or analysis (including, without limitation, benchmarks and performance tests) from any source relating to the Products;
- (g) access the database or any other third party product that is embedded in the Products with applications (including spiders, robots, crawlers or any other similar data mining tools) other than the Products;
- (h) use the Products / Services or reports generated by the Products / Services in End User's products or services or in its marketing of products or services to third parties;
- (i) use the Product / Services or reports generated by the Products / Services to develop, commercialize, license or sell any product, service or technology that could, directly or indirectly, compete with the Products / Services;
- (j) use the Products / Services to store, transmit, upload or post any infringing or otherwise unlawful or tortious material or any data for which it does not have the necessary consents or rights to store, transmit, upload or post (as applicable) in connection with the Products;
- (k) use the Products / Services in a way that does not comply with applicable law; or
- (l) use the Products / Services other than as expressly authorized in this Agreement.

### 8.3 Feedback.

From time to time End User may provide Thales with suggestions, feature requests, comments and feedback with regard to the Products and Services (collectively, "**Feedback**"). End User grants Thales a perpetual, irrevocable, royalty-free and fully-paid up license to use and exploit

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

all Feedback in connection with Thales' business purposes, including, without limitation, the testing, development, maintenance and improvement of Thales' Products and Services.

## 9 INDEMNIFICATION

9.1 Subject to Sections 9.2 to 9.4 (inclusive) of Part 1 of this Agreement, Thales shall defend End User against any third party claim that the Products as provided infringe any patent, or any copyright, or misappropriates any third party trade secrets ("**Infringement Claim**") and indemnify End User from the resulting costs and damages finally awarded against End User to the third party making such Infringement Claim, by a court of competent jurisdiction or agreed to in a settlement; provided that End User:

- (a) promptly notifies Thales of any and all threats, claims and proceedings involving such Infringement Claim;
- (b) gives reasonable assistance in response to Thales' request for assistance; and
- (c) grants Thales sole control over defense and settlement of the Infringement Claim.

9.2 Section 9.1 of Part 1 of this Agreement shall not apply to any Infringement Claim or associated costs or damages arising out of or in connection with the Products or portions or components:

- (a) that are modified by any party other than Thales or its authorized agents;
- (b) that are combined with other products, services, processes, software, content, data or materials, where the alleged infringement relates to such combination or such other products, services, processes, software, content, data or materials;
- (c) where modifications that would have avoided the alleged infringement have been made available to End User, and End User continues the allegedly infringing activity after being notified of it by Thales; or
- (d) where End User's use of such Products is not strictly in accordance with this Agreement.

9.3 In the event that a Product is held to or believed by Thales to infringe or misappropriate any Intellectual Property Rights of a third party, Thales at its discretion, shall have the option to:

- (a) modify the allegedly infringing Product to be non-infringing;
- (b) obtain for End User a license to continue using the Product; or
- (c) request the return of or terminate access to the infringing Product (as the case may be) and upon such return or termination, refund to End User (or have the applicable Authorized Third Party refund) the amount of fees paid for such infringing Product for any unused, prepaid portion of the term remaining as of the effective date of termination.

9.4 **THIS SECTION 9 SETS OUT THALES' SOLE OBLIGATION AND END USER'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF AN INFRINGEMENT CLAIM AND RELATED VIOLATIONS OF THIRD PARTY RIGHTS.**

10 **GENERAL.**

10.1 **Export.**

10.1.1 In connection with its actions under or related to the Agreement, End User shall comply with all applicable export controls and economic sanctions (the "**Export Laws**"), including, as applicable, the Export Administration Regulations maintained by the U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, export controls and restrictive measures maintained by the UK Government and EU.

10.1.2 End User acknowledges that the Products and Services contain encryption technology that is subject to export restrictions by the U.S. government and import restrictions by certain other governments. End User shall not directly or indirectly and shall not allow any third-party to remove or export, or allow the export or re-export of, any part of the Products or Services or any direct product of the Products and Services:

- (a) into (or to a national or resident of) any territory to the extent the U.S. government or any agency of it restricts export or re-export to such countries;
- (b) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals;
- (c) to any country to which such export or re-export is restricted or prohibited, or as to which the U.S. government or any agency of it requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval;
- (d) to the extent the Products or Services fall under the scope of Article 12g of Council Regulation (EU) No 833/2014 or No 756/2006 (i) to the Russian Federation, Belarus or for use in the Russian Federation, Belarus or in the Ukrainian territories controlled by the Russian Federation, or (ii) to any individual or entity subject to E.U. sanctions or restrictive measures, as well as to any entity owned, controlled or acting for individuals or entities subject to EU sanctions or restrictive measures; or
- (e) otherwise in violation of any export or import restrictions, laws or regulations of any U.S. or other government agency or authority.

10.1.3 End User shall immediately notify Thales of any violation of Section 10.1.2 of Part 1 of this Agreement.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 10.1.4 End User agrees to the foregoing and warrants that it is not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list. The Products and Services are restricted from being used for the design or development of nuclear, chemical, or biological weapons or missile technology without the prior permission of the U.S. government.
- 10.1.5 End User shall obtain and bear all expenses relating to any necessary licenses and/or exemptions with respect to the export of all Thales products from the U.S., from any EU member state or from any other applicable country where End User is located to any location and shall demonstrate to Thales compliance with all applicable laws and regulations prior to delivery thereof by Thales.
- 10.1.6 End User shall not to engage in any activity related to this Agreement that would cause the other Thales to violate France, E.U., U.S. or relevant foreign sanctions programs.
- 10.1.7 End User represents that it will not offer employment, continue to employ, engage or contract with an individual or entity who is included on applicable French, E.U., U.S. or foreign sanctions lists, including those maintained by OFAC of specially designated nationals and blocked persons subject to financial sanctions. End User shall inform Thales immediately in the event that any representatives (i.e. employees, officers, representatives and advisers) appear on any sanctions list, and will immediately remove such representatives from performing work with Thales products or applications.
- 10.1.8 End User agrees to indemnify and hold Thales, its partners and suppliers harmless against any claims, losses or expenses arising out of End User's breach of this Section 10.1.
- 10.1.9 Any breach of this Section 10.1 shall be deemed a material breach which is not capable of remedy.

### 10.2 Anti-corruption

End User shall comply with any and all applicable anti-corruption and influence-peddling laws and regulations, including but not limited to the U.S. Foreign Corrupt Practices Act, the UK Bribery Act 2010 and French law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and the modernisation of the economy (the "**Sapin II Law**"). Without limiting the foregoing, End User shall not, directly or indirectly, make, promise to make, or accept any payment, promise, donation, gift, offer or transfer of anything of value in connection with this Agreement to: (i) anyone working in an official capacity for a government, government entity (including employees of government owned or controlled corporations) or public international organization; (ii) any political party, party official, or candidate for political office; (iii) an intermediary for payment to any of the foregoing; (iv) any officer, director, employee of any actual or potential customer of End User; (v) any officer, director or employee of Thales or any

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

of its affiliates; or (vi) any other person or entity if such payment, offer or transfer would violate the laws of the country in which made or which would be linked to a misuse that would be made by that person, or that has already been made by that person, of his/her real or supposed influence with a view to obtaining, for itself or for others, a distinction, a job, a contract or any other favourable decision. It is the intent of the parties that no payments, offers or transfers of value shall be made which have the purpose or effect of public or commercial bribery, acceptance or acquiescence in extortion, kickbacks or other unlawful or improper means of obtaining or retaining business or directing business to any person or entity. Neither party shall solicit or accept for itself any offer, promise, donation, gift or benefit of any kind, for the purpose of misusing its influence with a view to making or obtaining any favourable decision. Each of the Parties declares that it has implemented a compliance program that meets the requirements of the Sapin II Law, insofar as it is subject to it.

### **10.3 Force Majeure.**

Neither party shall be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a party's payment obligations) if the delay or failure is due to events which are beyond the reasonable control of the parties, including, but not limited to strikes, pandemics, epidemics, public health emergencies, blockade, government-imposed travel restrictions and quarantines, war, terrorism, riots, natural disasters, refusal of license by the government or other governmental agencies, communications failure, and internet and power outages or disruptions.

### **10.4 Governing Law; Jurisdiction.**

10.4.1 If End User's address on the first page of this Agreement is in the United States, Canada or elsewhere in the Americas, this Agreement will be governed by and construed in accordance with the internal laws of the State of Delaware, without giving effect to its conflict of laws principles. Any litigation relating to the formation, interpretation or alleged breach of this Agreement must be brought exclusively in the state and federal courts having jurisdiction in the city of Wilmington, Delaware, and End User irrevocably consents to the jurisdiction of and venue in such courts.

10.4.2 If End User's address on the first page of this Agreement is outside of the Americas, this Agreement will be governed by and construed in accordance with the laws of England and Wales, without giving effect to conflict of laws principles that would result in a different law being applicable. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

**10.4.3 EACH PARTY IRREVOCABLY AND UNCONDITIONALLY WAIVES ANY RIGHT IT MAY HAVE TO A TRIAL BY JURY IN RESPECT OF ANY LEGAL ACTION ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.**

10.4.4 The parties agree that in all cases the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer Information Transactions Act are specifically excluded from application to this Agreement.

**10.5 End User Mention.**

End User consents to Thales using its name and logo to identify End User as a customer of Thales, including use on Thales' website and other marketing materials. Any use shall be subject to Thales complying with any guidelines that End User may deliver to Thales from time to time regarding the use of its name and logo. This consent terminates upon termination of this Agreement.

**10.6 Independent contractors.**

The parties are independent contractors under this Agreement and nothing in this Agreement authorizes a party to act as an agent of the other or bind the other to any transaction or agreement.

**10.7 Assignment.**

This Agreement shall bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign or transfer this Agreement in whole or in part by operation of law or otherwise, without the other party's prior written consent (such consent not to be unreasonably withheld or delayed). Any attempt to transfer or assign this Agreement without such written consent shall be null and void. Notwithstanding the foregoing, however, Thales may assign this Agreement without consent to a Group Company or to the acquiring or surviving entity in a merger or acquisition in which Thales (or a subsidiary, division or group of Thales) is the acquired entity (whether by merger, reorganization, acquisition or sale of stock), or to the purchaser in connection with the sale of all or a portion of Thales' assets, without written consent. Additionally, End User grants Thales a general written authorisation to engage subcontractors.

**10.8 Third party rights.**

The parties agree that there shall be no third party beneficiaries to this Agreement, except to the extent set out in the Third Party Terms that an entity is an intended third party beneficiary of this Agreement (which may be amended without the consent of such beneficiaries).

**10.9 Waiver and remedies.**

10.9.1 Except as specifically provided in this Agreement, the exercise by either party of any rights and remedies under this Agreement (including any right to terminate this Agreement) shall be without prejudice to its other remedies under this Agreement or otherwise.

10.9.2 A waiver of any breach under this Agreement shall not constitute a waiver of any other breach or future breaches.

10.9.3 Except as otherwise set out in this Agreement:

- (a) no failure to exercise, or delay in exercising, any rights, remedy, power or privilege arising from this Agreement shall operate or be construed as a waiver; and
- (b) no single or partial exercise of any right, remedy, power, or privilege pursuant to this Agreement shall preclude any other or further exercise of it or the exercise of any other right, remedy, power, or privilege.

**10.10 Amendments.**

This Agreement may be modified or waived only in a written instrument signed by duly authorized representatives of both parties.

**10.11 Counterparts.**

This Agreement may be executed in counterparts, including by transmission in.pdf or other means of electronic transmission, each of which shall constitute an original and together shall constitute one instrument.

**10.12 Notices.**

10.12.1 All notices, requests, legal proceedings, demands and other communications pursuant to this Agreement shall:

- (a) if issued to Thales: be in writing by major commercial delivery service, delivery verified, to the Thales DIS CPL, Inc. headquarters address;
- (b) if issued to End User: be in writing, (i) by email to the most recent address on Thales' files; or (ii) by major commercial delivery service, delivery verified, to the most recent address on Thales' files; and

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- (c) with respect to either party, be deemed given twenty four (24) hours after it is sent: (i) by a major commercial delivery service, delivery verified; or (ii) to the most recent email address in Thales' files.

10.12.2 Either party may, by like notice, specify or change an address to which notices and communications shall from then on be sent.

### **10.13 Entire Agreement.**

10.13.1 Along with the relevant Order in respect of the Products and / or Services to which it relates, this Agreement contains the entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all previous communications, representations, understandings and agreements, either oral or written between the parties with respect to said subject matter, including any prior non-disclosure agreements.

10.13.2 Without limiting the generality of Section 10.15.1 of Part 1 of this Agreement, any terms and conditions contained in any purchase order, vendor / supplier registration form, questionnaire or any other form or document that End User may provide to Thales in connection with this Agreement and/or the Products or Services shall be void, regardless of whether Thales fails to object to such terms and whether such forms were provided prior to or after the Effective Date.

10.13.3 Each party acknowledges that, in agreeing to enter into this Agreement, it has not relied on any express or implied representation, warranty, collateral contract or other assurance (except those set out in this Agreement). Each party waives all rights and remedies which, but for this Section 10.15, might otherwise be available to it in respect of any such express or implied representation, warranty, collateral contract or other assurance.

10.13.4 Nothing in this Agreement limits or excludes any liability for fraud.

### **10.14 Severability and binding effect.**

If any provision of this Agreement is deemed invalid or unenforceable by a court of competent jurisdiction, the provision shall be changed and interpreted, if possible, to accomplish the original intent of the parties within the constraints of the law, or if not possible, the provision shall be stricken from the Agreement. The remaining provisions of the Agreement shall remain in full force and effect.

### **10.15 Authority to contract.**

Each party represents that it has the required legal capacity, corporate power and authority to enter into and perform this Agreement, and that this Agreement has been duly and validly executed and constitutes the legal, valid and binding obligation of such party and is enforceable against such party in accordance with its terms.

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

**10.16 NON-SOLICITATION**

10.16.1 The End User undertakes during the term of this Agreement and for one year after its termination not to solicit, hire, employ or offer employment, directly or indirectly through its affiliates, to any of Thales' employees who has been engaged in providing Services pursuant hereto without Thales' prior written consent; provided, however, that nothing herein shall preclude the hiring of any such individual who:

- (a) responds to general solicitation of employment through an advertisement not directed at such employees of Thales;
- (b) contacts End User on his or her own initiative and without any direct solicitation by End User;
- (c) has terminated employment with Thales prior to commencement of solicitation of such employee by End User.

10.16.2 This Section does not apply where explicitly prohibited by local law and/or regulation.

**10.17 Thales Entity.**

10.17.1 Where the Purchaser places an Order for Thales Products and/or Thales Services, the applicable Thales contracting entity shall be determined in accordance with the table set out below.

<b>Location of Purchaser</b>	<b>Thales Counterparty</b>	<b>Notice Address</b>
United States of America and the Caribbean	Thales DIS CPL USA, Inc.	9442 Capital of Texas Hwy, Plaza II, Suite 400, Austin, TX, 78759, USA
Canada	Thales DIS CPL Canada, Inc.	20 Colonnade Road - Suite 200, Ottawa, ON K2E 7M6
Brazil	Thales DIS Brasil Cartões e Soluções Tecnológicas Ltda	9442 Capital of Texas Hwy, Plaza II, Suite 400, Austin, TX, 78759, USA
Mexico & Rest of the LATAM countries (except as noted)	Thales DIS Mexico SA DE CV	9442 Capital of Texas Hwy, Plaza II, Suite 400, Austin, TX, 78759, USA

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

Hong Kong, China and the rest of Asia (except as noted)	Thales DIS CPL Hong Kong Limited	Units 1105 to 1107, 11/F, New Kowloon Plaza, 38 Tai Kok Tsui Road, KL, Hong Kong
Japan	Thales DIS Japan KK	8th Floor, Akasaka Tameike Tower, 2-17-7 Akasaka, Minatoku, Tokyo 107-0052, Japan
India	Thales DIS India Private Limited	1st Floor, Plot No. 12 A, Sec-125, Distt. Gautam Budh Nagar Noida, Uttar Pradesh, 201301, India
Australia & New Zealand	Thales DIS CPL Australia Pty Ltd.	Northpoint Tower, Level 40, 100 Miller Street, North Sydney 2060, Australia
Germany	Thales DIS CPL Deutschland GmbH	Werinherstrasse 81, 81541 München, Germany
United Kingdom	Thales DIS CPL UK Limited	350 Longwater Avenue, Green Park Business Park, Reading, Berkshire RG2 6GF, United Kingdom
EMEA (except as noted)	Thales DIS Technologies BV	Seattleweg 5, Rotterdam-Pernis, 3195 ND, The Netherlands
Israel	Thales DIS Israel Ltd	35 Efal St., Kiryat Arye, P.O. Box 3968. Petach Tikvah, 4951132, Israel.

10.17.2 Where the Purchaser places an Order for Imperva Products and/or Imperva Services, the Thales contracting entity shall be Imperva Inc, with a registered address of Arboretum Plaza II, Suite 400, 9442 Capital of Texas Highway North | Austin, TX 78759. 10.18 **Thales locations**

Thales may utilise any of the regions or countries listed in Section 10.19 to provide the Products and Services.

