# Cyber

**DEFCON 658**
Edition 10/22

## 1. Definitions

1.1. In this Condition the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

"**Associated Company**" means:

(a) any associated company of the Contractor from time to time within the meaning of Section 449 of the Corporate Tax Act 2010 or any subordinate legislation; and

(b) any parent undertaking or subsidiary undertaking of the Contractor from time to time within the meaning of section 1162 Companies Act 2006 and it is further agreed that where the ownership of shares in any such undertaking have been pledged or transferred to a third party by way of security, the original parent shall still be considered a member of the subsidiary undertaking;

"**Cyber Risk Profile**" means the level of cyber risk relating to this Contract assessed by the Authority or in relation to any Sub-contract assessed by the Contractor, in each case in accordance with the Cyber Security Model;

"**Cyber Implementation Plan**" means the plan referred to in Clause 3 of this Condition;

"**Cyber Security Incident**" means an event, act or omission which gives rise or may give rise to:

(a) unauthorised access to an information system or electronic communications network on which MOD Identifiable Information resides;

(b) disruption or change of the operation (including but not limited to takeover of control) of an information system or electronic communications network on which MOD Identifiable Information resides;

(c) unauthorised destruction, damage, deletion or the change of MOD Identifiable Information residing in an information system or electronic communications network;

(d) unauthorised or unintentional removal or limiting the possibility to use MOD Identifiable Information residing in an information system or electronic communications network; or

(e) the appropriation, publication, dissemination or any other use of non-public MOD Identifiable Information by persons unauthorised to do so;

"**Cyber Security Instructions**" means DEFSTAN 05-138, together with any relevant ISN and specific security instructions relating to this Contract issued by the Authority to the Contractor;

"**Cyber Security Model**" and "CSM" mean the process by which the Authority ensures that MOD Identifiable Information is adequately protected from Cyber Security Incident and includes the CSM Risk

Assessment Process, DEFSTAN 05-138 and the CSM Supplier Assurance Questionnaire conducted via the Supplier Cyber Protection Service;

"**CSM Risk Assessment Process**" means the risk assessment process which forms part of the Cyber Security Model and is used to measure the Cyber Risk Profile for this Contract and any Sub-contract;

"**CSM Supplier Assurance Questionnaire**" means the supplier assessment questionnaire which forms part of the Cyber Security Model and is to be used by the Contractor to demonstrate compliance with this Condition;

"**Data**" means any data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;

"**DEFSTAN 05-138**" means the Defence Standard 05-138 as amended or replaced from time to time;

"**Electronic Information**" means all information generated, processed, transferred or otherwise dealt with under or in connection with the Contract, including but not limited to Data, recorded or preserved in electronic form and held on any information system or electronic communications network;

"**Good Industry Practice**" means in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgment and the making of any expenditure that would reasonably be expected from a skilled person in the same type of undertaking under the same or similar circumstances;

"**ISN**" means Industry Security Notices issued by the Authority to the Contractor whether directly or by issue on the gov.uk website at: https://www.gov.uk/government/publications/industry-security-notices-isns;

"**JSyCC WARP**" means the Joint Security Co-ordination Centre MOD Defence Industry Warning, Advice and Reporting Point or any successor body notified by way of ISN;

"**MOD Identifiable Information**" means all Electronic Information which is attributed to or could identify an existing or proposed MOD capability, defence activities or personnel and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure;

"**NSA/DSA**" means, as appropriate, the National or Designated Security Authority of the Contractor that is responsible for the oversight of the security requirements to be applied by the Contractor and for ensuring compliance with applicable national security regulations;

"**Sites**" means any premises from which Contractor Deliverables are provided in connection with this Contract or from which the Contractor or any relevant Sub-contractor manages, organises or otherwise directs the provision or the use of the Contractor Deliverables and/or any sites from which the Contractor or any relevant Sub-contractor generates, processes, stores or transmits MOD Identifiable Information in relation to this Contract;

"**Sub-contract**" means any sub-contract awarded directly by the Contractor as a consequence of or in connection with this Contract;

"**Sub-contractor**" means a sub-contractor or any Associated Company of the Contractor who provides Contractor Deliverables in connection with this Contract but only to the extent that the Sub-contractor processes, stores or transmits MOD Identifiable Information under their Sub-contract;

"**Supplier Cyber Protection Service**" means the tool incorporating the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire.

