Crown
Commercial
Service

SECURITY GUIDANCE

SPEND ANALYTICS AND RECOVERY SERVICE II

REFERENCE NUMBER

RM3820

ATTACHMENT 6

CONTENTS

1. OFFICIAL-SENSITIVE 1
2. SECURITY GRADING 1
3. OFFICIAL SECRETS ACTS 1
4. PROTECTION OF OFFICIAL-SENSITIVE INFORMATION 2
5. ACCESS 2
6. HARD COPY DISTRIBUTION OF INFORMATION 3
7. ELECTRONIC COMMUNICATION, TELEPHONY AND FACSIMILE SERVICES 3
8. USE OF INFORMATION SYSTEMS 3
9. LAPTOPS 6
10. LOSS AND INCIDENT REPORTING 7
11. SUB-CONTRACTS 7
12. PUBLICITY MATERIAL 7
13. DESTRUCTION 7
14. INTERPRETATION/GUIDANCE 8

ANNEXE 1 SECURITY ASPECTS LETTER……8

1. OFFICIAL-SENSITIVE

1.1. There is **no** requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes.

1.2. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the "OFFICIAL" classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the "need to know". In such cases where there is a clear and justifiable requirement to reinforce the "need to know", assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'.

2. SECURITY GRADING

2.1. The Supplier will mark all OFFICIAL-SENSITIVE documents which it originates or copies during the Framework Agreement/ Call Off Agreement period clearly with the OFFICIAL-SENSITIVE classification

Aspect	Classification
Customer data	Official
Documentation that details contractual matters relevant to the service	Official Sensitive
General system description documentation with no specific details of the aspects listed below.	Not protectively marked
All other Documentation	Official Sensitive
Details of Software used in the development or operational environment	Official Sensitive
Firewalls, Switches, Routers	Official Sensitive
System Administration services	Official Sensitive
Hosting Platforms	Official Sensitive
Auditing	Official Sensitive

2.2. It is possible that other sensitive matters will be identified during the development and support of this service. When such matters are identified, the supplier will be instructed on the protective marking assigned to that particular subject and any restrictions relevant to its dissemination and use.

3. OFFICIAL SECRETS ACTS

3.1. The Supplier's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Supplier will take all reasonable steps to make sure that all individuals employed on any work in connection with the Framework Agreement/ Call Off Agreement

(including Sub-contractors) have notice that these statutory provisions, or any others provided by the Contracting Authority, apply to them and will continue so to apply after the completion or earlier termination of the Framework Agreement.

4. PROTECTION OF OFFICIAL-SENSITIVE INFORMATION

4.1 The Supplier will protect OFFICIAL-SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Contracting Authority. The Supplier will take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

4.2 OFFICIAL-SENSITIVE information will be protected in a manner to avoid unauthorised access. The Supplier will take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

4.3 All OFFICIAL-SENSITIVE material including documents, media and other material will be physically secured to prevent unauthorised access. When not in use OFFICIAL-SENSITIVE documents/material will be stored under lock and key. As a minimum, when not in use, OFFICIAL SENSITIVE material will be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.

4.4 Disclosure of OFFICIAL-SENSITIVE information will be strictly in accordance with the "need to know" principle. Except with the written consent of the Contracting Authority, the Supplier will not disclose any of the classified aspects of the Framework Agreement/ Call Off Agreement detailed in the Security Aspects Letter other than to a person directly employed by the Supplier or Sub-contractor.

4.5 Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Contracting Authority for the purposes of the Framework Agreement/ Call Off Agreement remain the property of the Contracting Authority and will be returned on completion of the Framework Agreement / Call Off Agreement or, if directed by the Contracting Authority, destroyed in accordance with paragraph 13.

5. ACCESS

5.1 Access to OFFICIAL-SENSITIVE information will be confined to those individuals who have a “need-to-know” and whose access is essential for the purpose of his or her duties.

5.2 The Supplier will ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Suppliers will apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the Gov.UK website at: https://www.gov.uk/government/publications/security-policy-framework.

6. HARD COPY DISTRIBUTION OF INFORMATION

6.1 OFFICIAL-SENSITIVE documents will be distributed, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words OFFICIAL-SENSITIVE will **not** appear on the envelope. The envelope should bear a stamp or details that clearly indicate the full address of the office from which it was sent.

6.2 Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL-SENSITIVE hardware will be sought from the Contracting Authority.

7. ELECTRONIC COMMUNICATION, TELEPHONY AND FACSIMILE SERVICES

7.1 OFFICIAL-SENSITIVE information will be emailed unencrypted over the internet **only** where there is a strong business need to do so and only with the **prior** approval of the Contracting Authority. It will only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Contracting Authority will require. Such limitations, including any regarding publication, further circulation or other handling instructions will be clearly identified in the email sent with the material.

7.2 OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot of) unauthorised persons.

7.3 OFFICIAL-SENSITIVE information may be faxed to UK recipients.

8. USE OF INFORMATION SYSTEMS

8.1 The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack. However the Accreditation process and annual Check Assurance (outlined above) will be used to test the adequacy of any security controls in place.