**11 INTERPRETATION****11.1 DEFINED TERMS.**

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

In this Agreement, the following capitalized terms shall have the meanings set out below:

<b>“Agreement”</b>	has the meaning set out on the cover page;
<b>“Appliance”</b>	means the hardware on which certain Software operates, in each case as identified by the applicable SKU;
<b>“Authorized Third Party”</b>	means a third party that has a valid entitlement to procure Products and Services for onward resale (directly or indirectly) to an End User;
<b>“Cloud Services”</b>	means services provided by Thales and made available to End Users through the internet;
<b>“Confidential Information”</b>	has the meaning set out in Section 4.1.1 of Part 1 of this Agreement;
<b>“Console”</b>	means the interface through which certain features of the Software or Infrastructure may be accessed and configured;
<b>“Customer Support Guide”</b>	means the part of the Documentation that describes support;
<b>“Data and Security Terms and Conditions”</b>	means the terms and conditions set out in Part 4 of this Agreement;
<b>“Delivery”</b>	means, (i) in the case of Software, when the Software is made available by Thales for End User to electronically download; (ii) in the case of a Cloud Service or Infrastructure, when the Cloud Service or Infrastructure (as applicable) has been made available by Thales for End User to access; (iii) in the case of an Appliance that is an Imperva Product, when the Appliance has been tendered by Thales for shipment; and (iv) in the case of an Appliance that is a Thales Product and Hardware, F.C.A. (Incoterms 2020) at Thales’ facility. The term <b>“Deliver”</b> shall be construed accordingly;
<b>“Direct Orders”</b>	has the meaning set out in Section 1.2 of Part 1 of this Agreement;
<b>“Disclosing Party”</b>	has the meaning set out in Section 4.1.1 of Part 1 of this Agreement;

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

<b>“Documentation”</b>	means Thales’ standard materials that describe the Products, including the installation, use, operation, features and / or functionality of the Products, and how Thales provides maintenance and / or support in relation to the same, as available at <a href="https://thalesdocs.com/">https://thalesdocs.com/</a> , <a href="https://docs.imperva.com/">https://docs.imperva.com/</a> and <a href="https://cpl.thalesgroup.com/legal">https://cpl.thalesgroup.com/legal</a> , as updated by Thales from time to time;
<b>“DPA”</b>	means the relevant Data Protection Agreement(s) as set out in Sub-parts 2.6 and 3.5 or referenced in Sub-parts 4.6 and 4.7 of this Agreement, applicable to certain Products and/or Services that may be ordered by Purchaser in accordance with this Agreement;
<b>“DPOD Platform”</b>	means the Thales Data Protection On Demand Platform, a Cloud Service made available to End Users pursuant to Sub-part 3.1 of the Product Specific Terms Conditions (including the Annex to Sub-part 3.1 of the Product Specific Terms and Conditions);
<b>“DPOD Service Description”</b>	means the part(s) of the Documentation that detail the specific part of the Cloud Service comprised in the relevant Order that is available via the DPOD Platform;
<b>“Effective Date”</b>	means the date set out on the cover page of this Agreement;
<b>“End User”</b>	means the entity set out on the cover page;
<b>“Evaluation License”</b>	has the meaning set out in Sub-part 2.5, Sub-part 3.4 or Sub-part 4.4, as applicable;
<b>“Evaluation Period”</b>	has the meaning set out in Sub-part 2.5, Sub-part 3.4 or Sub-part 4.4 as applicable;
<b>“Evaluation Product”</b>	means a Product that Thales has elected to make available to End User on a temporary, without charge basis, for non-commercial use solely for internal evaluation purposes;
<b>“Failure”</b>	means any reproducible defect in the Product that causes the Product to fail to perform substantially in accordance with the Documentation;
<b>“Feedback”</b>	has the meaning set out in Section 8.3 of Part 1 of this Agreement;

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

<b>“General Terms and Conditions”</b>	means the terms and conditions set out in this Part 1 of this Agreement;
<b>“Group Companies”</b>	means all entities which are controlled by Thales, or under common control with Thales, where “control” means the indirect or direct or beneficial ownership of a voting interest of more than fifty percent (50%) and “Group Company” shall be construed accordingly;
<b>“Hardware”</b>	means the hardware on which certain Software operates, in each case as identified by the applicable SKU;
<b>“Imperva Products”</b>	means the Products for which Imperva, Inc. is the relevant Group Company listed on the Quote;

<b>“Imperva Services”</b>	means the Services for which Imperva, Inc. is the relevant Group Company on the Quote;
<b>“Information Notice”</b>	means the notice for processing of contact details under Thales agreements available <a href="#">here</a> or such other URL as may be published from time to time;
<b>“Infrastructure”</b>	means Thales’ or its licensor’s application and / or network protection solutions, in each case as identified by the applicable SKU;
<b>“Infrastructure SLA”</b>	has the meaning set out in Section 3 of Sub-part 2.2 of this Agreement;
<b>“Infringement Claim”</b>	has the meaning set out in Section 9.1 of Part 1 of this Agreement;

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

<b>“Intellectual Property Rights”</b>	means any and all intellectual property rights in any part of the world, arising under statutory or common law or by agreement and whether or not perfected, registered or unregistered, now existing or hereafter filed, issued, or acquired, and any renewals, extensions and other government issued indicia of ownership thereof, including, but not limited to, rights comprising or relating to: (a) patents, patent disclosures and inventions (whether patentable or not); (b) rights associated with works of authorship including copyrights and copyrightable works (including, but not limited to, computer programs), copyright registrations and applications for copyright registration, “moral” rights and mask work rights (all “copyrights”); (c) rights relating to the protection of trade secrets, know-how and other Confidential Information; (d) trademarks, trade dress, trade names, logos and service marks, together with the goodwill or business symbolized by or associated therewith; (e) domain names, web addresses and social media identifiers; (f) any registrations or applications for registration for any of the foregoing, including any provisionals, divisions, continuations, continuations-in-part, renewals, reissuances, re-examinations and extensions (as applicable); and (g) analogous rights to those set forth above;
<b>“License Definitions and Rules”</b>	means the document set out <a href="#">here</a> or such other location as Thales may specify from time to time;
<b>“Licensed Volume”</b>	means the volume or other measurement or conditions of permitted use for the Products as set out for the applicable SKU or as otherwise set out in a Quote;
<b>“Order”</b>	means, (i) an order form executed by End User and submitted to Thales or (ii) a purchase order submitted by End User, or by an Authorized Third Party on behalf of End User, in each case, in response to a Quote (which the Order is deemed to include) and that is accepted by Thales;
<b>“Order Acknowledgment”</b>	means a written (confirmation notice electronic or otherwise) that the relevant Thales entity issues to End User confirming the purchase and/or license of the Products and/or Services by End User.
<b>“Packaged Services”</b>	means Thales’ pre-formulated, defined scope, service offerings, as identified by the applicable SKU and subject to Sub-part 5.1 of the Services Specific Terms;

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

<b>“Product Specific Terms and Conditions”</b>	means the terms and conditions set out in Parts 2, 3 and 4 of this Agreement;
<b>“Products”</b>	means the Software, Infrastructure, Console, Cloud Services, Hardware and Appliances, as may be supplied to an End User in accordance with this Agreement;
<b>“Purchaser”</b>	means the entity which has submitted an Order in response to a Quote for the Products and/or Services which shall be: (i) for Orders placed directly with Thales, the End User; and (ii) for orders placed by an Authorised Third Party, the Authorised Third Party that submits the order directly to Thales;
<b>“Quote”</b>	means a Thales sales quotation which sets out Products and Services by SKU and which may include corresponding descriptions and details of the applicable Licensed Volume;
<b>“Receiving Party”</b>	has the meaning set out in Section 4.1.1 of Part 1 of this Agreement;
<b>“Scoped Services”</b>	means such other services set out in a Statement of Work that Thales may provide pursuant to this Agreement, excluding Packaged Services and Training Services and subject to Sub-part 5.2 of the Services Specific Terms;
<b>“Service Description”</b>	has the meaning set out in Section 1.1 of Sub-part 5.1 of this Agreement;
<b>“Service Outcome”</b>	means a specific set of configuration tasks as set out in the Service Description;
<b>“Services”</b>	means the Packaged Services, Scoped Services, Training Services and Support Services, as may be ordered by Purchaser in accordance with this Agreement;
<b>“Services Specific Terms and Conditions”</b>	means the terms and conditions set out in Part 5 of this Agreement;

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

<b>“SKU”</b>	means Thales’ internal stock keeping unit for each of its Products and Services, which may include corresponding Product descriptions and details of the applicable Licensed Volume;
<b>“SLA”</b>	means the description and definition of certain features of a Product or Service set out in the Documentation;
<b>“Software”</b>	means Thales’ or its licensors’ software (in object code format), provided to End User by Thales or an Authorized Third Party, in each case as identified by the applicable SKU and subject to Sub-part 2.1, Sub-part 3.2 and Sub-part 4.2 of the Product Specific Terms Conditions;
<b>“Statement of Work”</b>	means a signed description of Scoped Services;
<b>“Support Services”</b>	means the services described in the relevant Support Terms;
<b>“Support Terms”</b>	means solely where there is a valid subsisting Order that includes support: (a) in respect of the Imperva Products, the Customer Support Guide; or (b) in respect of the Thales Products, Sub-part 5.4 of the Services Specific Terms;
<b>“Thales Products”</b>	means Products, for which a Group Company other than Imperva, Inc. is listed on the Quote;
<b>“Thales Services”</b>	means Services, for which a Group Company other than Imperva, Inc. is listed on the Quote;
<b>“Third Party Products”</b>	means Products which are licensed to Thales by a third party and are subject to the Third Party Terms;
<b>“Third Party Terms”</b>	means the document set out <a href="#">here</a> or such other location as Thales may specify from time to time;
<b>“Threat Data”</b>	has the meaning set out in Section 2.3.2(c) of Sub-part 2.2;
<b>“Traffic”</b>	has the meaning set out in Section 2.3.2(b) of Sub-part 2.2 of this Agreement;

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

<b>“Training Services”</b>	means the training services set out in Thales’ training catalog, in each case as identified by the applicable SKU and subject to Sub-part 5.3 of the Services Specific Terms;
<b>“Usage Data”</b>	has the meaning set out in Section 5.2.2 of Sub-part 3.2 of this Agreement; and
<b>“Welcome Pack”</b>	means the guide to using Thales technical support services located <a href="#">here</a> or such other document at such other URL as may be updated from time to time by Thales in its sole discretion and for this purpose including the details of the support plans set out in the Documentation.

**11.2 Interpretation.**

In this Agreement (except where the context otherwise requires):

- (a) any reference to a Section is to the relevant Section of the relevant part or sub-part of this Agreement as applicable;
- (b) the Section headings are included for convenience only and shall not affect the construction or interpretation of this Agreement;
- (c) words importing a particular gender do not exclude other genders;
- (d) use of the singular includes the plural and vice versa;
- (e) references to any law include a reference to that law together with all rules and regulations made under it or them, all as from time to time amended, consolidated or re-enacted;
- (f) any phrase introduced by the terms "including", "include", "in particular" or any similar expression shall be construed as illustrative and the words following any of those terms shall not limit the sense of the words preceding those terms;
- (g) references to other documents that are incorporated by reference shall include those documents as amended from time to time; and
- (h) any grant of license, permission or other right set out in this Agreement for the benefit of Thales shall be deemed to confer the same benefit on Thales’ Group Companies.

Version: 2 April 2025



## THALES CYBER SECURITY PRODUCTS END USER AGREEMENT

### PART 2: APPLICATION SECURITY PRODUCT SPECIFIC TERMS AND CONDITIONS

#### 1. OVERVIEW.

1.1 This part of the Agreement is divided into the following sub-parts:

Product Area	Sub-part	Product Specific Terms and Conditions
Application Security	2.1	Software Specific Terms and Conditions
	2.2	Infrastructure Specific Terms and Conditions
	2.3	Console Specific Terms and Conditions
	2.4	Appliances Specific Terms and Conditions
	2.5	Evaluation Specific Terms and Conditions
	2.6	Data Protection and Security Terms and Conditions

### PART 2: APPLICATION SECURITY

#### 1) SUB-PART 2.1: SOFTWARE SPECIFIC TERMS AND CONDITIONS

**THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

**1. LICENSE TERMS.**

**1.1 Grant.**

- (a) Subject to End User's compliance with this Agreement, and upon acceptance of an Order, Thales grants End User a non-exclusive, non-transferable, non-sublicensable, revocable license to use the Software, in accordance with its corresponding Documentation, solely for End User's internal business purposes, on the Appliances (where applicable), subject to and up to the Licensed Volume, and for the license term, each as described in the relevant Quote.
- (b) If End User receives a license to the Software pursuant to this Agreement on a standalone basis, the license granted in this Section shall include the right to copy the Software up to the Licensed Volume.
- (c) End User acknowledges and agrees that the Licensed Volume shall be interpreted in accordance with the License Definitions and Rules.
- (d) In respect of Third Party Products, End User shall be bound by the Third Party Terms.

**1.2 Warranty.**

Thales warrants that during the sixty (60) day period commencing on the date of first Delivery, the Software shall perform substantially in accordance with the Documentation. In the event of a breach of the foregoing warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, either replace the Software with Software conforming to the warranty in this Section 1.2, or use reasonable efforts to modify the Software so that it performs substantially in accordance with the Documentation. The rights and remedies granted to End User under this Section state Thales' entire liability, and End User's exclusive remedy, with respect to any breach of the warranty set out in this Section.

**2. DELIVERY.**

**2.1 Delivery.**

Upon acceptance of an Order, Thales shall use commercially reasonable efforts to Deliver any Software license keys that may be required to use the Software in accordance with the

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

Documentation for the duration of the Order. Direct Orders shall be Delivered to End User and Orders via an Authorized Third Party shall be Delivered via the Authorized Third Party. Software shall be deemed accepted by End User upon Delivery.

### **2.2 Delay.**

Provided that Thales has used commercially reasonable efforts, Thales shall in no event be liable for any delay in Delivery or for failure to give notice of delay.

## **3. MAINTENANCE AND SUPPORT.**

Maintenance and support are provided in accordance with the Customer Support Guide.

## **4. DATA RECOVERY.**

End User is solely responsible for End User's data back-up, data recovery, and disaster recovery measures. Thales shall not be responsible for End User's internal processes and procedures to ensure the protection of End User's data or information stored within End User's own environment. End User shall maintain an unmodified copy of all Software and all related Documentation, archival files and configuration files necessary to reinstall, reconfigure or reconstruct any lost, altered or damaged Software.

## **5. POLICIES.**

### **5.1 Security maintenance.**

Where Thales reasonably considers End User's use of the Software could (i) pose a security risk to Thales, the Software or any third party; (ii) adversely impact Thales' systems, the Software or the systems, traffic or data of any other Thales partner or customer; (iii) subject Thales, its partner, suppliers or any third party to liability, or (iv) be fraudulent, Thales shall have the right to suspend in whole or in part End User's rights to access or use the Software (including any Support Services) immediately upon notice. During any such suspension, End User shall remain responsible for all fees during the period of suspension.

### **5.2 End of life policy.**

All Software is subject to Thales' then-current End of Life Policy (available [here](#) or such alternate URL or other repository as Thales may specify from time to time).

## **PART 2: APPLICATION SECURITY**

### **SUB-PART 2.2: INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS**

**THESE INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. LICENSE TERMS.**

##### **1.1 Grant.**

- (a) Subject to End User's compliance with this Agreement, and upon acceptance of an Order by Thales, Thales grants End User a non-exclusive, non-transferable, non-sublicensable, revocable license to use the Infrastructure, in accordance with its corresponding Documentation, solely for End User's internal business purposes, subject to and up to the Licensed Volume, and for the license term, each as described in the relevant Quote.
- (b) End User acknowledges and agrees that the Licensed Volume shall be interpreted in accordance with the License Definitions and Rules.
- (c) In respect of Third Party Products, End User shall be bound by the Third Party Terms.

##### **1.2 Warranty.**

Thales warrants that during the term of the relevant Order, the Infrastructure shall perform substantially in accordance with the Documentation and in compliance with the Infrastructure SLA. In the event of a breach of this warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, correct the Infrastructure so that it performs substantially in accordance with the Documentation and, either directly issue or have an Authorized Third Party issue, any credits to which End User may be entitled pursuant to the Infrastructure SLA.

#### **2. Access and use of Infrastructure.**

##### **2.1 Delivery.**

- 2.1.1** Upon acceptance of an Order, Thales shall use commercially reasonable efforts to Deliver (either directly or via an Authorized Third Party, as applicable) any Infrastructure credentials that may be required to use the Infrastructure in accordance with the Documentation for the duration of the Order. Infrastructure shall be deemed accepted by End User upon Delivery.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 2.1.2** Provided that Thales has used commercially reasonable efforts, Thales shall in no event be liable for any delay in Delivery or for failure to give notice of delay.

### **2.2 Set up**

Except as explicitly set out in this Agreement, End User is solely responsible for acquiring and maintaining all of the equipment, software, services and items necessary to access and make use of the Infrastructure, including without limitation paying all fees, charges, taxes, and other costs related to internet access and for configuration changes that may be required to route activity to the Infrastructure. End User may access the Infrastructure only through the interfaces and protocols provided or authorized by Thales and agrees to set up, maintain and use the Infrastructure in strict compliance with Thales' and its Authorized Third Party's instructions.

### **2.3 Consents**

- 2.3.1** The routine operation of the Infrastructure involves End User traffic routing through the Thales network. Thales has no right to use any of the data within the traffic except as set out in this Agreement.

- 2.3.2** All of the consents granted in this Section 2.3 are to be exercised in accordance with the relevant DPA. End User consents to Thales using, and grants a nonexclusive, royalty-free, fully-paid up right and license to Thales to:

- (a) use, transfer, display, minimize and compress the content and material on End User's websites, in any media formats, in connection with the performance, improvement and support of the Infrastructure;
- (b) use, transfer, monitor and inspect End User's traffic that is routed via the Infrastructure, including any related logs or other data as may be required ("**Traffic**"), in connection with the performance, improvement and support of the Infrastructure; and
- (c) collect, analyze, use for the performance and improvement of the Products and Services, and the development of new products and services, and solely in a non-attributable format publish, the specific parts of the Infrastructure that relate directly and indirectly to purported attempts to compromise the security of End User via malicious traffic including but not limited to DDoS attacks, hacking attempts, and bot assaults plus false positives of the same ("**Threat Data**").