## 2. Authority Obligations

2.1. The Authority shall:

2.1.1. determine the Cyber Risk Profile appropriate to this Contract and notify the Contractor of the same at the earliest possible date; and

2.1.2. notify the Contractor as soon as reasonably practicable where the Authority reassesses the Cyber Risk Profile relating to this Contract, which shall be in accordance with Clause 7.

## 3. Contractor Obligations

3.1. The Contractor shall, and shall procure that their Sub-contractors shall:

3.1.1. comply with DEFSTAN 05-138 or, where applicable, the Cyber Implementation Plan attached to this Contract and for the avoidance of doubt any Cyber Implementation Plan shall be prepared and implemented in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the Authority and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect their own proprietary information;

3.1.2. complete the CSM Risk Assessment Process in accordance with the Authority's instructions, ensuring that any change in the Cyber Risk Profile is notified to any affected Sub-contractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the Contractor's supply chain or on receipt of any reasonable request by the Authority;

3.1.3. re-perform the CSM Supplier Assurance Questionnaire no less than once in each year of this Contract commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire to demonstrate continued compliance with the Cyber Security Instructions;

3.1.4. having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge their obligations under this Condition in accordance with Good Industry Practice *provided always that* where there is a conflict between the Contractor's obligations under 3.1.1 above and this 3.1.4 the Contractor shall notify the Authority in accordance with the notification provisions in DEFSTAN 05-138 as soon as they become aware of the conflict and the Authority shall determine which standard or measure shall take precedence;

3.1.5. comply with all Cyber Security Instructions notified to it by the Authority as soon as reasonably practicable;

3.1.6. notify the JSyCC WARP in accordance with ISN 2017/03 as amended or updated from time to time and the Contractors NSA/DSA, and in the case of a Sub-contractor also notify the Contractor, immediately in writing as soon as they know or believe that a Cyber Security Incident has

or may have taken place providing initial details of the circumstances of the incident and any mitigation measures already taken or intended to be taken, and providing further information in phases, as full details become available;

3.1.7. in coordination with their NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the Authority and its agents and representatives to take all steps to mitigate the impact of the Cyber Security Incident and minimise the likelihood of any further similar Cyber Security Incidents. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the Authority and the Contractors NSA/DSA in the circumstances and taking into account the Cyber Risk Profile; and

3.1.8. consent to the Authority recording and using information obtained via the Supplier Cyber Protection Service in relation to the Contract for the purposes of the Cyber Security Model which shall include any agreed Cyber Implementation Plan. For the avoidance of doubt such information shall include the cyber security accreditation of the Contractor and/or Sub-contractor as appropriate; and

3.1.9. include provisions equivalent to those set out in the Annex to this Condition (the “equivalent provisions”) in all relevant Sub-contracts.

## 4. Management Of Sub-Contractors

4.1. Provided that it is reasonable in all the circumstances to do so, the Authority agrees that the Contractor shall be entitled to rely on the self-certification by the Sub-contractor of their compliance with this Condition in accordance with 3.1.1 above.

4.2. Where a Sub-contractor notifies the Contractor that it cannot comply with the requirements of DEFSTAN 05-138, the Contractor shall require a Sub-contractor to prepare and implement a Cyber Implementation Plan in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the Contractor and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect the proprietary information of the Sub-contractor. Where the Contractor has reasonably relied on the Sub-contractor's self-certification and the Sub-contractor is subsequently found to be in breach of their obligations, the Contractor shall not be in breach of this Condition.