8.2 There may also be a requirement for the service to be accessed via the Public Services Network (PSN). The PSN is the UK government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. It unified the provision of network infrastructure across the United Kingdom public sector into an interconnected "network of networks" to increase efficiency and reduce overall public expenditure. Advice regarding this requirement (and how to gain PSN certification) should be sought from the Contracting Authority.

8.3 As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

8.4 The following describes the minimum security requirements for processing and accessing OFFICIAL-SENSITIVE information on IT systems.

a. Access

Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” will be applied to System Administrators. Users of the IT System (Administrators should not conduct “standard‟ User functions using their privileged accounts.

b. Identification and Authentication (ID&A).

All systems will have the following functionality:

(1) Up-to-date lists of authorised users.
(2) Positive identification of all users at the start of each processing session.

c. Passwords.

Passwords are part of most ID&A, Security Measures. Passwords will be “strong‟ using an appropriate method to achieve this, for example including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control.

All systems will have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission.

Unless the Contracting Authority authorises otherwise, OFFICIAL-SENSITIVE information will be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using commercial encryption devices accepted by the Contracting Authority. Advice on encryption requirements for the transmission of OFFICIAL-SENSITIVE information will be sought from the Contracting Authority.

f. Security Accounting and Audit.

Security relevant events fall into two categories, namely legitimate events and violations.

1. The following events will always be recorded:
    a. All log on attempts whether successful or failed.
    b. Log off (including time out where applicable).
    c. The creation, deletion or alteration of access rights and privileges.

d. The creation, deletion or alteration of passwords.

2. For each of the events listed above, the following information is to be recorded:

    a. Type of event,
    b. User ID,
    c. Date & Time
    d. Device ID

3. The accounting records will have a facility to provide the System Manager with a hard copy of all or selected activity. There will also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

4. If the operating system is unable to provide this then the equipment will be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability.

The following supporting measures will be implemented:

1. Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)
2. Defined Business Continuity/Contingency Plan
3. Data backup with local storage
4. Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).
5. Operating systems, applications and firmware should be supported
6. Patching of Operating Systems and Applications used will be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners

Wherever possible, a “Logon Banner” will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

A suggested format for the text depending on national legal requirements could be:

(a) “Unauthorised access to this computer system may constitute a criminal offence”

i.Unattended Terminals.

Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections.

Computer systems will not be connected direct to the Internet or “untrusted‟ systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Contracting Authority’s Principal Security Advisor.

k. Disposal.

Before IT storage media (e.g. disks) are disposed of, an erasure product will be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

9. LAPTOPS

9.1. Laptops holding any supplied or Supplier generated OFFICIAL-SENSITIVE information are to be encrypted using a Foundation Grade product or equivalent, for example FIPS 140-2 approved full disk encryption. https://www.cesg.gov.uk/articles/foundation-grade-explained

9.2. Unencrypted laptops not on a secure site (Secure sites are defined as either Government premises or a secured office on the Supplier premises) are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Contracting Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term “drives” includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

9.3. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

9.4. Portable Communication and Information systems (CIS) devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

10. LOSS AND INCIDENT REPORTING

10.1. The Supplier will immediately report any loss or otherwise compromise of OFFICIAL-SENSITIVE information to the Contracting Authority. Any security incident involving OFFICIAL-SENSITIVE information will be immediately reported to the Contracting Authority.

11. SUB-CONTRACTS

11.1. The Supplier may Subcontract any elements of this Framework Agreement/ Call Off Agreement to Subcontractors within the United Kingdom notifying the Contracting Authority. When Subcontracting to a Subcontractor located in the UK the Supplier will ensure that these Security Conditions will be incorporated within the Subcontract document. The **prior** approval of the Contracting Authority will be obtained should the Supplier wish to Subcontract any OFFICIAL-SENSITIVE elements of the Contract to a Subcontractor located **in another country**. If the Subcontract is approved, the Contracting Authority will provide the Supplier with the security conditions that will be incorporated within the Subcontract document.

12. PUBLICITY MATERIAL

12.1 Suppliers wishing to release any publicity material or display hardware that arises from this Framework Agreement/ Call Off Agreement will seek the prior approval of the Contracting Authority. Publicity material includes open publication in the Supplier's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Contracting Authority or any other government department.

13. DESTRUCTION

13.1 As soon as no longer required, OFFICIAL-SENSITIVE information/material will be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice will be sought from the Contracting Authority when information/material cannot be destroyed or, unless already authorised by the Contracting Authority, when its retention is considered by the Supplier to be necessary or desirable. Unwanted OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way will be returned to the Contracting Authority.

14. INTERPRETATION/GUIDANCE

14.1. Advice regarding the interpretation of the above requirements should be sought from the Contracting Authority.

14.2. Where considered necessary by the Contracting Authority, the Supplier will provide evidence of compliance with this Security Condition and/or permit the inspection of the Suppliers processes and facilities by representatives of the Contracting Authority to ensure compliance with these requirements.