- 2.3.3** End User represents and warrants that it has all rights and permissions necessary to transfer, disclose and grant, to Thales, the rights contemplated by this Agreement, with respect to Traffic and Threat Data.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

### 2.4 Abuse

- 2.4.1** Thales operates an abuse desk for disputes about the use of the Infrastructure, including matters such as copyright infringement, child protection, spamming or another matter which potentially suggests that a site protected by Thales is involved in illegal activity.
- 2.4.2** Certain parts of the Infrastructure route traffic through the Thales network using a reverse proxy, before transmitting that traffic on to End User's specified destination server where data is stored. When a DNS lookup is performed, it appears that Thales is hosting the relevant website. Complaints are filed at [abuse@thalesgroup.com](mailto:abuse@thalesgroup.com) or such other location as Thales may specify from time to time. Thales does not have access to the host servers where data is stored and as such is unable to modify or take down any content from such websites.
- 2.4.3** Where a claim is submitted, Thales may share such information to any third party it considers appropriate, including End User that is the subject of the complaint and any relevant service provider related to the complaint.

### 2.5 End User responsibilities

- 2.5.1** End User shall ensure that its use of the Infrastructure complies with all applicable laws, rules, codes and regulations regarding online conduct and the collection and transmission of data, including all laws, rules, codes and regulations of the countries in which End User operates and from which it collects or otherwise processes data.
- 2.5.2** The Infrastructure may include a shared web caching service, which means a number of different end users' sites are cached on the same server. End User shall not use the Infrastructure in a manner that could disrupt or otherwise adversely affect or impair the performance of any other sites of other end users and customers of Thales.
- 2.5.3** End User is responsible for configuring the encryption for Traffic that is routed through the Infrastructure and for any rules that End User implements or actions that may be taken that could result in performance degradation or other availability, access or performance issues.
- 2.5.4** In the event of expiration or termination of any Infrastructure that require DNS routing, End User shall be solely responsible for rerouting its DNS traffic and Thales, its partners and suppliers shall have no liability for End User's failure to do so.

### 2.6 Modifications

- 2.6.1** Subject to Section 2.6.2, Thales engages in the constant evolution, innovation and improvement of its Infrastructure, and implements modifications that reflect new or enhanced features or functionalities. Thales may modify the features or functionalities of the Infrastructure provided that such modifications will not materially degrade the core functionality of the Infrastructure. Thales may discontinue the Infrastructure and will use commercially reasonable efforts to transfer End User to a substantially similar service. If Thales does not have a substantially similar service, Thales will refund to End User or Authorized Third Party the unused portion of any prepaid fee for End User's Infrastructure. Thales may notify End User of its actions pursuant to this section, provided that End User subscribed to receive such notification.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 2.6.2** Section 2.6.1 shall not apply to any changes to any point of presence, cross-connect or other aspect of the network that forms part of the Infrastructure.

### **3. SERVICE LEVELS.**

The applicable service level document (available at such location as Thales may specify from time to time) shall apply to the Infrastructure ("**Infrastructure SLA**").

### **4. SUPPORT.**

Support is provided in accordance with the Customer Support Guide.

### **5. DATA RECOVERY.**

End User is solely responsible for End User's data back-up, data recovery, and disaster recovery measures. Thales shall not be responsible for End User's internal processes and procedures to ensure the protection of End User's data. End User shall maintain a copy of all configuration files necessary to reinstall, reconfigure or reconstruct any lost, altered or damaged data of that nature.

### **6. POLICIES.**

#### **6.1 Security maintenance.**

Where Thales reasonably considers End User's use of the Infrastructure could: (i) pose a security risk to Thales, the Software or any third party; (ii) adversely impact Thales' systems, the Software or the systems, traffic or data of any other Thales partner or customer; (iii) subject Thales, its partner, suppliers or any third party to liability, or (iv) be fraudulent, Thales shall have the right to suspend in whole or in part End User's rights to access or use the Infrastructure immediately upon notice. During any such suspension, End User shall remain responsible for all fees during the period of suspension and shall not be entitled to any service credits that would have otherwise arisen pursuant to the Infrastructure SLA.

#### **6.2 End of life policy.**

The Infrastructure is subject to Thales' then current-End of Life Policy (available [here](#) or such alternate URL or other repository as Thales may specify from time to time).

### **6.3 Acceptable use policy.**

End User agrees that at all times it shall comply with the then-current Acceptable Use Policy (available [here](#) or such alternate URL or other repository as Thales may specify from time to time). Thales may flag or block content, block access to End User's sites from particular jurisdictions or suspend or terminate End User's access to the Infrastructure immediately upon notice to End User where Imperva reasonably determines use of the Infrastructure to be contrary to the Acceptable Use Policy.

## **PART 2: APPLICATION SECURITY**

### **SUB-PART 2.3: CONSOLE SPECIFIC TERMS AND CONDITIONS**

**THESE CONSOLE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS AND THE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND / OR INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE CONSOLE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL. IN THE EVENT OF CONFLICT BETWEEN THESE CONSOLE SPECIFIC TERMS AND CONDITIONS AND THE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND / OR INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS, THE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND / OR INFRASTRUCTURE SERVICES SPECIFIC TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. OVERVIEW.**

Certain Software and Infrastructure allow End User to access a Console. The specific details and purpose of the relevant Console is set out in the Documentation. Broadly, where a Software or Infrastructure includes a Console, the Console shall enable End User to access and configure certain features of the Product.

#### **1. CONSOLE-SPECIFIC TERMS.**

##### **1.1 Grant.**

The grant of a license to a Console shall be on the same terms and conditions as the relevant Software or Infrastructure.

##### **1.2 Access.**

- (a) End User is solely responsible for maintaining the confidentiality of any passwords and account information required to access the Console, for all acts that occur in connection with End User's account and to immediately notify Thales of any unauthorized use of End User's account. End User shall take notify Thales promptly in writing if it is aware of any unauthorized access or use of a Console.
- (b) Except as explicitly set out in this Agreement, End User is solely responsible for acquiring and maintaining all of the equipment, software, services and items necessary to access and make use of a Console, including without limitation paying all fees, charges, taxes, and other costs related to internet access.

##### **1.3 Records.**

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- (a) End User is solely responsible for End User's data back-up, data recovery, and disaster recovery measures. Thales shall not be responsible for End User's internal processes and procedures to ensure the maintenance of copies of records made available to End User as part of the Console.
- (b) Thales does not provide backup services. If End User's use of the Console terminates for any reason, Thales may, without notice, delete or deny End User access to any records made available to End User as part of the Console.

### **1.4 Consents.**

Where an End User utilizes certain Consoles, End User grants Thales a license to collect, analyze, use for the performance and improvement of the Products and Services, and the development of new products and services, and solely in a non-attributable format publish, Threat Data. The consents granted in this Section 2.4 are to be exercised in accordance with Part 2.6 of this Agreement (Data Protection and Security Terms and Conditions). End User represents and warrants that it has all rights and permissions necessary to transfer, disclose and grant, to Thales, the rights contemplated by this Agreement, with respect to Threat Data.

## **PART 2: APPLICATION SECURITY**

### **SUB-PART 2.4: APPLIANCES SPECIFIC TERMS**

**THESE APPLIANCES SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE APPLIANCES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

### **1. OVERVIEW.**

1.2 This section sets out the terms specific to Appliances only.

1.3 In respect of Third Party Products, End User shall be bound by the Third Party Terms.

### **2. DELIVERY, RISK AND TITLE.**

2.1 Thales shall use commercially reasonable efforts to Deliver the Appliances in accordance with any reasonable delivery times requested in accepted Orders (in partial or full shipments). Provided Thales has used commercially reasonable efforts to Deliver the Appliances in accordance with any such requested delivery times, Thales shall in no event be liable for any delay in Delivery or for failure to give notice of delay. Appliances shall be deemed accepted by End User upon Delivery.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 2.2 Risk of loss and, if applicable, title to Appliances shall pass to End User upon Delivery; provided that title shall not pass to End User for:
- (a) any Software contained in or installed on such Appliances; or
  - (b) any Appliances for which End User has not purchased outright and paid for in full.
- 2.3 Appliances shall be delivered Ex Works (Incoterms 2020) to Thales' designated manufacturing facility.
- 2.4 End User may specify shipping instructions with the Order, which are subject to Thales' acceptance. In the absence of specific shipping instructions from End User, which have been agreed to by Thales, Thales shall ship by the method it deems appropriate.
- 2.5 End User shall pay and be exclusively liable for all costs associated with shipping and delivery including without limitation, freight, shipping, customs charges and expenses, cost of special packaging or handling and insurance premiums.
- 2.6 In its discretion, Thales may advance shipping charges on behalf of End User on Appliances shipped to End User, and End User agrees to reimburse Thales for any such advanced charges and expenses.
- 2.7 If End User enters into a term agreement for use of Appliances, all right, title and interest in such Appliances shall remain with Thales and must be returned by End User within fifteen (15) days after the end of the applicable term or End User shall be charged and pay for the Appliances at Thales' then-current list price. End User must keep such Appliances free from liens or pledges, shall be responsible for any damage to such Appliances during the applicable term, reasonable wear and tear excepted, and shall carry a policy of fire and extended coverage (all risks), in an amount equal to the full replacement value of such Appliances.

### **3. SOFTWARE.**

- 3.1 End User acknowledges that the Software included with the Appliance is licensed, and not sold, with the applicable license terms set out in Sub-part 2.1 of this Agreement.
- 3.2 Software is licensed solely in conjunction with such Appliance (and not separately or apart from such Appliance). If End User sells, leases, lends, rents, distributes or otherwise transfers any Appliance to any third party or if Thales terminates this Agreement or any relevant Order, then End User shall erase all Software from such Appliance.

### **4. MAINTENANCE AND SUPPORT.**

Maintenance and support are provided in accordance with the Customer Support Guide.

### **5. WARRANTY.**

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

Thales warrants that during the ninety (90) day period commencing on the date of first Delivery, the Appliances shall perform substantially in accordance with the Documentation. In the event of a breach of this warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, following the return of such Appliance by End User, either repair the Appliance or replace the Appliance with a new or reconditioned Appliance that performs substantially in accordance with the Documentation. This warranty extends only to the original purchaser of the Appliance and shall not apply where there has been damage to the Appliance returned to Thales.

## **PART 2: APPLICATION SECURITY**

### **SUB-PART 2.5: EVALUATION SPECIFIC TERMS AND CONDITIONS**

**THESE EVALUATION SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS AND THE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND / OR INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE EVALUATION SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. APPLICABLE TERMS AND CONDITIONS.**

1.1 From time to time, Thales may make available Evaluation Products to End User on a temporary basis for evaluation purposes, pursuant to an Order or otherwise.

1.2 Where an End User utilises an Evaluation Product:

1.2.1 for Software the following Sections of the Software Specific Terms and Conditions set out in Sub-part 2.1 of this Agreement shall not apply: 1.1 and 1.2;

1.2.2 for Infrastructure, the following Sections of the Infrastructure Specific Terms and Conditions set out in Subpart 2.2 of this Agreement shall not apply: 1.1, 1.2 and 3;

1.2.3 for Console, the following Sections of the Console Specific Terms and Conditions set out in Sub-part 2.3 of this Agreement shall not apply: 2.1;

1.2.4 for Appliances, the following Sections of the Appliances Specific Terms and Conditions set out in Sub-part 2.4 of this Agreement shall not apply: 2 and 5; and

1.2.5 the following Sections of the General Terms and Conditions shall not apply: 6, 7 and 9.

#### **2. EVALUATION LICENSE.**

Where Thales agrees to make an Evaluation Product available to an End User, Thales grants to End User during the Evaluation Period, a cost-free, non-sublicensable, non-transferable, non-assignable and non-exclusive, revocable at will license to use the Evaluation Product, solely at the location identified in writing by End User and solely for End User's internal evaluation of the Evaluation Product ("**Evaluation License**").

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **3. EVALUATION PERIOD.**

3.1 Unless otherwise agreed to in writing, or terminated earlier in accordance with this Agreement, the term of the license to an Evaluation Product shall commence upon Delivery of the Evaluation Product and continue until the earlier of:

3.1.1 thirty (30) days from Delivery; or

3.1.2 the date that Thales provides written notice of termination to End User ("**Evaluation Period**").

3.2 Upon the expiration or termination of the Evaluation Period:

3.2.1 the Evaluation License shall cease;

3.2.2 End User shall immediately:

(a) return the Evaluation Product to Imperva;

(b) destroy or erase any intangible copies of the Evaluation Product; and

(c) certify in a writing signed by an officer of End User and delivered to Thales that all such copies of have been returned, destroyed or erased.

### **4. WARRANTY.**

**NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, END USER ACKNOWLEDGES AND AGREES THAT THE EVALUATION PRODUCT IS PROVIDED FOR EVALUATION "AS-IS" AND THALES AND ITS SUPPLIERS MAKE NO REPRESENTATIONS, CONDITIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE EVALUATION PRODUCT, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, INFORMATIONAL CONTENT, SYSTEM INTEGRATION, ENJOYMENT, NONINFRINGEMENT OR ANY OTHER WARRANTIES ARISING OUT OF COURSE OF DEALING, USAGE OR TRADE.**

### **5. LIABILITY.**

**NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, IN NO EVENT SHALL THALES' TOTAL AND AGGREGATE LIABILITY IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE EVALUATION PRODUCT EXCEED ONE HUNDRED DOLLARS (\$100).**

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

**PART 2: APPLICATION SECURITY****SUB-PART 2.6: DATA PROTECTION AND SECURITY**

Where the End User submits an Order for Imperva Products and/or Services, the Data Processing Addendum and Security Addendum set below, shall apply to the use of the applicable Imperva Products and/or Imperva Services.

<a href="#"><u>Data Processing Addendum</u></a>
<a href="#"><u>Security Addendum</u></a>

Version: 2 April 2025



## THALES CYBER SECURITY PRODUCTS END USER AGREEMENT

### PART 3: DATA SECURITY PRODUCT SPECIFIC TERMS AND CONDITIONS

#### 1. OVERVIEW.

1.1 This part of the Agreement is divided into the following sub-parts:

Product Area	Sub-part	Product Specific Terms and Conditions
Data Security	3.1	Cloud Services Specific Terms and Conditions  (Annex 1: Data Protection on Demand (DPOD) Platform Services Supplemental Terms and Conditions)
	3.2	Software Specific Terms and Conditions
	3.3	Appliances Specific Terms and Conditions
	3.4	Evaluation Specific Terms and Conditions
	3.5	Data Protection and Security

### PART 3: DATA SECURITY

#### SUB-PART 3.1: CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS

**THESE CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS GOVERN THE END USER'S ACCESS AND USE OF CLOUD SERVICES AND INCORPORATE AND ARE**

**SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

**1. LICENCE TERMS.**

**1.1 Grant.**

Subject to End User's compliance with this Agreement, and upon acceptance of an Order or, where transacted via the Thales marketplace, completion of the Order by an End User, Thales grants End User a non-exclusive, non-transferable, non-sublicensable, revocable right, during the Term, to access and use the Cloud Services, in accordance with its corresponding Documentation, solely for End User's internal business purposes, subject to and up to the Licensed Volume and for the license term. In respect of Third Party Products, End User shall be bound by the Third Party Terms.

**2. WARRANTY, SUPPORT AND SLA.**

2.1 Thales warrants that during the term of the relevant Order, the Cloud Services shall perform substantially in accordance with the Documentation and in compliance with the SLA. In the event of a breach of this warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, correct the Cloud Services so that it performs substantially in accordance with the Documentation and, either directly issue or have an Authorized Third Party issue, any credits to which End User may be entitled pursuant to the SLA.

2.2 If Thales suspends the Cloud Services in accordance with Section 6 of Sub-part 3.1, then during any such suspension, End User shall remain responsible for all fees during the period of suspension and shall not be entitled to any service credits that would have otherwise arisen pursuant to SLA.

2.3 Support is provided in accordance with the Support Terms.

**3. ACCESS AND USE OF CLOUD SERVICES.**

1.1 To access the Cloud Services, End User is required to set up an account or complete an Order for each Cloud Service. End User is responsible for ensuring the accuracy of the information required to set up the account. Thales' ability to deliver the Cloud Services depends upon End User's cooperation in setting up the account and on the accuracy of the information provided. If End User does not set up an account or if the information provided is inaccurate, Thales may not be able to perform the Cloud Services.

1.2 End User is responsible for the access to, and use of, the Cloud Services and for compliance with this Agreement, for which End User shall remain directly liable to Thales. End User will ensure that individuals which may access the Cloud Services

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

maintain the confidentiality of login credentials and promptly notify Thales of any security breaches including compromise of End User accounts or credentials. End User shall maintain a written, up to date, list of all current individuals which may access the Cloud Services and provide such list to Thales within seven (7) days of Thales' written request from time to time. In addition, Thales reserves the right to monitor End User's use of the Cloud Services from time to time to assess whether such usage is in accordance with this Agreement (including any agreed usage limits). Where such monitoring reveals that End User has exceeded any agreed usage limits, Thales reserves the right to increase the Fees and End User shall pay such increased Fees to Thales.

- 1.3 Thales engages in the constant evolution, innovation and improvement of its Cloud Services, and implements modifications that reflect new or enhanced features or functionalities. Thales may modify the features or functionalities of the Cloud Services provided that such modifications will not materially degrade the core functionality of the Cloud Services. Thales may discontinue the Cloud Services and will use commercially reasonable efforts to transfer End User to a substantially similar Cloud Service. If Thales does not have a substantially similar Cloud Service, Thales will refund to End User or Authorized Third Party the unused portion of any prepaid fee for End User's Cloud Service. Thales may notify End User of its actions pursuant to this section, provided that End User subscribed to receive such notification. Thales may perform scheduled or emergency maintenance of the Cloud Services during which time End User may experience interruption of the Cloud Services.
- 1.4 End User is responsible for ensuring the individuals using the Cloud Services comply with such acceptable use provisions relating to the Cloud Services as Thales may specify from time to time. Thales reserves the right to, without liability or prejudice to its other rights or remedies, disable any Users credentials and/or access to all or part of the Cloud Services in the event it reasonably suspects a breach of such acceptable use provisions. Thales shall notify the End User of its intention to disable any credentials pursuant to this Section 3.4 of Sub-part 3.1 before it disables such credentials.
- 1.5 Except as explicitly set out in this Agreement, End User is solely responsible for acquiring and maintaining all of the equipment, software, services and items necessary to access and make use of the Cloud Services including without limitation paying all fees, charges, taxes, and other costs related to internet access and for configuration changes that may be required to route activity to the Cloud Services. End User may access the Cloud Services only through the interfaces and protocols provided or authorized by Thales and agrees to set up, maintain and use the Cloud Services in strict compliance with Thales' and its Authorized Third Party's instructions.
- 1.6 Except to the extent set out in the Documentation, and where configuration is in accordance with the express requirements of the Documentation, use of the Cloud Services in conjunction with third party products is at End User's own risk.
- 1.7 End User acknowledges that Thales does not control the transfer of data over communications facilities, including the internet, and that the subscription may be subject to limitations, delays, and other problems inherent in the use of such communications facilities.