4.3. The Contractor shall, and shall require their Sub-contractors to, include provisions equivalent to those set out in the Annex to this Condition in all relevant Sub-contracts and shall notify the Authority in the event that they become aware of any material breach of the provisions set out in the Annex by their Sub-contractor.

## 5. Records

5.1. The Contractor shall keep and maintain, and shall ensure that any Sub-contractor shall keep and maintain, until 6 years after termination or end of Contract term or final payment under this Contract, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:

5.1.1. copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Condition, including but not limited to any

information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance Questionnaire, together with any certificates issued to the Contractor and/or Sub-contractor; and

5.1.2. copies of all documents demonstrating compliance with 3.1.5 and in relation to any notifications made under 3.1.6 and/or investigation under 3.1.7.

5.2. The Contractor shall, and shall ensure that any Sub-contractor shall, on request provide the Authority, the Authority's representatives and/or the Contractors NSA/DSA such access to those records under 5.1 as may be required in connection with this Contract.

## 6. Audit

6.1. In the event of a Cyber Security Incident the Contractor agrees that the Authority and its representatives, in coordination with the Contractor's NSA/DSA, may conduct such audits as are required to establish (i) the cause of the Cyber Security Incident, (ii) the impact of the Cyber Security Incident, (iii) the MOD Identifiable Information affected, and (iv) the work carried out by the Contractor to resolve the Cyber Security Incident and to mitigate the effects, to ensure that the Cyber Security Incident is resolved to the satisfaction of the Authority and the NSA/DSA.

6.2. In addition to the rights in 6.1 above the Authority or its representatives and/or the Contractor's NSA/DSA, either solely or in any combination, may at any time during the Contract and for a period of six (6) years after termination of the Contract or the end of the Contract term or final payment under the Contract whichever is the later, but not more than once in any calendar year , conduct an audit for the following purposes where the Contractor continues to hold MOD Identifiable Information:

6.2.1. to review and verify the integrity, confidentiality and security of any MOD Identifiable Information; and

6.2.2. to review the Contractor's and/or any Sub-contractor's compliance with their obligations under DEFSTAN 05-138 or a Cyber Implementation Plan; and

6.2.3. to review any records created during the provision of the Contractor Deliverables, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of 5.1.1 and 5.1.2 above.

6.3. The Authority, acting reasonably and having regard to the confidentiality and security obligations owed by the Contractor to third parties, shall propose the scope of each audit in writing with a view to seeking the agreement of the Contractor but shall make the ultimate decision on the scope. For the avoidance of doubt the scope of the audit shall not grant the Authority any unsupervised access to any of the Contractor's information systems or electronic communications networks. The Authority shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Contractor and/or Sub-contractor or delay the provision of the Contractor Deliverables and supplier information received by the Authority in connection with the audit shall be treated as confidential information.

6.4. The Contractor shall, and shall ensure that any Sub-contractor shall on demand provide the Authority and any relevant regulatory body, including the Contractor's NSA/DSA, (and/or their agents or representatives), together "the

Auditors", with all reasonable co-operation and assistance in relation to each audit, including but not limited to:

6.4.1. all information requested by the Authority within the permitted scope of the audit;

6.4.2. reasonable access to any Sites controlled by the Contractor or any Associated Company used in the performance of the Contract to the extent required within the permitted scope of the audit and, where such Sites are outwith the control of the Contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and

6.4.3. access to any relevant staff.

6.5. The Authority shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice of its intention to conduct an audit.

6.6. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Condition, unless the audit identifies a material breach of the terms of this Condition by the Contractor in which case the Contractor shall reimburse the Authority for all the Authority's reasonable costs incurred (which shall be evidence to the Contractor) in the course of the audit.

6.7. The Contractor shall in their Sub-contracts procure rights for the Authority to enforce the terms of clause 6 of this Condition in accordance with the Contracts (Rights of Third Parties) Act 1999.

## 7. General

7.1. On termination or expiry of this Contract the provisions of this Condition excepting 3.1.2 and 3.1.3 above shall continue in force so long as the Contractor and/or and Sub-contractor holds any MOD Identifiable Information relating to this Contract.