**4. EVALUATION SERVICES.**

Thales may offer Cloud Services as Evaluation Products. Any such use shall be pursuant to the terms of Sub-Part 3.4 of this Agreement.

**5. COMPLIANCE WITH LAWS.**

End User is solely responsible for and will comply with all laws or regulations of any governmental entity or authority applicable to End User's access or use of the Cloud Services.

**6. SUSPENSION OF THE CLOUD SERVICES.**

Thales may suspend End User's access to the Cloud Services in whole or part immediately and without any liability should Thales reasonably determine that End User's use of the Cloud Services: (i) is in breach of this Agreement, (ii) poses a security risk to Thales, the Cloud Services or any third party; (iii) may adversely impact Thales's systems, the Cloud Services or the systems, traffic or data of any other Thales partner or customer; (iv) subject Thales, its partner, suppliers or any third party to liability, (v) be fraudulent, or (vi) as otherwise required by laws or regulations of any governmental entity or authority. During any such suspension, End User shall remain responsible for all fees during the period of suspension and shall not be entitled to any service credits that would have otherwise arisen pursuant to the SLA.

**ANNEX 1**

**DPOD PLATFORM SERVICES SUPPLEMENTAL TERMS AND CONDITIONS**

**THESE DPOD PLATFORM SERVICES SUPPLEMENTAL TERMS AND CONDITIONS GOVERN THE END USER'S ACCESS AND USE OF THE DPOD PLATFORM, AND SHALL BE INCORPORATED WITHIN AND SUBJECT TO THE GENERAL TERMS AND CONDITIONS CONTAINED AT PART 1 AND THE CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS SET OUT IN SUB-PART 3.1.**

**1. ORDERING PROCESS.**

**1.1 Account Set Up.**

Thales' provision of the DPOD Platform shall be conditional upon End User setting up an account for each Cloud Service on the DPOD Platform. End User is solely responsible for ensuring the accuracy of the information required to set up the DPOD Platform account. Thales' ability to deliver the Cloud Services depends upon End User's cooperation in setting up the account and on the accuracy of the information provided. If End User does not set up an account

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

or if the information provided is inaccurate, Thales may not be able to perform the Cloud Services.

### **1.2 DPOD Platform Orders.**

End User may purchase Cloud Services entitlements directly from Thales on the DPOD Platform. Where an End User orders directly from Thales, the term and applicable fees (including when payments are due) shall be set out in the Order. In each case, End User may elect to terminate an order upon no less than thirty (30) days' notice to Thales before the end of the current term, or enter into a new order to renew the Cloud Service entitlements. In the absence of a termination notice or renewal order, the End User's entitlements shall continue on a rolling basis chargeable at the then current Thales rates, until the End User provides written notice to terminate of no less than thirty (30) days' to Thales.

### **1.3 Service Descriptions.**

Each Order for a Cloud Service on the DPOD Platform shall incorporate the relevant DPOD service description as set out in the Documentation.

## **PART 3: DATA SECURITY**

### **SUB-PART 3.2: SOFTWARE SPECIFIC TERMS AND CONDITIONS**

**THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

## **2. LICENSE TERMS.**

### **1.1 Grant.**

- (a) Subject to End User's timely payment of the Fees, compliance with this Agreement, and upon acceptance of an Order, Thales grants End User a non-exclusive, non-transferable, non-sublicensable, revocable license to use the Software, in accordance with its corresponding Documentation, solely for End User's internal business purposes, on the Appliances (where applicable), subject to and up to the Licensed Volume, and for the license term, each as described in the relevant Quote.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- (b) If End User receives a license to the Software pursuant to this Agreement on a standalone basis, the license granted in this Section shall include the right to copy the Software up to the Licensed Volume. End User may make one copy of the Software solely for archival purposes and one copy of the Software solely for backup purposes, provided the backup copy may only be used where the installed copy is inoperable and the inoperable copy is deleted.
- (c) All copies of the Software and the Documentation made by End User: (i) will be the exclusive property of Thales; (ii) will be subject to the terms and conditions of this Agreement; and (iii) must include all Intellectual Property Rights notices contained in the original delivered to End User.
- (d) End User acknowledges and agrees that, where applicable, the Licensed Volume shall be interpreted in accordance with the License Definitions and Rules.
- (e) In respect of Third Party Products, End User shall be bound by the Third Party Terms.

### 1.2 **Warranty.**

1.2.1 Thales warrants that during the ninety (90) day period commencing on the date of first Delivery, the Software shall perform substantially in accordance with the Documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. In the event of a breach of this warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, either replace the Software with Software conforming to the warranty in this Section 1.2, or use reasonable efforts to modify the Software so that it performs substantially in accordance with the Documentation. The rights and remedies granted to End User under this Section 1.2 state Thales' entire liability, and End User's exclusive remedy, with respect to any breach of the warranty set out in this Section.

1.2.2 Warranty claims must be made in writing during the warranty period accompanied by evidence of the defect satisfactory to Thales together with any available details that may reasonably assist Thales to reproduce the noncompliance and effect a cure. Thales' obligations under this express warranty are subject to Thales' examination of the Software and Thales' determination to its reasonable satisfaction that the claimed defect or fault actually exists, and is not excluded from this warranty. If Thales determines that the Software is not defective or faulty within the terms of this warranty, End User shall be liable for all of Thales' costs at Thales' then prevailing repair rates.

1.2.3 This warranty is conditioned upon payment of the purchase invoice and proper use of the Software, in accordance with the Documentation. Thales shall have no obligation under this warranty unless End-User promptly notifies

Thales in writing of any failures within the applicable warranty periods. This warranty extends only to the EndUser.

1.2.4 This warranty shall not apply to Software that has been: (i) improperly installed, modified or repaired by anyone other than Thales; (ii) used in a manner other than as authorized under the Documentation applicable to the Software purchased; (iii) installed, operated or maintained not in accordance with the instructions supplied by Thales, including but not limited to the installation, operation or maintenance of the Software on any hardware, operating system or tools (including their specific configurations) that are not compatible with the Software; (iv) modified, altered or repaired by a party other than Thales or a party authorized by Thales; (v) operated or maintained in unsuitable environmental conditions, or by any other cause external to the Software or otherwise beyond Thales' reasonable control, including any extreme power surge or failure or electromagnetic field, rough handling during transportation, fire or other act of God; (vi) use of the Software with telecommunication interfaces other than those supplied or approved by Thales not meeting or not maintained in accordance with Thales' specifications as described in the Documentation, unless Thales has specifically agreed in writing to include such modifications within the scope of this Agreement; (vii) damaged due to failure of power, air conditioning or humidity control, or failures of storage media not furnished by Thales or for consumable operating supplies or accessories outside the parameters designated in the Documentation or elsewhere, unless specifically included in this Agreement; (viii) subjected to accident, unusual physical, electrical or electromagnetic stress, neglect, or misuse fault or negligence of End User, its employees, agents, contractors or visitors, operator error; or (ix) where the serial numbers, warranty data or quality assurance decals on the hardware are removed or altered. Thales's warranty does not apply to (i) products manufactured by third parties and resold by Thales without re-marking under Thales's trademarks, (ii) software products that are not developed by Thales, and (iii) consumable items (e.g. batteries).

## **2. DELIVERY.**

### **2.1 Delivery.**

Upon acceptance of an Order, Thales shall use commercially reasonable efforts to Deliver any Software license keys that may be required to use the Software in accordance with the Documentation for the duration of the Order. Direct Orders shall be Delivered to End User and Orders via an Authorized Third Party shall be Delivered via the Authorized Third Party. Software shall be deemed accepted by End User upon Delivery. Unless otherwise mutually agreed, Thales shall make available the Software for electronic download by the End User.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **2.2 Delay.**

Provided that Thales has used commercially reasonable efforts, Imperva shall in no event be liable for any delay in Delivery or for failure to give notice of delay.

## **3. MAINTENANCE AND SUPPORT.**

3.1 If Thales is providing Imperva Products to the End User in accordance with these Software Specific Terms and Conditions set out in this Sub-part 3.2, maintenance and support are provided in accordance with the Customer Support Guide.

3.2 If Thales is providing Thales Products to the End User in accordance with these Software Specific Terms and Conditions set out in this Sub-part 3.2, the license granted hereunder does not entitle End User to any Software maintenance or Support Services unless End User purchases such maintenance and Support Services from Thales or an Authorized Third Party. Except as otherwise agreed by Thales under a separate written agreement, Support Services are subject to the Support Terms.

## **4. DATA RECOVERY.**

End User is solely responsible for End User's data back-up, data recovery, and disaster recovery measures. Imperva shall not be responsible for End User's internal processes and procedures to ensure the protection of End User's data or information stored within End User's own environment. End User shall maintain an unmodified copy of all Software and all related Documentation, archival files and configuration files necessary to reinstall, reconfigure or reconstruct any lost, altered or damaged Software.

## **5. AUDIT AND USAGE DATA.**

### **5.1 Audit of Thales Products**

5.1.1 In addition to the audit provisions set out in Section 5 of Part 1 (General Terms and Conditions) of this Agreement, the following audit terms shall apply to Software that is a Thales Product provided under the Software Specific Terms and Conditions set out in Sub-part 3.2 of this Agreement.

5.1.2 Upon Thales' written request, End User shall conduct a review of use of the Software and certify to Thales in a written instrument signed by an authorized representative of End User that it is in full compliance with this Agreement and, in particular, that it is not using more than the Licensed Volume. In the event of non-compliance,

End User shall immediately remedy such non-compliance and provide Thales with written notice signed by the authorized representative to confirm the same. End User shall provide

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

Thales with all access and assistance as Thales reasonably requests to further evaluate and remedy such noncompliance.

5.1.3 If the audit or any of the measures taken or implemented under this Section 5.1, determines that the End User's use of the Software exceeds the Licensed Volume:

- (a) End User shall, within thirty (30) days following the date of such determination by Thales, pay to Thales or the relevant Authorized Third Party the retroactive fees for such excess use at the then-current rates for such licenses;
- (b) If the use exceeds the Licensed Volume by more than ten percent (10%), End User shall pay Thales' reasonable costs incurred in conducting the audit; and
- (c) If the use exceeds the Licensed Volume by more than twenty percent (20%), Thales may terminate this Agreement and the license to the Software, effective immediately upon written notice to End User.

5.1.4 Thales's remedies set forth in this Section 5.1 are cumulative and are in addition to, and not in lieu of, all other remedies the Thales may have at law or inequity.

## 5.2 Usage Data for Imperva Products

5.2.1 In addition to the audit provisions set out in Section 5 of Part 1 (General Terms and Conditions) of this Agreement, the following audit terms shall apply to Software that is an Imperva Product provided under the Software Specific Terms and Conditions set out in Sub-part 3.2 of this Agreement.

5.2.2 Notwithstanding anything to the contrary in this Agreement, Thales has the right to collect and use Usage Data to develop, improve, support, and operate its products and services during and after the term of this Agreement and to verify an End User's usage in compliance with this Agreement. With respect to Software that includes a feature permitting transmission of Usage Data to Imperva, an End User may choose to disable such feature, in which case Imperva shall not collect Usage Data automatically from the Software. Where an End User opts to disable automatic transmission of Usage Data to Imperva within the Software, End User shall be obliged to manually produce a Usage Data report using a manual feature within the Software and transmit the same to Imperva no less than every three (3) months by following the instructions in the Documentation from time to time. End User shall take such other reasonable steps as Imperva may require from time to time to facilitate the provision of Usage Data to Imperva. **"Usage Data"** means data directly or indirectly related to items such as versioning, volumetrics, feature usage, traffic type, settings, telemetry and any other data (other than End User payload data) relating to the operation, support and/or about use of the Software by an End User and its authorized users.

**6. STANDARD SOFTWARE.**

All Software shall be Thales' standard Software. Thales shall have no obligation to create special or customized versions of any Software, or to ensure that the Software operates with End User's equipment, software, or systems. Thales reserves the right, without prior approval from or notice to End User, to make changes to any Software: (i) to meet published Documentation; (ii) that do not adversely affect the performance of the Software such that the functionality or performance is less than that specified in the published Documentation; or (iii) when required for purposes of safety. Thales also reserves the right to make changes to any Software without any obligation to make the same changes to Software previously ordered by or licensed to End User.

**7. POLICIES.**

**7.1 Security maintenance.**

Where Thales reasonably considers End User's use of the Software could (i) pose a security risk to Thales, the Software or any third party; (ii) adversely impact Thales' systems, the Software or the systems, traffic or data of any other Thales partner or customer; (iii) subject Thales, its partner, suppliers or any third party to liability, or (iv) be fraudulent, Thales shall have the right to suspend in whole or in part End User's rights to access or use the Software immediately upon notice. During any such suspension, End User shall remain responsible for all fees during the period of suspension.

**7.2 End of life policy.**

All Software that is a Thales Product is subject to Thales' then-current Cloud Protection and Licensing End of Life Policy (available [here](#) or such alternate URL or other repository as Thales may specify from time to time). All Software that is an Imperva Product is subject to Thales' then current-End of Life Policy (available [here](#) or such alternate URL or other repository as Thales may specify from time to time).

**SUB-PART 3: DATA SECURITY**

**SUB-PART 3.3: APPLIANCE SPECIFIC TERMS AND CONDITIONS**

**THESE APPLIANCE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

**1. OVERVIEW.**

1.1 This section sets out the terms specific to Appliances only.

1.2 In respect of Third Party Products, End User shall be bound by the Third Party Terms.

**2. THALES PRODUCTS: DELIVERY, RISK AND TITLE**

2.1 Unless otherwise agreed by Thales in the Order Acknowledgment, delivery of Thales Products shall be F.C.A. (Incoterms 2020) at Thales's nominated facility.

2.2 Title to the Thales Products, and risk of damage or loss, shall pass to End User upon delivery of the Thales Products at Thales's nominated facility to the carrier for shipment to End User, as applicable.

2.3 Acceptance of the Thales Products shall occur upon delivery to the common carrier.

2.4 Thales will select the carrier of its choice, but in no event will Thales assume any liability in connection with the shipment, nor shall the carrier be considered an agent of Thales. Thales, in its sole discretion, may ship "collect", prepaid or subject to invoice payment terms.

2.5 Delivery dates specified in any Documentation, the Order or Order Acknowledgement are estimates only and shall not be binding on Thales, and the time of delivery is not of the essence. Thales shall not have any liability for damages or losses sustained by Purchaser as a result of (i) delivery dates or times not being met; (ii) any delay in delivery of the Products that is caused by a Force Majeure event; or (iii) End User's failure to provide Thales with adequate delivery instructions or any other instructions that are relevant to the supply of the Products.

2.6 Except as provided herein, Thales shall have no responsibility to store any Thales Products for End User except as may be required during manufacturing or processing. Thales reserves the right to make deliveries of Products in instalments, and any delay in delivery, or other default of any instalment of any one or more products, shall not relieve End User of its obligation to accept and pay for the remaining deliveries. If delivery is delayed due to End User, Thales may store the Thales Products at End User's risk and issue an invoice for the Thales Product as if it had been delivered.

**3. IMPERVA PRODUCTS: DELIVERY, RISK AND TITLE.**

3.1 If Thales is providing Imperva Products to the End User in accordance with these Appliance Specific Terms and Conditions set out in this Sub-part 3.3, Thales shall use commercially reasonable efforts to Deliver the Imperva Appliances in accordance with

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

any reasonable delivery times requested in accepted Orders (in partial or full shipments). Provided Thales has used commercially reasonable efforts to Deliver the Imperva Appliances in accordance with any such requested delivery times, Thales shall in no event be liable for any delay in Delivery or for failure to give notice of delay. Imperva Appliances shall be deemed accepted by End User upon Delivery.

- 3.2 Risk of loss and, if applicable, title to Imperva Appliances shall pass to End User upon Delivery; provided that title shall not pass to End User for:

- (a) any Software contained in or installed on such Imperva Appliances; or
- (b) any Imperva Appliances for which End User has not purchased outright and paid for in full.

- 3.3 Imperva Appliances shall be delivered Ex Works (Incoterms 2020) to Imperva's designated manufacturing facility.

- 3.4 End User may specify shipping instructions with the Order, which are subject to Thales' acceptance. In the absence of specific shipping instructions from End User, which have been agreed to by Thales, Thales shall ship by the method it deems appropriate.

- 3.5 End User shall pay and be exclusively liable for all costs associated with shipping and delivery including without limitation, freight, shipping, customs charges and expenses, cost of special packaging or handling and insurance premiums.

- 3.6 In its discretion, Thales may advance shipping charges on behalf of End User on Appliances shipped to End User, and End User agrees to reimburse Thales for any such advanced charges and expenses.

## **4. SOFTWARE.**

- 4.1 End User acknowledges that the Software included with the Appliance is licensed, and not sold, with the applicable license terms set out in Sub-Part 3.2 of this Agreement.

- 4.2 Software is licensed solely in conjunction with such Appliance (and not separately or apart from such Appliance). If End User sells, leases, lends, rents, distributes or otherwise transfers any Appliance to any third party or if Thales terminates this Agreement or any relevant Order, then End User shall erase all Software from such Appliance.

## **5. MAINTENANCE AND SUPPORT.**

- 5.1 If Thales is providing Imperva Products to the End User in accordance with these Appliance Specific Terms and Conditions set out in this Sub-part 3.3, maintenance and support are provided in accordance with the Customer Support Guide.

- 5.2 If Thales is providing Thales Products to the End User in accordance with these Appliance Specific Terms and Conditions set out in this Sub-part 3.3, Support Services

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

are subject to the Support Services Terms and Conditions set out at Sub-part 5.4 of this Agreement.

### 6. WARRANTY.

- 6.1 Thales warrants that during a one (1) year period commencing on the date of first Delivery, the Appliances shall perform substantially in accordance with the Documentation. In the event Thales determines that the Appliances are in a breach of the warranty in this Section 6.1, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, following the return of such Appliance by End User, either repair the Appliance or replace the Appliance with a new or reconditioned Appliance that performs substantially in accordance with the Documentation. This warranty extends only to the original purchaser of the Appliance and shall not apply where there has been damage to the Appliance returned to Thales. For clarity, any Software pre-installed in the Appliance is subject to the warranty set forth in Section 1.2 of Sub-part 3.2.
- 6.2 Warranty claims must be made in writing during the warranty period accompanied by evidence of the defect satisfactory to Thales together with any available details that may reasonably assist Thales to reproduce the noncompliance and effect a cure. All returns must comply with Thales' then-current return material authorization policy set forth in the Support Terms. If End-User receives a replacement unit of the Appliance, End-User may retain such Appliance, at Thales' option, in full satisfaction of any replacement remedy provided herein. Thales' obligations under this express warranty are subject to Thales' examination of the Appliance and Thales' determination to its reasonable satisfaction that the claimed defect or fault actually exists, and is not excluded from this warranty. If Thales determines that the Appliance is not defective or faulty within the terms of this warranty, End User shall be liable for all costs of handling, transportation and repairs at Thales' then prevailing repair rates.
- 6.3 This warranty is conditioned upon payment of the purchase invoice and proper use of the Appliances, in accordance with the Documentation or any other instructions or manuals issued by Thales. Thales shall have no obligation under this Warranty unless End-User promptly notifies Thales in writing of any failures within the applicable warranty periods. This warranty extends only to the End-User.
- 6.4 This warranty shall not apply to Appliances that have been: (i) improperly installed, modified or repaired by anyone other than Thales; (ii) used in a manner other than as authorized under the Documentation applicable to the Appliance purchased; (iii) installed, operated or maintained not in accordance with the instructions supplied by Thales, including but not limited to the installation, operation or maintenance of the Appliances on any hardware, operating system or tools (including their specific configurations) that are not compatible with the Appliances; (iv) modified, altered or repaired by a party other than Thales or a party authorized by Thales; (v) operated or maintained in unsuitable environmental conditions, or by any other cause external to the Appliances or otherwise beyond Thales' reasonable control, including any extreme power surge or failure or electromagnetic field, rough handling during transportation, fire or other act of God; (vi) use of the Appliances with telecommunication interfaces other than those supplied or approved by Thales not meeting or not maintained in accordance with Thales' specifications as described in the Documentation, unless Thales has specifically agreed in writing to include such modifications within the scope

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

of this Agreement; (vii) damaged due to failure of power, air conditioning or humidity control, or failures of storage media not furnished by Thales or for consumable operating supplies or accessories outside the parameters designated in the Documentation or elsewhere, unless specifically included in this Agreement; (viii) subjected to accident, unusual physical, electrical or electromagnetic stress, neglect, or misuse fault or negligence of Purchaser, its employees, agents, contractors or visitors, operator error; or (ix) where the serial numbers, warranty data or quality assurance decals on the Appliances are removed or altered. Thales's warranty does not apply to (i) products manufactured by third parties and resold by Thales without re-marking under Thales's trademarks, (ii) software products that are not developed by Thales, and (iii) consumable items (e.g. batteries).

### **7. STANDARD APPLIANCES.**

All Appliances shall be Thales' standard Appliances. Thales shall have no obligation to create special or customized versions of any Appliances, or to ensure that the Appliances operate with End User's equipment, software, or systems. Thales reserves the right, without prior approval from or notice to End User, to make changes to any Appliances: (i) to meet published Documentation; (ii) that do not adversely affect the performance of the Appliances such that the functionality or performance is less than that specified in the published Documentation; or (iii) when required for purposes of safety. Thales also reserves the right to make changes to any Appliances without any obligation to make the same changes to Appliances previously ordered by or licensed to End User.

## **SUB-PART 3: DATA SECURITY**

### **SUB-PART 3.4: EVALUATION SPECIFIC TERMS AND CONDITIONS**

**THESE EVALUATION SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS AND THE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND / OR SOFTWARE SPECIFIC TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE EVALUATION SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. APPLICABLE TERMS AND CONDITIONS.**

- 1.1 From time to time, Thales may make available Evaluation Products to End User on a temporary basis for evaluation purposes, pursuant to an Order or otherwise. This Sub-Part 3.4 shall not apply to Appliances which are subject to a separate written agreement.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

### 1.2 Where an End User utilises an Evaluation Product:

1.2.1 for Cloud Services the following Sections of the Cloud Specific Terms and Conditions set out in Sub-Part 3.1 of this Agreement shall not apply: 1.1 and in Annex 1 to Sub-Part 3.1, Section 2;

1.2.2 for Software the following Sections of the Software Specific Terms and Conditions set out in Sub-Part 3.2 of this Agreement shall not apply: 1.1 and 1.2; and

1.2.3 the following Sections of the General Terms and Conditions shall not apply: 6, 7 and 9.

## 2. EVALUATION LICENSE.

Where Thales agrees to make an Evaluation Product available to an End User, Thales grants to End User during the Evaluation Period, a cost-free, non-sublicensable, non-transferable, non-assignable and non-exclusive, revocable at will license to use the Evaluation Product, solely at the location identified in writing by End User and solely for End User's internal evaluation of the Evaluation Product ("**Evaluation License**"). This Evaluation License does not include any rights to copy, alter, modify, reverse engineer, decompile, disassemble, make derivative works of, rent, lease, disclose, sublicense, or otherwise transfer the Product, related documentation, or other proprietary information of Thales. Thales will not provide any support or maintenance services with respect to the Product.

## 3. RESTRICTIONS ON USE.

The End User acknowledges that the Product and its related documentation will not be used in any way except as permitted by this Agreement, and except as explicitly permitted herein, will not be disclosed to any third party without Thales' prior written consent.

## 4. EVALUATION PERIOD.

4.1 Unless otherwise agreed to in writing, or terminated earlier in accordance with this Agreement, the term of the license to an Evaluation Product shall commence upon Delivery of the Evaluation Product and continue until the earlier of:

4.1.1 thirty (30) days from Delivery; or

4.1.2 the date that Thales provides written notice of termination to End User ("**Evaluation Period**").

4.2 Upon the expiration or termination of the Evaluation Period:

4.2.1 the Evaluation License shall cease;

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

4.2.2 End User shall immediately:

- (a) return the Evaluation Product to Imperva;
- (b) destroy or erase any intangible copies of the Evaluation Product; and
- (c) certify in a writing signed by an officer of End User and delivered to Thales that all such copies of have been returned, destroyed or erased.

## **5 WARRANTY.**

**NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, END USER ACKNOWLEDGES AND AGREES THAT THE EVALUATION PRODUCT IS PROVIDED FOR EVALUATION “AS-IS” AND THALES AND ITS SUPPLIERS MAKE NO REPRESENTATIONS, CONDITIONS OR**

**WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE EVALUATION PRODUCT, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, INFORMATIONAL CONTENT, SYSTEM INTEGRATION, ENJOYMENT, NONINFRINGEMENT OR ANY OTHER WARRANTIES ARISING OUT OF COURSE OF DEALING, USAGE OR TRADE.**

## **6 LIABILITY.**

**NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, IN NO EVENT SHALL THALES’ TOTAL AND AGGREGATE LIABILITY IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE EVALUATION PRODUCT EXCEED ONE HUNDRED DOLLARS (\$100).**

## **7 RETURN OR DESTRUCTION OF PRODUCT.**

If the End User wishes to purchase the Product following the Term, the End User may retain the Product and any related documentation, upon the submission of a purchase order for the Product or whilst the parties work in good faith to enter into a definitive agreement governing the purchase. In all circumstances, End User agrees to either destroy the Product (in the case of software) or return the Product to Thales without the requirement of demand and in good working order (excepting wear and tear from normal use with respect to hardware Product), to be received by Thales within ten (10) days of from the end of the Term (the “Return Date”), and in the case of destruction End User will send Thales a confirmation of such destruction signed by an authorized representative of End User within ten (10) business days from the end of the Term. Furthermore, if the Product includes software, the End User will immediately destroy or erase all copies of such software in its possession at the end of the Term. With

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

respect to any unreturned Product: 1) that has not been, a) communicated to Thales in writing (via email acceptable) of End User's intent to purchase the Product by the end of end of the Term, or b) not received by Thales by the Return Date; or 2) any Product returned in damaged condition (as determined at Thales' discretion), Thales will invoice End User electronically via email to End User's Email Address and/or mail the invoice, at Thales' discretion, to End User's Invoice Address specified below, and End User shall pay the list price for such Product applicable as of the Effective Date in accordance with the Thales issued invoice.

### PART 3: DATA SECURITY

#### SUB-PART 3.5: DATA PROTECTION AND SECURITY

## 1. OVERVIEW

1.1 This part of the Agreement is divided into the following sub-parts:

1.1.1 Where the Purchaser submits an Order for Imperva Products the Data Processing Addendum and the Security Addendum set out below, shall apply to the use of the applicable Imperva Products including all associated Services:

<a href="#"><u>Data Processing Addendum</u></a>
<a href="#"><u>Security Addendum</u></a>

1.1.2 Where the Purchaser submits an Order for Thales Products, the corresponding Data Processing Addendums set out below shall apply to the use of the applicable Thales Products including all associated Services:

<a href="#"><u>Data Protection on Demand Data Processing Addendum</u></a>
<a href="#"><u>Processing of Personal Data for Support Services for Thales Products Data Protection Agreement</u></a>

Version: 2 April 2025



## THALES CYBER SECURITY PRODUCTS END USER AGREEMENT

### PART 4: IDENTITY AND ACCESS MANAGEMENT SPECIFIC TERMS AND CONDITIONS

#### 1. OVERVIEW

1.1 This part of the Agreement is divided into the following sub-parts:

Product Area	Sub-part	Product Specific Terms and Conditions
Identity and Access Management	4.1	Cloud Services Specific Terms and Conditions
	4.2	Software Specific Terms and Conditions
	4.3	Hardware Specific Terms and Conditions
	4.4	Evaluation Specific Terms and Conditions
	4.5	CIAM Supplemental Terms and Conditions
	4.6	STA Supplemental Terms and Conditions
	4.7	IdCloud Supplemental Terms and Conditions

#### PART 4: IDENTITY AND ACCESS MANAGEMENT

SUB-PART 4.1: CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS

**THESE CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS GOVERN THE END USER'S ACCESS AND USE OF CLOUD SERVICES AND INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

**1. LICENCE TERMS.**

**1.1 Grant.**

Subject to End User's compliance with this Agreement, and upon acceptance of an Order or, where transacted via the Thales marketplace, completion of the Order by an End User, Thales grants End User a non-exclusive, non-transferable, non-sublicensable, revocable right, during the Term, to access and use the Cloud Services, in accordance with its corresponding Documentation, solely for End User's internal business purposes, subject to and up to the Licensed Volume and for the license term. In respect of Third Party Products, End User shall be bound by the Third Party Terms.

**2. WARRANTY, SUPPORT AND SLA.**

1.1 Thales warrants that during the term of the relevant Order, the Cloud Services shall perform substantially in accordance with the Documentation and in compliance with the SLA. In the event of a breach of this warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, correct the Cloud Services so that it performs substantially in accordance with the Documentation and, either directly issue or have an Authorized Third Party issue, any credits to which End User may be entitled pursuant to the SLA.

1.2 If Thales suspends the Cloud Services in accordance with Section 6 of Sub-part 4.1, then during any such suspension, End User shall remain responsible for all fees during the period of suspension and shall not be entitled to any service credits that would have otherwise arisen pursuant to SLA.

1.3 Support is provided in accordance with the Support Terms.

**3. ACCESS AND USE OF CLOUD SERVICES.**

3.1 To access the Cloud Services, End User is required to set up an account or complete an Order for each Cloud Service. End User is responsible for ensuring the accuracy of the

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

information required to set up the account. Thales' ability to deliver the Cloud Services depends upon End User's cooperation in setting up the account and on the accuracy of the information provided. If End User does not set up an account or if the information provided is inaccurate, Thales may not be able to perform the Cloud Services.

- 3.2 End User is responsible for the access to, and use of, the Cloud Services and for compliance with this Agreement, for which End User shall remain directly liable to Thales. End User will ensure that individuals which may access the Cloud Services maintain the confidentiality of login credentials and promptly notify Thales of any security breaches including compromise of accounts or credentials. Thales reserves the right to monitor End User's use of the Cloud Services from time to time to assess whether such usage is in accordance with this Agreement (including any agreed usage limits). Where such monitoring reveals that End User has exceeded any agreed usage limits, Thales reserves the right to additional Fees and End User shall pay such additional Fees to Thales at Thales's then current list price.
- 3.3 Thales engages in the constant evolution, innovation and improvement of its Cloud Services, and implements modifications that reflect new or enhanced features or functionalities. Thales may modify the features or functionalities of the Cloud Services provided that such modifications will not materially degrade the core functionality of the Cloud Services. Thales may discontinue the Cloud Services and will use commercially reasonable efforts to transfer End User to a substantially similar Cloud Service. If Thales does not have a substantially similar Cloud Service, Thales will refund to End User or Authorized Third Party the unused portion of any prepaid fee for End User's Cloud Service. Thales may notify End User of its actions pursuant to this section, provided that End User subscribed to receive such notification.
- 3.4 End User is responsible for ensuring the individuals using the Cloud Services comply with such acceptable use provisions relating to the Cloud Services as Thales may specify from time to time. Thales reserves the right to, without liability or prejudice to its other rights or remedies, disable any End User access to all or part of the Cloud Services in the event it reasonably suspects a breach of such acceptable use provisions. Thales shall notify the End User of its intention to disable any credentials pursuant to this Section before it disables such credentials.
- 3.5 Except as explicitly set out in this Agreement, End User is solely responsible for acquiring and maintaining all of the equipment, software, services and items necessary to access and make use of the Cloud Services including without limitation paying all fees, charges, taxes, and other costs related to internet access and for configuration changes that may be required to route activity to the Cloud Services. End User may access the Cloud Services only through the interfaces and protocols provided or authorized by Thales and agrees to set up, maintain and use the Cloud Services in strict compliance with Thales' and its Authorized Third Party's instructions.
- 3.6 Except to the extent set out in the Documentation, and where configuration is in accordance with the express requirements of the Documentation, use of the Cloud Services in conjunction with third party products is at End User's own risk.
- 3.7 End User acknowledges that Thales does not control the transfer of data over communications facilities, including the internet, and that the subscription may be

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

subject to limitations, delays, and other problems inherent in the use of such communications facilities.

- 3.8 Thales may anonymously compile statistical information related to the performance of the Products for purposes of improving the Products, for statistical purposes, and for compliance verification provided that such information does not identify End User data or End User's name.

### **4. EVALUATION SERVICES.**

Thales may offer Cloud Services as Evaluation Products. Any such use shall be pursuant to the terms of Sub-Part 4.4 of this Agreement.

### **5. COMPLIANCE WITH LAWS.**

End User is solely responsible for and will comply with all laws or regulations of any governmental entity or authority applicable to End User's access or use of the Cloud Services.

### **6. SUSPENSION OF THE CLOUD SERVICES.**

Thales may suspend End User's access to the Cloud Services in whole or part immediately and without any liability should Thales reasonably determine that End User's use of the Cloud Services: (i) is in breach of this Agreement, (ii) poses a security risk to Thales, the Cloud Services or any third party; (iii) may adversely impact Thales's systems, the Cloud Services or the systems, traffic or data of any other Thales partner or customer; (iv) subject Thales, its partner, suppliers or any third party to liability, (v) be fraudulent, or (vi) as otherwise required by laws or regulations of any governmental entity or authority. During any such suspension, End User shall remain responsible for all fees during the period of suspension and shall not be entitled to any service credits that would have otherwise arisen pursuant to the SLA.

## **PART 4: IDENTITY AND ACCESS MANAGEMENT**

### **SUB-PART 4.2: SOFTWARE SPECIFIC TERMS AND CONDITIONS**

**THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

## **1. LICENSE TERMS.**

### **1.1 Grant.**

- (a) Subject to End User's compliance with this Agreement, and upon acceptance of an Order, Thales grants End User a non-exclusive, non-transferable, non-sublicensable, revocable license to use the Software, in accordance with its corresponding Documentation, solely for End User's internal business purposes, on the Hardware (where applicable), subject to and up to the Licensed Volume, and for the license term, each as described in the relevant Quote.
- (b) If End User receives a license to the Software pursuant to this Agreement on a standalone basis, the license granted in this Section shall include the right to copy the Software up to the Licensed Volume.

### **1.2 Warranty.**

Thales warrants that during the sixty (60) day period commencing on the date of first Delivery, the Software shall perform substantially in accordance with the Documentation. In the event of a breach of the foregoing warranty, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, either replace the Software with Software conforming to the warranty in this Section 1.2, or use reasonable efforts to modify the Software so that it performs substantially in accordance with the Documentation. The rights and remedies granted to End User under this Section state Thales' entire liability, and End User's exclusive remedy, with respect to any breach of the warranty set out in this Section.