7.2. Termination or expiry of this Contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Condition that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination or expiry.

7.3. The Contractor agrees that the Authority has absolute discretion to determine changes to DEFSTAN 05-138 or the Cyber Risk Profile or both and issue new or updated Cyber Security Instructions. In the event that there is such a change to DEFSTAN 05-138 or the Cyber Risk Profile or both, then either Party may seek an adjustment to the Contract Price for any associated increase or decrease in costs and the Contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Cyber Risk Profile or both *provided always that* the Contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and *further provided that* such costs shall not be allowed unless they are considered to be appropriate, attributable to the Contract and reasonable in all the circumstances.

7.4. Subject to 7.3 above, where the Contractor seeks such adjustment or extension, the Authority will proceed in accordance with DEFCON 620 or any agreed alternative change control procedure to determine the request for adjustment or extension. The Contractor must deliver a Contractor Change Proposal to the Authority within eight (8) weeks (or other period agreed by the

parties) of the occurrence of the change in DEFSTAN 05-138 or Cyber Risk Profile or both, identifying the impact of that change and accompanied by full details of the request for adjustment. For the avoidance of doubt, the Authority shall not be required to withdraw any Authority Notice of Change which may have been issued insofar as it relates to DEFSTAN 05-138 or the Cyber Risk Profile or both whether or not the Contractor Change Proposal is rejected. If the Contractor does not agree with the Authority's determination, then the provisions of DEFCON 530 or any agreed alternative dispute resolution procedure provided for in the Contract shall apply.

7.5. The Contractor shall not recover any costs and/or other losses under or in connection with this Condition where such costs and/or other losses are recoverable or have been recovered by the Contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Cyber Security Incident or otherwise, where the Contractor is able to or has recovered such sums in any other provision of this Contract or has recovered such costs and/or losses in other contracts between the Contractor and the Authority or with other bodies.

# Annex to DEFCON 658

# Cyber

# Provisions to be Included in Relevant Sub-Contracts

## 1. Definitions

1.1. In this Condition the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

"**Associated Company**" means:

(a) any associated company of the Sub-contractor from time to time within the meaning of Section 449 of the Corporate Tax Act 2010 or any subordinate legislation; and

(b) any parent undertaking or subsidiary undertaking of the Sub-contractor from time to time within the meaning of section 1162 Companies Act 2006 and it is further agreed that where the ownership of shares in any such undertaking have been pledged or transferred to a third party by way of security, the original parent shall still be considered a member of the subsidiary undertaking;

"**Cyber Risk Profile**" means the level of cyber risk relating to this Sub-contract or any lower tier Sub-contract assessed in accordance with the Cyber Security Model;

"**Cyber Implementation Plan**" means the plan referred to in Clause 2 of this Condition;

"**Cyber Security Incident**" means an event, act or omission which gives rise or may give rise to:

(a) unauthorised access to an information system or electronic communications network on which MOD Identifiable Information resides;

(b) disruption or change of the operation (including but not limited to takeover of control) of an information system or electronic communications network on which MOD Identifiable Information resides;

(c) unauthorised destruction, damage, deletion or the change of MOD Identifiable Information residing in an information system or electronic communications network;

(d) unauthorised or unintentional removal or limiting the possibility to use MOD Identifiable Information residing in an information system or electronic communications network; or

(e) the appropriation, publication, dissemination or any other use of non-public MOD Identifiable Information by persons unauthorised to do so.

"**Cyber Security Instructions**" means DEFSTAN 05-138, together with any relevant ISN and specific security instructions relating to this Sub-contract issued by the MOD to the Prime Contractor;

"**Cyber Security Model**" and "CSM" mean the process by which the MOD ensures that MOD Identifiable Information is adequately protected from

Cyber Security Incident and includes the CSM Risk Assessment Process, DEFSTAN 05-138 and the CSM Supplier Assurance Questionnaire conducted via the Supplier Cyber Protection Service;

"**CSM Risk Assessment Process**" means the risk assessment process which forms part of the Cyber Security Model and is used to measure the Cyber Risk Profile for this Sub-contract and any lower tier Sub-contract;

"**CSM Supplier Assurance Questionnaire**" means the supplier assessment questionnaire which forms part of the Cyber Security Model and is to be used by the Sub-contractor to demonstrate compliance with this Condition;

"**Data**" means any data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;

"**DEFSTAN 05-138**"means the Defence Standard 05-138 as amended or replaced from time to time;

"**Electronic Information**" means all information generated, processed, transferred or otherwise dealt with under or in connection with this Sub-contract, including but not limited to Data, recorded or preserved in electronic form and held on any information system or electronic communications network;

"**Good Industry Practice**" means in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgment and the making of any expenditure that would reasonably be expected from a skilled person in the same type of undertaking under the same or similar circumstances;

"**ISN**" means Industry Security Notices issued by the MOD to the Prime Contractor whether directly or by issue on the gov.uk website at: https://www.gov.uk/government/publications/industry-security-notices-isns;

"**JSyCC WARP**" means the Joint Security Co-ordination Centre MOD Defence Industry Warning, Advice and Reporting Point or any successor body notified by way of ISN;

**"MOD**" means the UK Ministry of Defence of 1 Horseguards, London acting by [ ] project team at [insert contact details];

"**MOD Identifiable Information**" means all Electronic Information which is attributed to or could identify an existing or proposed MOD capability, defence activities or personnel and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure;

**"Prime Contract"** means [contract reference] [insert details of prime contract] made between the MOD and the Contractor;

**"Prime Contractor"** means the Contractor named in the Prime Contract with MOD;

"**NSA/DSA**" means, as appropriate, the National or Designated Security Authority of the Prime or Sub-contractor that is responsible for the oversight of the security requirements to be applied by the Prime or Sub-contractor and for ensuring compliance with applicable national security regulations;

"**Sites**" means any premises from which Contractor Deliverables are provided in connection with this Sub-contract or from which the Sub-contractor or any relevant lower tier Sub-contractor manages, organises or otherwise directs the provision or the use of the Contractor Deliverables and/or any sites from which the Sub-contractor or any relevant lower tier Sub-contractor generates, processes, stores or transmits MOD Identifiable Information in relation to this Sub-contract;

"**Sub-contract**" means any sub-contract at any level of the supply chain, whether this Sub-contract which is awarded by the Prime Contractor or any related Sub-contract which is awarded by the Sub-Contractor or any lower tier Sub-contractor or Associated Company, which is entered into as a consequence of or in connection with this Sub-contract;

"**Sub-contractor**" means a sub-contractor of the Prime Contractor or any Associated Company whether a direct Sub-contractor or at any lower level of the supply chain who provides any Contractor Deliverables in connection with the Prime Contract but only to the extent that the Sub-contractor processes, stores or transmits MOD Identifiable Information under their Sub-contract;

"**Supplier Cyber Protection Service**" means the tool incorporating the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire;

## 2. Sub-Contractor Obligations

2.1. The Sub-contractor shall, and shall procure that their lower tier Sub-contractors shall:

2.1.1. comply with DEFSTAN 05-138 or, where applicable, the Cyber Implementation Plan attached to this Sub-contract and for the avoidance of doubt any Cyber Implementation Plan shall be prepared and implemented in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the MOD and the Prime Contractor and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect their own proprietary information;

2.1.2. complete the CSM Risk Assessment Process in accordance with the MOD and the Prime Contractor's instructions, ensuring that any change in the Cyber Risk Profile is notified to the MOD, the Prime Contractor and any affected lower tier Sub-contractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the supply chain or on receipt of any reasonable request by the MOD;

2.1.3. re-perform the CSM Supplier Assurance Questionnaire no less than once in each year of this Sub-contract commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire to demonstrate continued compliance with the Cyber Security Instructions;