## **2. DELIVERY.**

### **2.1 Delivery.**

Upon acceptance of an Order, Thales shall use commercially reasonable efforts to Deliver any Software license keys that may be required to use the Software in accordance with the Documentation for the duration of the Order. Direct Orders shall be Delivered to End User and Orders via an Authorized Third Party shall be Delivered via the Authorized Third Party. Software shall be deemed accepted by End User upon Delivery.

### **2.2 Delay.**

Provided that Thales has used commercially reasonable efforts, Thales shall in no event be liable for any delay in Delivery or for failure to give notice of delay.

### **3. MAINTENANCE AND SUPPORT.**

Maintenance and support are provided in accordance with the Support Terms.

### **4. DATA RECOVERY.**

End User is solely responsible for End User's data back-up, data recovery, and disaster recovery measures. Thales shall not be responsible for End User's internal processes and procedures to ensure the protection of End User's data or information stored within End User's own environment. End User shall maintain an unmodified copy of all Software and all related Documentation, archival files and configuration files necessary to reinstall, reconfigure or reconstruct any lost, altered or damaged Software. Upon termination or discontinuation for any reason or for any non-renewal, Thales may delete all information, keys, certificates, user material and/or any other data or information related to End User's use of the Products and may discontinue End User's access to and use of the Services.

### **5. AUDIT**

- 5.1 In addition to the audit provisions set out in Section 5 of Part 1 (General Terms and Conditions) of this Agreement, the following audit terms shall apply to Software.
- 5.2 Upon Thales' written request, End User shall conduct a review of use of the Software and certify to Thales in a written instrument signed by an authorized representative of End User that it is in full compliance with this Agreement and, in particular, that it is not using more than the Licensed Volume. In the event of non-compliance, End User shall immediately remedy such non-compliance and provide Thales with written notice signed by the authorized representative to confirm the same. End User shall provide Thales with all access and assistance as Thales reasonably requests to further evaluate and remedy such noncompliance.
- 5.3 If the audit or any of the measures taken or implemented under this Section 5, determines that the End User's use of the Software exceeds the Licensed Volume:
  - (a) End User shall, within thirty (30) days following the date of such determination by Thales, pay to Thales or the relevant Authorized Third Party the retroactive fees for such excess use at the then-current rates for such licenses;
  - (b) If the use exceeds the Licensed Volume by more than ten percent (10%), End User shall pay Thales' reasonable costs incurred in conducting the audit; and
  - (c) If the use exceeds the Licensed Volume by more than twenty percent (20%), Thales may terminate this Agreement and the license to the Software, effective immediately upon written notice to End User.
- 5.4 Thales's remedies set forth in this Section 5 are cumulative and are in addition to, and not in lieu of, all other remedies the Thales may have at law or inequity.

## **5. POLICIES.**

### **5.1 Security maintenance.**

Where Thales reasonably considers End User's use of the Software could (i) pose a security risk to Thales, the Software or any third party; (ii) adversely impact Thales' systems, the Software or the systems, traffic or data of any other Thales partner or customer; (iii) subject Thales, its partner, suppliers or any third party to liability, or (iv) be fraudulent, Thales shall have the right to suspend in whole or in part End User's rights to access or use the Software (including any Support Services) immediately upon notice. During any such suspension, End User shall remain responsible for all fees during the period of suspension.

### **5.2 End of life policy.**

All Software is subject to Thales' then-current End of Life Policy (available [here](#) or such alternate URL or other repository as Thales may specify from time to time).

### **5.3 Usage data.**

Thales may anonymously compile statistical information related to the performance of the Products for purposes of improving the Products, for statistical purposes, and for compliance verification provided that such information does not identify End User data or End User's name.

## **PART 4: IDENTITY AND ACCESS MANAGEMENT**

### **SUB-PART 4.3: HARDWARE SPECIFIC TERMS AND CONDITIONS**

**THESE HARDWARE SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. OVERVIEW.**

- 1.1 This section sets out the terms specific to Hardware only.
- 1.2 In respect of Third Party Products, End User shall be bound by the Third Party Terms.

#### **2. DELIVERY, RISK AND TITLE**

- 2.1 Unless otherwise agreed by Thales in the Order Acknowledgment, delivery of Thales Products shall be F.C.A. (Incoterms 2020) at Thales's nominated facility.
- 2.2 Title to the Thales Products, and risk of damage or loss, shall pass to End User upon delivery of the Thales Products at Thales's nominated facility to the carrier for shipment to End User, as applicable.
- 2.3 Acceptance of the Thales Products shall occur upon delivery to the common carrier.
- 2.4 Thales will select the carrier of its choice, but in no event will Thales assume any liability in connection with the shipment, nor shall the carrier be considered an agent of Thales. Thales, in its sole discretion, may ship "collect", prepaid or subject to invoice payment terms.
- 2.5 Delivery dates specified in any Documentation, the Order or Order Acknowledgement are estimates only and shall not be binding on Thales, and the time of delivery is not of the essence. Thales shall not have any liability for damages or losses sustained by Purchaser as a result of (i) delivery dates or times not being met; (ii) any delay in delivery of the Products that is caused by a Force Majeure event; or (iii) End User's failure to provide Thales with adequate delivery instructions or any other instructions that are relevant to the supply of the Products.
- 2.6 Except as provided herein, Thales shall have no responsibility to store any Thales Products for End User except as may be required during manufacturing or processing. Thales reserves the right to make deliveries of Products in instalments, and any delay in delivery, or other default of any instalment of any one or more products, shall not relieve End User of its obligation to accept and pay for the remaining deliveries. If

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

delivery is delayed due to End User, Thales may store the Thales Products at End User's risk and issue an invoice for the Thales Product as if it had been delivered.

### **3. SOFTWARE.**

- 3.1 End User acknowledges that the Software included with the Hardware is licensed, and not sold, with the applicable license terms set out in Sub-Part 4.2 of this Agreement.
- 3.2 Software is licensed solely in conjunction with such Hardware (and not separately or apart from such Hardware). If End User sells, leases, lends, rents, distributes or otherwise transfers any Hardware to any third party or if Thales terminates this Agreement or any relevant Order, then End User shall erase all Software from such Hardware.

### **4. MAINTENANCE AND SUPPORT.**

- 4.1 Support Services are provided in accordance with the Support Terms.

### **5. WARRANTY.**

- 5.1 Thales warrants that during a one (1) year period commencing on the date of first Delivery, the Hardware shall perform substantially in accordance with the Documentation. In the event Thales determines that the Hardware are in a breach of the warranty in this Section 5.1, as End User's sole and exclusive remedy, Thales shall, at its sole expense and discretion, following the return of such Appliance by End User, either repair the Appliance or replace the Appliance with a new or reconditioned Appliance that performs substantially in accordance with the Documentation. This warranty extends only to the original purchaser of the Appliance and shall not apply where there has been damage to the Appliance returned to Thales. For clarity, any Software pre-installed in the Appliance is subject to the warranty set forth in Section 1.2 of Sub-part 4.2.
- 5.2 Warranty claims must be made in writing during the warranty period accompanied by evidence of the defect satisfactory to Thales together with any available details that may reasonably assist Thales to reproduce the noncompliance and effect a cure. All returns must comply with Thales' then-current return material authorization policy set forth in the Support Terms. If End-User receives a replacement unit of the Appliance, End-User may retain such Appliance, at Thales' option, in full satisfaction of any replacement remedy provided herein. Thales' obligations under this express warranty are subject to Thales' examination of the Appliance and Thales' determination to its reasonable satisfaction that the claimed defect or fault actually exists, and is not excluded from this warranty. If Thales determines that the Appliance is not defective or faulty within the terms of this warranty, End User shall be liable for all costs of handling, transportation and repairs at Thales' then prevailing repair rates.
- 5.3 This warranty is conditioned upon payment of the purchase invoice and proper use of the Hardware, in accordance with the Documentation or any other instructions or manuals issued by Thales. Thales shall have no obligation under this Warranty unless End-User promptly notifies Thales in writing of any failures within the applicable warranty periods. This warranty extends only to the End-User.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 5.4 This warranty shall not apply to Hardware that have been: (i) improperly installed, modified or repaired by anyone other than Thales; (ii) used in a manner other than as authorized under the Documentation applicable to the Appliance purchased; (iii) installed, operated or maintained not in accordance with the instructions supplied by Thales, including but not limited to the installation, operation or maintenance of the Hardware on any hardware, operating system or tools (including their specific configurations) that are not compatible with the Hardware; (iv) modified, altered or repaired by a party other than Thales or a party authorized by Thales; (v) operated or maintained in unsuitable environmental conditions, or by any other cause external to the Hardware or otherwise beyond Thales' reasonable control, including any extreme power surge or failure or electromagnetic field, rough handling during transportation, fire or other act of God; (vi) use of the Hardware with telecommunication interfaces other than those supplied or approved by Thales not meeting or not maintained in accordance with Thales' specifications as described in the Documentation, unless Thales has specifically agreed in writing to include such modifications within the scope of this Agreement; (vii) damaged due to failure of power, air conditioning or humidity control, or failures of storage media not furnished by Thales or for consumable operating supplies or accessories outside the parameters designated in the Documentation or elsewhere, unless specifically included in this Agreement; (viii) subjected to accident, unusual physical, electrical or electromagnetic stress, neglect, or misuse fault or negligence of Purchaser, its employees, agents, contractors or visitors, operator error; or (ix) where the serial numbers, warranty data or quality assurance decals on the Hardware are removed or altered. Thales's warranty does not apply to (i) products manufactured by third parties and resold by Thales without re-marking under Thales's trademarks, (ii) software products that are not developed by Thales, and (iii) consumable items (e.g. batteries).

## **6. STANDARD APPLIANCES.**

All Hardware shall be Thales' standard Hardware. Thales shall have no obligation to create special or customized versions of any Hardware, or to ensure that the Hardware operate with End User's equipment, software, or systems. Thales reserves the right, without prior approval from or notice to End User, to make changes to any Hardware: (i) to meet published Documentation; (ii) that do not adversely affect the performance of the Hardware such that the functionality or performance is less than that specified in the published Documentation; or (iii) when required for purposes of safety. Thales also reserves the right to make changes to any Hardware without any obligation to make the same changes to Hardware previously ordered by or licensed to End User.

## PART 4: IDENTITY AND ACCESS MANAGEMENT

### SUB-PART 4.4: EVALUATION SPECIFIC TERMS AND CONDITIONS

**THESE EVALUATION SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS AND THE SOFTWARE SPECIFIC TERMS AND CONDITIONS AND / OR INFRASTRUCTURE SPECIFIC TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE EVALUATION SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### 1. APPLICABLE TERMS AND CONDITIONS.

- 1.1 From time to time, Thales may make available Evaluation Products to End User on a temporary basis for evaluation purposes, pursuant to an Order or otherwise. This Sub-Part 4.4 shall not apply to Hardware which are subject to a separate written agreement.
- 1.2 Where an End User utilises an Evaluation Product:
  - 1.2.1 for Cloud Services the following Sections of the Cloud Specific Terms and Conditions set out in Sub-Part 4.1 of this Agreement shall not apply: 1.1 and in Annex 1 to Sub-Part 4.1, Section 2;
  - 1.2.2 for Software the following Sections of the Software Specific Terms and Conditions set out in Sub-Part 4.2 of this Agreement shall not apply: 1.1 and 1.2; and
  - 1.2.3 the following Sections of the General Terms and Conditions shall not apply: 6, 7 and 9.

#### 2. EVALUATION LICENSE.

Where Thales agrees to make an Evaluation Product available to and End User, Thales grants to End User during the Evaluation Period, a cost-free, non-sublicensable, non-transferable, non-assignable and non-exclusive, revocable at will license to use the Evaluation Product, solely at the location identified in writing by End User and solely for End User's internal evaluation of the Evaluation Product ("**Evaluation License**"). This Evaluation License does not include any rights to copy, alter, modify, reverse engineer, decompile, disassemble, make derivative works of, rent, lease, disclose, sublicense, or otherwise transfer the Product, related documentation, or other proprietary information of Thales. Thales will not provide any support or maintenance services with respect to the Product.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **3. RESTRICTIONS ON USE.**

The End User acknowledges that the Product and its related documentation will not be used in any way except as permitted by this Agreement, and except as explicitly permitted herein, will not be disclosed to any third party without Thales' prior written consent.

### **4. EVALUATION PERIOD.**

4.1 Unless otherwise agreed to in writing, or terminated earlier in accordance with this Agreement, the term of the license to an Evaluation Product shall commence upon Delivery of the Evaluation Product and continue until the earlier of:

4.1.1 thirty (30) days from Delivery; or

4.1.2 the date that Thales provides written notice of termination to End User ("**Evaluation Period**").

4.2 Upon the expiration or termination of the Evaluation Period:

4.2.1 the Evaluation License shall cease;

4.2.2 End User shall immediately:

- (a) return the Evaluation Product to Thales;
- (b) destroy or erase any intangible copies of the Evaluation Product; and
- (c) certify in a writing signed by an officer of End User and delivered to Thales that all such copies of have been returned, destroyed or erased.

### **5 WARRANTY.**

**NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, END USER ACKNOWLEDGES AND AGREES THAT THE EVALUATION PRODUCT IS PROVIDED FOR EVALUATION "AS-IS" AND THALES AND ITS SUPPLIERS MAKE NO REPRESENTATIONS, CONDITIONS OR**

**WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE EVALUATION PRODUCT, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, INFORMATIONAL CONTENT, SYSTEM INTEGRATION, ENJOYMENT, NONINFRINGEMENT OR ANY OTHER WARRANTIES ARISING OUT OF COURSE OF DEALING, USAGE OR TRADE.**

**6 LIABILITY.**

**NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, IN NO EVENT SHALL THALES' TOTAL AND AGGREGATE LIABILITY IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE EVALUATION PRODUCT EXCEED ONE HUNDRED DOLLARS (\$100).**

**7 RETURN OR DESTRUCTION OF PRODUCT.**

If the End User wishes to purchase the Product following the Term, the End User may retain the Product and any related documentation, upon the submission of a purchase order for the Product or whilst the parties work in good faith to enter into a definitive agreement governing the purchase. In all circumstances, End User agrees to either destroy the Product (in the case of software) or return the Product to Thales without the requirement of demand and in good working order (excepting wear and tear from normal use with respect to hardware Product), to be received by Thales within ten (10) days of from the end of the Term (the "Return Date"), and in the case of destruction End User will send Thales a confirmation of such destruction signed by an authorized representative of End User within ten (10) business days from the end of the Term. Furthermore, if the Product includes software, the End User will immediately destroy or erase all copies of such software in its possession at the end of the Term. With respect to any unreturned Product: 1) that has not been, a) communicated to Thales in writing (via email acceptable) of End User's intent to purchase the Product by the end of end of the Term, or b) not received by Thales by the Return Date; or 2) any Product returned in damaged condition (as determined at Thales' discretion), Thales will invoice End User electronically via email to End User's Email Address and/or mail the invoice, at Thales' discretion, to End User's Invoice Address specified below, and End User shall pay the list price for such Product applicable as of the Effective Date in accordance with the Thales issued invoice.

**PART 4: IDENTITY AND ACCESS MANAGEMENT**

**SUB-PART 4.5: CIAM SUPPLEMENTAL TERMS AND CONDITIONS**

**THESE CIAM SUPPLEMENTAL TERMS AND CONDITIONS GOVERN THE END USER'S ACCESS AND USE OF THE CIAM PRODUCT, AND SHALL BE INCORPORATED WITHIN AND SUBJECT TO THE GENERAL TERMS AND**

**CONDITIONS CONTAINED AT PART 1 AND THE CLOUD SERVICES SPECIFIC  
TERMS AND CONDITIONS SET OUT IN SUB-PART 4.1.**

**1 CONTRACTING ENTITY**

For customers who already had a CIAM Order on 1 December 2023 via OneWelcome B.V., the Thales contracting entity shall continue as OneWelcome B.V. for each renewal order.

**2 AUTO-RENEWAL**

On Order will automatically renew for a period equal to the previous Order term unless either Party gives the other Party at least a sixty (60) days' prior written notice of non-renewal before the end of the relevant Order term.

**3 METERED BILLING**

Some CIAM features are charged based on the amount used. An Order may include a base price for a specific minimum amount of units for a resource ('minimum usage') with an additional fee for the units consumed beyond that minimum. If the amount of that resource used is more than the minimum usage, then End User will promptly inform Thales of the exact amount of the resource used and pay to Thales (or any Authorised Third Party) under the Agreement any additional fees for all use of that resource. Thales regularly measures the resource amounts used. If the amount as measured by Thales is higher than the minimum usage, then the higher number will apply and fees will be payable by End User in accordance with the amount of resources used.

**4 ACCESS CONTROLS**

End User will: (a) notify Thales immediately of any unauthorized use of any password or user id or any other known or suspected breach of security; (b) report to Thales immediately and use reasonable efforts to stop any unauthorized use of the Products that is known or suspected by the End User or its customers, and (c) not provide false identity information to gain access to or use the Products. Thales will not be liable for any loss of data or functionality caused directly or indirectly by any administrator.

## **5 REGULATED DATA**

End User shall not process through the Subscription any protected health information (“PHI”) as defined under the USA Health Insurance Portability and Accountability Act of 1996, as amended and supplemented from time to time

("HIPAA") or any cardholder data as defined under PCI-DSS ("Cardholder Data") unless (a) Customer has entered into an Order expressly permitting Customer to process PHI and/or Cardholder Data, as applicable; (b) Customer configures and operates the Services in accordance with any applicable Documentation; and (c) in the case of PHI, Customer has entered into a Business Associate Agreement with Thales. Thales will have no liability under the Agreement relating to PHI or Cardholder Data that is not processed in accordance with this Section notwithstanding anything in the Agreement, or in HIPAA or PCI-DSS (as applicable), or any other laws.

## **6 DPA**

The CIAM product is subject to the data processing agreement available [here](#) or such other URL as Thales may specify from time to time.