2.1.4. having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge their obligations under this Condition in accordance with Good Industry Practice *provided always that* where there is a conflict between the Sub-contractor's obligations under 2.1.1 above and this 2.1.4 the Sub-contractor shall notify the Prime Contractor and the MOD in accordance with the notification provisions in DEFSTAN 05-138 as soon as they become aware of the conflict and the MOD shall determine which standard or measure shall take precedence;

2.1.5. comply with all Cyber Security Instructions notified to them by the MOD and/or the Prime Contractor as soon as reasonably practicable;

2.1.6. notify the JSyCC WARP in accordance with ISN 2017/03 as amended or updated from time to time and the Prime Contractor and the Sub-Contractor's NSA/DSA immediately in writing as soon as they know or believe that a Cyber Security Incident has or may have taken place providing initial details of the circumstances of the incident and any mitigation measures already taken or intended to be taken, and providing further information in phases, as full details become available;

2.1.7. in coordination with their NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the MOD, the Prime Contractor and their agents and representatives to take all steps to mitigate the impact of the Cyber Security Incident and minimise the likelihood of any further similar Cyber Security Incidents. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the MOD and the relevant Prime and/or Sub-contractor's NSA/DSA in the circumstances and taking into account the Cyber Risk Profile; and

2.1.8. consent to the MOD recording and using information obtained via the Supplier Cyber Protection Service in relation to the Sub-contract for the purposes of the Cyber Security Model which shall include any agreed Cyber Implementation Plan. For the avoidance of doubt such information shall include the cyber security accreditation of the Sub-contractor and/or lower tier Sub-contractor as appropriate; and

2.1.9. include provisions equivalent to this Condition in all lower tier Sub-contracts (the "equivalent provisions") and, where a lower tier Sub-contractor breaches terms implementing this Condition in a Sub-contract, the Sub-contractor shall, and shall procure that their lower tier Sub-contractors shall, in exercising their rights or remedies under the relevant Sub-contract:

2.1.9.1. notify the Prime Contractor and the MOD of any such breach and consult with the Prime Contractor and the MOD regarding any remedial or other measures which are proposed as a consequence of such breach, taking the MOD's views into consideration; and

2.1.9.2. have regard to the equivalent provisions.

## 3. Records

3.1. The Sub-contractor shall keep and maintain, and shall ensure that any lower tier Sub-contractor shall keep and maintain, until six (6) years after

termination of Contract term or final payment under this Sub-contract, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:

3.1.1. copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Condition, including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance Questionnaire, together with any certificates issued to the Sub-contractor and/or any lower tier Sub-contractor.

3.1.2. copies of all documents demonstrating compliance with 2.1.5 and in relation to any notifications made under 2.1.6 and/or investigation under 2.1.7.

3.2. The Sub-contractor shall, and shall ensure that any lower tier Sub-contractor shall, on request provide the MOD, the MOD's representatives and/or the relevant Prime or Sub-contractor's NSA/DSA such access to those records under 3.1 as may be required in connection with this Sub-contract.

## 4. Audit

4.1. In the event of a Cyber Security Incident the Sub-contractor agrees that the MOD and its representatives, in coordination with the relevant Prime or Sub-contractor's NSA/DSA, may conduct such audits as are required to establish (i) the cause of the Cyber Security Incident, (ii) the impact of the Cyber Security Incident, (iii) the MOD Identifiable Information affected, and (iv) the work carried out by the Sub-contractor to resolve the Cyber Security Incident and to mitigate the effects, to ensure that the Cyber Security Incident is resolved to the satisfaction of the MOD and the NSA/DSA.