## **PART 4: IDENTITY AND ACCESS MANAGEMENT**

### **SUB-PART 4.6: STA SUPPLEMENTAL TERMS AND CONDITIONS**

**THESE STA SUPPLEMENTAL TERMS AND CONDITIONS GOVERN THE END USER’S ACCESS AND USE OF THE STA PRODUCT, AND SHALL BE INCORPORATED WITHIN AND SUBJECT TO THE GENERAL TERMS AND CONDITIONS CONTAINED AT PART 1 AND THE CLOUD SERVICES SPECIFIC TERMS AND CONDITIONS SET OUT IN SUB-PART 4.1.**

### **1. SECURITY CREDENTIAL AND SECURITY TOKENS**

1.1 In this Section 1, the following terms shall have the following meanings:

“**Security Credentials**” means the one-time password (OTP) produced by a Security Token, password, PIN, or digital certificate used to authenticate to the Products; and

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

**“Security Token”** means a hardware or software-based multi-factor authentication security device used to authenticate to the Products.

- 1.2 The End User is solely responsible for managing all Security Credentials and Thales assumes no responsibility for the supervision, management, or control of End User’s Security Credentials. Thales assumes no responsibility and disclaims all liability for (a) any fraudulent access to and/or use of the Products, (b) any access to and/or use of the Products or any portion of them in violation of this Agreement, and (c) End User’s use of, or failure to protect, the Security Credentials.
- 1.3 If any Security Token is lost, damaged, stolen, or compromised, End User shall report these incidents immediately to the End User’s administrator to take the appropriate action including, but not limited to, disabling, changing, or replacing the affected Security Token. With respect to Security Tokens purchased from Thales or through an Authorized Third Party, End User will not, and will not permit any third party to, (a) reverse engineer, disassemble, decompile, decode, or alter the Security Tokens or any of their technology or components; (b) make or use any copies of any Security Tokens; (c) use a Security Token with any product other than STA; (e) use the Services or any component thereof other than as part of the Services or in any way other than the purposes for which the Services are intended.
- 1.4 End User will ensure that individuals using the Security Tokens comply with this Section.

## 2. AUTO-RENEWAL

On Order will automatically renew for a period equal to the previous Order term unless either Party gives the other Party at least a sixty (60) days’ prior written notice of non-renewal before the end of the relevant Order term.

## 3. THIRD-PARTY SITES.

The Products may contain links to, or call the servers of, third-party websites or services that are not under

Thales’s control (**“Third-Party Sites”**). As such, Thales is not responsible for, and doesn’t make any express or implied warranties with regard to, the information, content or other material, products, or services that are contained in, are accessible through, or the policies regarding the use and privacy of Third-Party Sites. Access to and use of Third-Party Sites, including information, content, material, products, and services on such websites or available through such websites, is solely at your risk.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **4. DATA COLLECTION.**

Thales may collect system data (excluding Personal Data) regarding your use of the Products and how the Products function to: (a) enhance and/or deliver the Products; (b) provide you the option of upgrades, new offerings, and enhancements to the Products; (c) for billing purposes including but not limited to usage-based billing; and (d) functioning of the Products for troubleshooting. You hereby consent to such collection activities and extension of offers from Thales or Authorized Third Party for upgrades, new offering, and enhancements.

### **5. STA DPA**

The STA product is subject to the data processing agreement available [here](#) or such other URL as Thales may specify from time to time.

## **PART 4: IDENTITY AND ACCESS MANAGEMENT**

### **SUB-PART 4.7: IDCLOUD SUPPLEMENTAL TERMS AND CONDITIONS**

#### **1. CONTRACTING ENTITY**

For customers who already had an IdCloud Order on or before 1 December 2023, the Thales contracting entity applicable to that order shall continue for each renewal Order unless and until Thales notifies you otherwise.

#### **2. IDCLOUD DPA**

The IdCloud Product is subject to the corresponding data processing agreement available below or such other URL as Thales may specify from time to time.

[IdCloud Access FIDO DPA](#)

[IdCloud Access OATH DPA](#)

[IdCloud Onboarding DPA](#)

[IdCloud Risk Management DPA](#)

Version: 2 April 2025



## **THALES CYBER SECURITY PRODUCTS END USER AGREEMENT**

### **PART 5: SERVICES SPECIFIC TERMS AND CONDITIONS**

#### **1. OVERVIEW**

1.1 This part of the Agreement is divided into the following sub-parts:

Sub-part 5.1	Packaged Services Specific Terms and Conditions
Sub-part 5.2	Scoped Services Specific Terms and Conditions
Sub-part 5.3	Training Specific Terms and Conditions
Sub-part 5.4	Support Services Specific Terms and Conditions

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **SUB-PART 5.1: PACKAGED SERVICES SPECIFIC TERMS AND CONDITIONS**

**THESE PACKAGED SERVICES SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE PACKAGED SERVICES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. SERVICE DESCRIPTION.**

- 1.1 Each Quote for Packaged Services contains a standard packaged offering and sets out the scope and term of such Packaged Services ("**Service Description**").
- 1.2 Within the Service Description, a fixed number of hours or Service Outcomes shall be set out, to be provided on a capped basis (either capped per week, month or other finite period of time or limited to the Service Outcomes within specified time period). Where a Service Description is time-based, unused hours shall not carry over to the next week or month and shall be deemed forfeited with no right of refund.
- 1.3 Packaged Services are limited to the activities set out in the Service Description and shall exclude hardware maintenance and repair, software maintenance and support, infrastructure, console, time and materials services, training services or any other activities not specifically described in the Service Description.
- 1.4 Packaged Services do not include any rights or entitlements to Products. Packaged Services are a distinct contractual entitlement from Products.

#### **2. OPERATIONAL MATTERS.**

##### **2.1 Remote only.**

All Packaged Services shall be provided remotely, unless otherwise expressly set out in the Service Description. Onsite services are available in Sub-part 5.2 of this Agreement.

##### **2.2 No custom development.**

No custom development shall take place in connection with any Packaged Services.

##### **2.3 End User dependencies.**

- 2.3.1 End User acknowledges that Thales is dependent on the cooperation of End User in order to provide Packaged Services.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

2.3.2 To the extent that End User fails to meet a dependency that Thales reasonably requires in order to provide Packaged Services, Thales shall be relieved of its obligations to provide Packaged Services.

2.3.3 For the purpose of this Section 2.3, Thales shall be deemed to be dependent on End User with respect to the following:

- (i) remote access and maintaining sufficient equipment and technology to facilitate Thales to provide the Packaged Services; and
- (ii) promptly providing Thales with such information as may be reasonably required to enable Thales to provide the Packaged Services.

### **3 WARRANTY AND DISCLAIMER.**

3.1 Thales warrants that the Packaged Services shall be performed in a professional and workmanlike manner.

3.2 In the event of a breach of Section 3.1, Thales shall at its sole option and expense, either:

- (a) re-perform the applicable Packaged Services in a manner that is compliant with such warranty; or
- (b) in the event Thales is unable to do so after using commercially reasonable efforts, terminate all or part of the applicable Packaged Services and upon such termination, Thales shall promptly refund End User all fees paid for the non-compliant Packaged Services.

3.3 The rights and remedies granted to End User under this Section 3 state Thales' entire liability, and End User's sole and exclusive remedy, with respect to any breach of the warranty set forth in this Section 3.

### **4 SERVICE COMMENCEMENT.**

4.1 All Packaged Services shall commence at a mutually agreed time between the parties, to take place as soon as reasonably possible following acceptance of the relevant Order.

4.2 If a Packaged Service is not fully utilized within twelve (12) months (or such shorter period set out in a Service Description) of the date of acceptance of the relevant Order, all unused Packaged Services shall be deemed forfeited without refund.

### **5. PERFORMANCE CONDITIONS.**

Thales will not be responsible for the loss or corruption of any End User data or for any system outage. Customer is responsible for creating backups of all End User data and scheduling system maintenance windows, as necessary for Thales to perform the Packaged Services.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

Thales will not be responsible for any application or host system access that encompasses coding, scripting, application analysis, system performance, troubleshooting, or applications logins outside of the services described in the applicable Service Description. Any and all future activity for trouble shooting, additions, or changes requested after End User's acceptance must be requested in writing by End User and is subject to a separate price quote. It is preferred that all technical inquiries are sent via email. Thales shall have five (5) business days from receipt of such inquiry to respond.

### **SUB-PART 5.2: SCOPED SERVICES SPECIFIC TERMS AND CONDITIONS**

**THESE SCOPED SERVICES SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SCOPED SERVICES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

#### **1. STATEMENT OF WORK.**

- 1.1 Where a Quote contains Scoped Services, the specific Scoped Services to be provided shall be set out in a Statement of Work which shall signed by duly authorized representatives of Thales and End User.
- 1.2 Scoped Services are limited to the activities set out in the Statement of Work and shall exclude hardware maintenance and repair, software maintenance and support, infrastructure, console, training services or any other activities not specifically described in the Statement of Work.
- 1.3 Scoped Services do not include any rights or entitlements to Products. Scoped Services are a distinct contractual entitlement from Products.
- 1.4 Unless otherwise specified in the Agreement, all dates and times for the provision of the Scoped Services are estimates only and time shall not be of the essence for the performance of the Scoped Services. Thales shall not have any liability for delay or for any damages or losses sustained by Customer as a result of such dates or times not being met.

#### **2. OPERATIONAL MATTERS.**

##### **2.1 Acceptance.**

- 2.1.1 Unless otherwise set forth in the applicable SOW, Scoped Services shall be deemed accepted upon the execution of the Certificate of Completion by the Customer or within 5 days of delivery of the Certification of Completion, whichever is sooner. If the Deliverables and/or Scoped Services are to be

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

incrementally delivered or otherwise completed in phases, each phase shall be independently accepted or deemed accepted (as appropriate).

- 2.1.2 Unless otherwise set forth in the applicable SOW, Thales is not responsible for any future trouble shooting, additions or changes requested after final delivery of all Deliverables provided under the applicable SOW.

### **2.2 Remote default.**

The default position is that the Scoped Services shall be provided remotely. Should on-site services be required, End User shall pay Thales additional travel, lodging and sustenance expenses in accordance with Thales' then current rates, except where otherwise set out in a SOW. For on-site Scoped Services, End User shall:

- (a) provide Thales personnel with reasonable office space and necessary access to hardware and other systems; and
- (b) comply in all material respects with applicable laws relating to the treatment of Thales personnel who are on End User's premises.

### **2.3 No custom development.**

No custom development shall take place in connection with any Scoped Services.

### **2.4 End User dependencies.**

- 2.4.1 End User acknowledges that Thales is dependent on the cooperation of End User in order to provide Scoped Services.
- 2.4.2 To the extent that End User fails to meet a dependency that Thales reasonably requires in order to provide Scoped Services, Thales shall be relieved of its obligation to provide Scoped Services.
- 2.4.3 For the purpose of this Section 2.4, Thales shall be deemed to be dependent on End User with respect to the following:
- (a) remote access and maintaining sufficient equipment and technology to facilitate Thales to provide the Scoped Services; and
  - (b) promptly providing Thales with such information as may be reasonably required to enable Thales to provide the Scoped Services.

## **2. INVOICE AND PAYMENT.**

The following section applies only to Direct Orders for Scoped Services:

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 2.1 Scoped Services will be invoiced in accordance with the invoicing milestones provided by Thales, as applicable. Where there are no invoicing milestones details provided, Thales may invoice at such reasonable times as it deems appropriate. Unless expressly set out otherwise in a SOW, End User will pay the reasonable travel, living, and out-of-pocket expenses incurred by Thales.
- 2.2 Invoices shall be deemed accepted by End User upon receipt, unless End User advises Thales in writing of a material error within ten (10) days after receipt.
- 2.3 End User may not offset, defer or deduct any invoiced amounts that Thales determined are not erroneous following such period.
- 2.4 Amounts payable to Thales for Scoped Services are payable in full without deduction (net of applicable taxes, costs and expenses) and End User shall pay all such applicable taxes, costs and expenses (exclusive of taxes on Thales' net income) within thirty (30) days from the date of invoice in the method and currency identified. No discount for early payment is authorized.
- 2.5 All payments made by End User and any unused Scoped Services purchased by End User are non-refundable.
- 2.6 Thales may suspend or terminate any or all Scoped Services and refuse additional Orders until overdue amounts are fully paid by End User. Any late payment will bear interest at a rate of one percent (1%) per month, or such other lesser rate as may be required by applicable law. Thales reserves the right to withdrawn any credit advanced at any time.

### **3. WARRANTY AND DISCLAIMER.**

- 3.1 Thales warrants that the Scoped Services shall be performed in a professional and workmanlike manner.
- 3.2 In the event of a breach of Section 4.1, Thales shall at its sole option and expense, either:
  - (a) re-perform the applicable Scoped Services in a manner that is compliant with such warranty; or
  - (b) in the event Thales is unable to do so after using commercially reasonable efforts, terminate all or part of the applicable Scoped Services and upon such termination, Thales shall promptly refund End User all fees paid for the non-compliant Scoped Services.
- 3.3 The rights and remedies granted to End User under this Section 4 state Thales' entire liability, and End User's sole and exclusive remedy, with respect to any breach of the warranty set forth in this Section 4.

### **4. SERVICE COMMENCEMENT.**

- 4.1 All Scoped Services shall commence at a mutually agreed time between the parties as set forth in the Statement of Work.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 4.2 If a Scoped Service is not fully utilized within twelve (12) months of the date of acceptance of the relevant Order, all unused Scoped Services shall be deemed forfeited with no right to a refund.

## **5. CHANGE MANAGEMENT PROCESS.**

The parties may request, in writing, additions, deletions, or modifications to the Scoped Services described in the applicable SOW ("Change Request"). Thales shall have 3 business days from receipt of the Change Request from End User or an Authorized Partner to research and document the proposed change, and prepare a Change Request form. The raising of a Change Request may necessitate additional time for the completion of the existing scope of the Scoped Services. No change to the applicable SOW shall be made unless it is accepted by Thales in writing, signed by an authorized signatory. Thales will not perform or commence work in connection with any proposed change until (i) a Change Request form is approved and signed by Thales and either the End User, or the Authorized Partner, as applicable; and (ii) to the extent the fees associated with the Scoped Services have changed based on the Change Request, Thales has received a purchase order for such changes.

## **6. PERFORMANCE CONDITIONS.**

Thales will not be responsible for the loss or corruption of any End User data or for any system outage. End User is responsible for creating backups of all End User data and scheduling system maintenance windows, as necessary for Thales to perform the Scoped Services. Thales will not be responsible for any application or host system access that encompasses coding, scripting, application analysis, system performance, troubleshooting, or applications logins outside of the services described in the applicable SOW. Any and all future activity for trouble shooting, additions, or changes requested after End User's acceptance must be requested in writing by End User and subject to a separate price quote. It is preferred that all technical inquiries are sent via email. Thales shall have five (5) business days from receipt of such inquiry to respond.

## **SUB-PART 5.3: TRAINING SERVICES SPECIFIC TERMS AND CONDITIONS**

**THESE TRAINING SERVICES SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE TRAINING SERVICES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **1. SCOPE.**

The scope of the relevant Training Services is set forth in Thales' training catalog.

### **2. EXPIRATION OF TRAINING.**

Training Services shall be completed within twelve (12) months of the date an Order is accepted. If Training Services are not fully utilized within twelve (12) months of the date of acceptance of the relevant Order, all unused Training Services shall be deemed forfeited with no right to a refund.

### **3. COURSE CANCELLATION.**

- 3.1 If a student is unable to attend the class in which they are enrolled, please contact Thales in writing in advance. A substitute may attend that student's place, or the student can participate in a later session, subject to Section 2 above.
- 3.2 For all Thales hosted training, students may cancel their enrollment no later than twenty-five (25) business days prior to the course's start date. Students canceling fewer than twenty-five (25) business days prior to the course start date must pay for the course and are not entitled to a refund. Students are responsible for all travel, accommodation and other associate expenses.
- 3.3 Thales shall notify students of course cancellation at least ten (10) business days prior to the start of the course, and shall credit paid tuition towards a future training.
- 3.4 For all Thales private training, End Users must cancel their booking by emailing Thales no later than twenty (20) business days prior to the course's date. End Users cancelling their private booking fewer than twenty (20) business days prior to the course start date must pay travel related expenses incurred by Thales.
- 3.5 Thales reserves the right to cancel a course. In the event that Thales must cancel a course, Thales assumes no financial liability for any cancellation fees, including non-refundable airfare, hotel and rental costs.
- 3.6 Online e-learning courses are non-refundable and no cancellation is permitted.
- 3.7 Subscriptions are non-refundable and no cancellation is permitted.
- 3.8 On-line registrations: If a student is unable to attend the class in which they are enrolled, but prefers to schedule for a different session, the student may do so by un-enrolling from the course in the online system or by contacting [training@imperva.com](mailto:training@imperva.com). The student must re-enrol and complete the training within 60 days.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 3.9 Thales Private Training: Any rescheduling of training with less than 20 business days prior written notice to [cpltechnicaltraining@thalesgroup.com](mailto:cpltechnicaltraining@thalesgroup.com), shall be subject to a rescheduling fee of US\$2,500; the fee is subject to modification or increase at Thales' discretion.