4.2. In addition to the rights in 4.1 above, the Sub-contractor agrees that the MOD, its representatives and/or the relevant Prime or Sub-contractor's NSA/DSA, either solely or in any combination, may at any time during the Contract and for a period of six (6) years after termination of this Sub-contract or the end of the Sub-contract term or final payment under the Sub-contract whichever is the later, but not more than once in any calendar year, conduct an audit for the following purposes where the Sub-Contractor continues to hold MOD Identifiable Information:

4.2.1. to review and verify the integrity, confidentiality and security of any MOD Identifiable Information;

4.2.2. to review the Sub-contractor's and/or any lower tier Sub-contractor's compliance with their obligations under DEFSTAN 05-138 or a Cyber Implementation Plan; and

4.2.3. to review any records created during the provision of the Contractor Deliverables, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of 3.1.1 and 3.1.2 above.

4.3. The MOD, acting reasonably and having regard to the confidentiality and security obligations owed by the Sub-contractor to third parties, shall propose the scope of each audit in writing with a view to seeking the agreement of the Sub-contractor but shall make the ultimate decision on the scope. For the avoidance of doubt the scope of the audit shall not grant the MOD any unsupervised access to any of the Sub-contractor’s information systems or electronic communications networks. The MOD and the Prime Contractor shall

use their reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Sub-contractor and/or lower tier Sub-contractor or delay the provision of the Contractor Deliverables and supplier information received in connection with the audit shall be treated as confidential information.

4.4. The Sub-contractor shall, and shall ensure that any lower tier Sub-contractor shall, on demand provide the MOD and any relevant regulatory body, including the relevant Prime or Sub-contractor's NSA/DSA, (and/or their agents or representatives), together "the Auditors", with all reasonable co-operation and assistance in relation to each audit, including but not limited to:

4.4.1. all information requested by the MOD within the permitted scope of the audit;

4.4.2. reasonable access to any Sites controlled by the Sub-contractor or any Associated Company and any lower tier Sub-contractor used in the performance of the Sub-contract to the extent required within the permitted scope of the audit and, where such Sites are outwith the control of the Sub-contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and

4.4.3. access to any relevant staff.

4.5. Where the Prime Contractor is provided with notice of the audit by the MOD and/or the relevant NSA/DSA, the Prime Contractor shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice to the Sub-contractor of the intention to conduct an audit.

4.6. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Condition, unless the audit identifies a material breach of the terms of this Condition by the Sub-contractor and/or a lower tier Sub-contractor in which case the Sub-contractor shall reimburse the Prime Contractor and the MOD as appropriate for all the reasonable costs incurred in the course of the audit.

4.7. The Sub-Contractor shall in their lower tier Sub-contracts procure rights for the MOD to enforce the terms of this clause 4 of this Condition in accordance with the Contracts (Rights of Third Parties) Act 1999.

## 5. General

5.1. On termination or expiry of this Sub-contract the provisions of this Condition shall continue in force so long as the Sub-contractor and/or any lower tier Sub-contractor holds any MOD Identifiable Information relating to this Sub-contract.

5.2. Termination or expiry of this Sub-contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Condition that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of this Sub-contract which existed at or before the date of termination or expiry.

5.3. The Sub-contractor agrees that the MOD has absolute discretion to determine changes to DEFSTAN 05-138 or the Cyber Risk Profile or both and issue new or updated Cyber Security Instructions. In the event that there is such a change to DEFSTAN 05-138 or the Cyber Risk Profile or both, then the Sub-contractor may seek an adjustment to the contract price from the Prime Contractor for any associated increase or decrease in costs and the Sub-contractor may request an extension of time for compliance with such revised or

amended DEFSTAN 05-138 or Cyber Risk Profile or both *provided always that* the Sub-contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and *further provided that* such costs shall not be allowed unless they are considered to be appropriate, attributable to this Sub-contract and reasonable in all the circumstances.

5.4. The Sub-contractor shall not recover any costs and/or other losses under or in connection with this Condition where such costs and/or other losses are recoverable or have been recovered by the Sub-contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Cyber Security Incident or otherwise, where the Sub-contractor is able to or has recovered such sums in any other provision of this Sub-contract or has recovered such costs and/or losses in other contracts between the Sub-contractor and the Prime Contractor or with other bodies.