## **4. LIMITED WARRANTY.**

**EXCEPT AS EXPRESSLY STATED HEREIN, THE TRAINING IS PROVIDED "AS IS" AND THALES MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. THALES HEREBY SPECIFICALLY DISCLAIMS, ON BEHALF OF ITSELF AND ITS PARTNERS AND SUPPLIERS, ALL IMPLIED WARRANTIES AND CONDITIONS, INCLUDING ANY WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. SAVE IN RESPECT OF THOSE LIABILITIES WHICH CAN NOT LEGALLY BE LIMITED, THALES (AND ITS SUPPLIERS OR PARTNERS) SHALL NOT BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, DIRECT, SPECIAL OR PUNITIVE DAMAGE, LOSS OR EXPENSES, BUSINESS INTERRUPTION, LOST BUSINESS, LOST PROFITS, LOST OPPORTUNITY, OR LOST SAVINGS, EVEN IF IT HAS BEEN ADVISED OF THEIR POSSIBLE EXISTENCE. NEITHER PARTY SHALL BE LIABLE FOR DELAYS OR FAILURE IN PERFORMANCE DUE TO CAUSES BEYOND ITS REASONABLE CONTROL.**

**SUB-PART 5.4: SUPPORT SERVICES SPECIFIC TERMS AND CONDITIONS**

**THESE SUPPORT TERMS APPLY TO SUPPORT SERVICES FOR THALES PRODUCTS PURCHASED BY END USER EITHER DIRECTLY OR THROUGH AN AUTHORIZED THIRD PARTY. THESE SUPPORT SERVICES SPECIFIC TERMS AND CONDITIONS INCORPORATE AND ARE SUBJECT TO THE GENERAL TERMS AND CONDITIONS. IN THE EVENT OF CONFLICT BETWEEN THESE SUPPORT SERVICES SPECIFIC TERMS AND CONDITIONS AND THE GENERAL TERMS AND CONDITIONS, THE GENERAL TERMS AND CONDITIONS SHALL PREVAIL.**

**1. PROVISION OF SUPPORT SERVICES.**

Subject to End User's timely payment of all fees owed to Thales, as applicable, Thales will provide Support Services to End User during the term of the relevant Order and at the support level purchased and confirmed by Thales in an Order Acknowledgment.

**2. SUPPORT PERIOD, EXPIRED SUPPORT SERVICES AND SUPPORT SERVICES RENEWAL.**

2.1 The Support Services shall commence and end as of the dates set forth in the Order Acknowledgement.

2.2 In the event of termination of Support Services, End User shall not be entitled to any refund for any unused portion of the fees or charges paid for Support Services.

2.3 In the event Support Services expire or are otherwise terminated: (i) any reinstatement of Support Services shall be purchased to cover the lapsed Support Services since expiration or cancelation, and must be renewed until the Support Services is current; and (ii) a reinstatement fee of 20% of the list price shall be charged by Thales to End User. In addition, End User shall warrant that as of the date of the Order for renewal that (to the best of its knowledge) all Products to which the Support Services apply are functioning correctly.

**3. SUPPORTED VERSIONS AND END OF LIFE.**

3.1 Unless otherwise specified by Thales, the provision of Support Services is limited to: (a) the current version; and (b) the immediately preceding version of the Product (where applicable). The Thales product-specific lifecycle policy and information defining currently supported versions is available upon request from Thales technical support team.

3.2 Thales will use commercially reasonable efforts to meet the response times in the Welcome Pack and herein. Access to the Support Help Center, e-mail or phone lines for the provision of Support Services may be suspended for brief periods due to scheduled maintenance and other factors.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **4. SUPPORT SERVICES.**

- 4.1 The available support levels and options and the Return Material Authorization policy are set forth in the Welcome Pack (specifically the ‘Thales client service support plans’ in the Documentation). Thales’ provision of Support Services is further subject to the information and disclaimers set forth the Thales product-specific lifecycle policy, available upon request from the Thales technical support team. During the term of an Order comprising Support Services, Thales will provide the following Support Services to End User in relation to the relevant Software:
- 4.1.1 Commercially reasonable efforts to investigate and resolve Failures reported by End User and confirmed by Thales in accordance with the priority level assigned to the Failure by Thales in its reasonable discretion. End User agrees that Thales may determine in its sole discretion that the only resolution may be upgrading to the most recent version of Thales’ Appliances, Hardware or Software.
- 4.1.2 Updating the Documentation as and when necessary.
- 4.1.3 The provision of generally available maintenance Software and Software release notes.
- 4.1.4 The provision, free of charge, during the term of an Order comprising Support Services, of generally available maintenance updates to the supported versions of the Software as and when available, in accordance with the support level purchased.
- 4.2 End User shall promptly download, distribute and install all Software maintenance updates as released by Thales during the term of an Order comprising Support Services. End User acknowledges that any failure to do so could result in End User’s inability to receive Support Services. Certain updates may require a Appliance or Hardware upgrade to function properly. Thales reserves the right to address support requirements in the future by migrating this product to a “form, fit, function” next-generation equivalent. ProtectFile and ProtectV are excluded from any term or maintenance agreements longer than 3 years.

### **5. EXCLUSIONS AND DISCLAIMERS.**

#### **5.1 CONDITIONS VOIDING SUPPORT SERVICES.**

For the avoidance of doubt, Thales will have no obligation to provide Support Services for any conditions attributable to:

- 5.1.1 use of the Products other than authorized by Thales or in accordance with Thales’ official specifications as found in the Documentation;
- 5.1.2 any accident, act of nature, unusual physical, electrical or electromagnetic stress, or by any other cause external to the Product or otherwise beyond Thales’ reasonable control, neglect, misuse, fault or negligence of End User, its employees, agents, contractors or visitors, operator error, or any other third party;

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

- 5.1.3 modifications, alteration or repairs made to the Product by a party other than Thales or a party authorized by Thales;
- 5.1.4 failure by End User to provide a suitable environment and operating conditions;
- 5.1.5 any customizable deliverables created by Thales or third-party service providers specifically for End User as part of professional services;
- 5.1.6 installation, operation or maintenance of the Products not in accordance with the instructions supplied by Thales, including but not limited to, installation, operation or maintenance of the Products on any hardware, operating system or tools (including their specific configurations) that are not compatible with the Products, as made available by Thales;
- 5.1.7 use of the Appliance, Hardware or Software with other hardware, software or telecommunication interfaces other than those supplied or approved by Thales or not meeting or not maintained in accordance with Thales' specifications as described in the Documentation, unless Thales has specifically agreed in writing to include such modifications within the scope of the Support Services; or
- 5.1.8 power, air conditioning or humidity controls, or to failures of storage media not furnished by Thales or for consumable operating supplies or accessories.

### **5.2 OTHER EXCLUSIONS.**

In addition, Thales shall have no obligation to:

- 5.2.1 create or modify custom business roles or reports, or support custom modification to databases, active server pages or other code, components or programs;
- 5.2.2 supply personnel to End User's premises;
- 5.2.3 provide software development or coding assistance or use of software developer tool kits to create or develop applications;
- 5.2.4 pay or reimburse End User for expenses relating to the import or export of Products, including custom clearances, inspection certificates, applications and license fees. Thales further disclaims any liability for delays resulting from an action by a government agency or from its failure to take timely action;
- 5.2.5 products in which the serial number, warranty data or quality assurance decals have been altered or removed; or
- 5.2.6 repair pre-existing defects in Products that are out of warranty.

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **5.3 ADDITIONAL COSTS.**

To the extent Thales reasonably determines that a Failure is caused by any condition that is not covered by Support Services pursuant hereto, Thales may charge End User Thales' then current hourly fees and costs associated with diagnosing and repairing such Failure.

## **6. END USER OBLIGATIONS.**

6.1 The End User shall:

- 6.1.1 promptly report any identified Failure to Thales by logging in the Support Help Center and submitting a request as described in the Welcome Pack, documenting it in sufficient detail for Thales to be able to recreate the Failure;
- 6.1.2 use the Product in accordance with the Documentation and promptly and regularly carry out all operator maintenance routines as and where specified;
- 6.1.3 use with the Product operating supplies and media which comply with Thales' recommendations;
- 6.1.4 permit only Thales or Thales' approved agents to adjust, repair, modify, maintain or enhance the hardware or software, save for any operator maintenance specified for Appliances or Hardware;
- 6.1.5 keep adequate back-up copies of the Product software, data, databases and application programs in accordance with best computing practice. End User agrees that it is solely responsible for any and all restoration and reconstruction of lost or altered files, data and programs;
- 6.1.6 consistently maintain the environmental conditions recommended by Thales;
- 6.1.7 permit the Products to be used or operated only by properly qualified operators in the employ of or under End User's control; and
- 6.1.8 install and implement all solutions, corrections, and new releases in accordance with Thales' installation instructions. End User acknowledges that failure to install such solutions, corrections, new releases may cause the Software to become unusable or non-conforming and may cause subsequent Failure corrections and updates to be unusable, including, without limitation, any updates provided pursuant hereto. Thales shall accept no liability for the performance of the Software in respect of Software that has not been installed in accordance with Thales' installation instructions.

## **7. ON-SITE WORK.**

Any provision by Thales of support and maintenance services on End User's premises are not included hereunder and shall be subject to a separate professional services agreement or statement of work.

## **8. END USER CONTROL AND RESPONSIBILITY**

8.1 The End User has and will retain sole responsibility for:

- 8.1.1 all information, instructions and materials provided by or on behalf of End User or any authorized user in connection with the Support Services;
- 8.1.2 End User's information technology infrastructure, including computers, software, databases, electronic systems (including database management systems) and networks, whether operated directly by End User or through the use of third-party services;
- 8.1.3 the security and use of End User's and its authorized users' access credentials; and
- 8.1.4 all access to and use of the Support Services and Products directly or indirectly by or through the End User's information technology infrastructure (as set out at Section 8.1.2 above) or its or its authorized users' access credentials, with or without End User's knowledge or consent, including all results obtained from, and all conclusions, decisions and actions based on, such access or use.

## **9. DISCLAIMER OF WARRANTIES**

- 9.1 **THALES WARRANTS THAT SUPPORT SERVICES WILL BE PERFORMED IN A PROFESSIONAL AND WORKMANLIKE MANNER. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF THALES EXCEED THE FEES PAID BY END USER FOR SUPPORT SERVICES IN THE 12 MONTHS PRECEDING THE DATE OF THE CLAIM. FOR PURPOSES OF THIS SECTION, A "CLAIM" SHALL MEAN, COLLECTIVELY ALL CAUSES OF ACTION, DAMAGES, CLAIMS OR DISPUTES OR SIMILAR REQUESTS FOR COMPENSATION THAT ARE RELATED TO OR ARISE FROM THIS AGREEMENT AND FROM A PARTICULAR EVENT, ACT, OMISSION, FAILURE OR ROOT CAUSE.**
- 9.2 **THALES SHALL ONLY HAVE LIABILITY FOR SUCH BREACHES OF WARRANTY IF END USER PROVIDES WRITTEN NOTICE OF THE BREACH TO THALES WITHIN THIRTY (30) DAYS OF THE PERFORMANCE OF THE APPLICABLE SUPPORT SERVICES.**
- 9.3 **NOTWITHSTANDING ANYTHING TO THE CONTRARY, IF END USER PURCHASES SUPPORT SERVICES AND MAINTENANCE SERVICES THROUGH AN AUTHORIZED PARTNER, THALES SHALL HAVE NO DIRECT LIABILITY TO END USER FOR ANY DAMAGES WHATSOEVER AND SHALL NOT BE REQUIRED TO INDEMNIFY END USER FOR ANY THIRD PARTY CLAIMS, INCLUDING, BUT NOT LIMITED TO, THOSE SET FORTH IN THIS SECTION.**
- 9.4 **THIS WARRANTY IS END USER'S EXCLUSIVE WARRANTY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THALES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED BY CUSTOM, TRADE USAGE OR OTHERWISE, INCLUDING, WITHOUT**

**LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. NO REPRESENTATION OR WARRANTY IS GIVEN THAT FAILURES (AS DEFINED HEREIN) WILL BE FIXED OR FIXED WITHIN A SPECIFIED PERIOD OF TIME.**

- 9.5 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THALES BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL LOSSES OR DAMAGES WHATSOEVER, OR FOR ANY LOSS OF GOODWILL, LOST PROFITS, LOSS OF BUSINESS OR LOST OPPORTUNITIES IN ANY WAY RELATING TO PROVIDING SUPPORT SERVICES, EVEN IF THALES HAS BEEN NOTIFIED OF, OR REASONABLY COULD HAVE FORESEEN, THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES OCCURRING, AND REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE.**

## ANNEX C

### Software Support & Maintenance Terms

#### Certificate Solutions and Identity & Access Management Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the “Support Schedule”), the Entrust General Terms and Conditions (“General Terms”) that are available at <https://www.entrust.com/general-terms.pdf>, and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

- 1.1. **“Covered Offering”** means each Hosted Service, Software, and third party software product resold or provided by Entrust, in each case, for which Entrust provides Support Services.
- 1.2. **“Customer-Hosted Offering”** means Covered Offerings that are hosted by Customer or installed on Customer’s premises.
- 1.3. **“Extended Support”** means the services which may be available from Entrust under a separate agreement or schedule for Superseded Products or non-standard support relating to reinstatement of Support Services.
- 1.4. **“Hosted Service”** for the purposes of this Schedule means Entrust’s Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.
- 1.5. **“Named Support Contacts”** means individual Users nominated by Customer to act as Customer’s support representatives.
- 1.6. **“Problem”** means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.
- 1.7. **“Production Environment”** means Customer’s live business environment with active users.
- 1.8. **“Response Time”** means the amount of time that elapses between the Customer’s report of a Service Request to Entrust and Entrust’s acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.
- 1.9. **“Service Plan”** means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.
- 1.10. **“Service Request”** means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 1.11. **“Software”** for the purposes of this Schedule means Identity Enterprise (formerly IdentityGuard), Identity Essentials, GetAccess, TransactionGuard, Entrust Certification Authority (formerly Security Manager), Administrative Services, CA Administration, CA Gateway, Certificate Hub, Certificate Enrollment Gateway, Entrust VA and TSA, KeyOne, Signing Automation Engine, Remote Signing Engine, Signing Automation Module, and any other Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.
- 1.12. **“Superseded Product”** means previous version(s) of Covered Offerings that are commercial software products.
- 1.13. **“Support Services”** means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.
- 1.14. **“Upgrade”** in the context of Covered Offerings that are commercial software products, means a subsequent release or version of the Covered Offering; Upgrade releases will be designated by a change in the release number.
2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.
3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.
4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.
5. **Support Fees.**
  - 5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.
  - 5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.
6. **Customer’s Responsibilities.**
  - 6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.
  - 6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust’s systems in association with Customer’s account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts conduct themselves at all times in a professional manner, and are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation. In the event that any Named Support Contact engages in hostile, violent or abusive language or behavior, Entrust shall have the right to suspend such individual’s access

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- to Support Services, without liability under the Agreement, and Customer shall be required to appoint a replacement Named Support Contact.
- 6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be classified as Severity 1 or Severity 2, it must make the Service Request by telephone.
- 6.4. When making a Service Request, Customer shall provide:
- 6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.
- 6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request
- 6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.
- 6.5. For Severity 1 Problems, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Problem. If no dedicated Customer resources are available, Entrust's obligations with respect to the Problem will be suspended until such time as such resources become available.
- 6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.
7. **Support Services.** Support Services include the following services:
- 7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:
- 7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;
- 7.1.2. download (where applicable) Covered Offerings; and
- 7.1.3. log, view and receive updates on Customer's Service Requests.
- 7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan.

### 7.3. Support for Third Party Products.

7.3.1. If Entrust provides Support Services for any third party software product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing ("Third Party Covered Offering"), Entrust will use commercially reasonable efforts to support such product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Covered Offering or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Covered Offering and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Covered Offering directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be classified as Severity 1 or Severity 2, it must report by telephone.

Severity 1	Production Environment server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced in a Production Environment. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Entrust shall make commercially reasonable efforts to respond to Service Requests within the target Response Times set out in the applicable Service Plan. In addition, Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. In the event of a Severity 1 or Severity 2 Service Request, Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Severity 1 or Severity 2 Service Requests. The resolution and correction of Severity 1 and Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

**Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

7.5.2. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

<b>Support Service</b>	<b>Silver Service Plan</b>	<b>Platinum Service Plan</b>
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	Support Business Week	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	Support Business Week (except for December 25 and January 1)	
Priority email handling:	No	Yes
Response Time target for reported Service Requests		
Severity 1	8 hours	4 hours
Severity 2	48 Support Business Week hours	24 Support Business Week hours
Severity 3	72 Support Business Week hours	48 Support Business Week hours

In the table above, “Support Business Week” means Sunday 20:00 to Friday 20:00 in the Eastern Standard (first Sunday in November to 2<sup>nd</sup> Sunday in March), or, when applicable, Eastern Daylight (2<sup>nd</sup> Sunday in March to 1<sup>st</sup> Sunday in November) time zone. The equivalence chart below is provided for convenience only:

Time Zone	1 <sup>st</sup> Sunday in November to 2 <sup>nd</sup> Sunday in March	2 <sup>nd</sup> Sunday in March to last Sunday in March	Last Sunday in March to Last Sunday in October	Last Sunday in October to 1st Sunday in November
Eastern Time (ET)	Sunday 20:00-Friday 20:00 (EST)	Sunday 20:00-Friday 20:00 (EDT)	Sunday 20:00-Friday 20:00 (EDT)	Sunday 20:00-Friday 20:00 (EDT)
British Time (BT)	Monday 1:00-Saturday 1:00 (GMT)	Monday 00:00-Saturday 00:00 (GMT)	Monday 1:00-Saturday 1:00 (BST)	Monday 00:00 - Saturday 00:00 (GMT)
Singapore Time (SGT)	Monday 9:00-Saturday 9:00	Monday 8:00-Saturday 8:00	Monday 8:00-Saturday 8:00	Monday 8:00-Saturday 8:00

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

### **8. Upgrades for Customer-Hosted Offerings.**

- 8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Covered Offerings generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.
- 8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

### **9. Exclusions.**

- 9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).
  - 9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.
  - 9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Covered Offerings, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.
10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.
11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support

## **Call-Off Schedule 6 (ICT Services)**

Call-Off Ref:

Crown Copyright 2018

Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support.



certificate-solutions-s  
upport-schedule.pdf

## **ANNEX D**

### **Software as a Service Terms**

#### **NOT USED**

## **Annex E**

### **As a Service Terms**

**NOT USED**