



Ministry of
JUSTICE

OFFICIAL SENSITIVE

Contract for the Provision of Learning and Skills at HMP & YOI Parc

SCHEDULE 6 – INFORMATION ASSURANCE & SECURITY



Contract for the Provision of Learning and Skills at HMP & YOI Parc

1. GENERAL

- 1.1 This Schedule 6 sets out the obligations of the Parties in relation to information assurance and cyber security, including those which the Contractor must comply with in delivering the Services under the Contract.
- 1.2 The Parties acknowledge that the purpose of the ISMS and the ISMP is to ensure a robust organisational approach to information assurance and cyber security under which the specific requirements of the Contract will be met.
- 1.3 The Parties shall each appoint and/or identify a board level individual or equivalent who has overall responsibility for information assurance and cyber security, including personnel security and information risk. The individual appointed by the Contractor, who is the Chief Security Officer, Chief Information Officer, Chief Technical Officer or equivalent and is responsible for compliance with the ISMS, is identified as Key Personnel and the provisions of clause B4 apply in relation to that person.
- 1.4 The Contractor shall act in accordance with Good Industry Practice in the day-to-day operation of any system which is used for the storage of Information Assets and/or the storage, processing or management of Authority Data and/or that could directly or indirectly affect Information Assets and/or Authority Data.
- 1.5 The Contractor shall ensure that an information security policy is in place in respect of the operation of its organisation and systems, which shall reflect relevant control objectives for the Contractor System, including those specified in the ISO27002 control set or equivalent, unless otherwise agreed by the Authority. The Contractor shall, upon request, provide a copy of this policy to the Authority as soon as reasonably practicable. The Contractor shall maintain and keep such policy updated and provide clear evidence of this as part of its ISMP.
- 1.6 The Contractor acknowledges that a compromise of Information Assets and/or Authority Data represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties. The Contractor shall provide clear evidence of regular communication with the Authority in relation to information risk as part of its ISMP.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

- 2.1 The Contractor shall, within 30 Working Days of the Commencement Date, submit to the Authority a proposed ISMS which:
- (a) has been tested; and
 - (b) complies with the requirements of paragraphs 2.2 and 2.3.
- 2.2 The Contractor shall at all times ensure that the level of security, include cyber security, provided by the ISMS is sufficient to protect the confidentiality, integrity and availability of Information Assets and Authority Data used in the provision of the Services and to provide robust risk management.
- 2.3 The Contractor shall implement, operate and maintain an ISMS which shall:



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (a) protect all aspects of and processes of Information Assets and Authority Data, including where these are held on the ICT Environment (to the extent that this is under the control of the Contractor);
- (b) be aligned to and certified to the relevant standards in ISO/IEC 27001: 2013 requirements in accordance with paragraph 5 unless otherwise Approved;
- (c) provide a level of security which ensures that the ISMS and the Contractor System:
 - (i) meet the requirements in the Contract;
 - (ii) are in accordance with applicable Law;
 - (iii) demonstrate Good Industry Practice, including the Government's Minimum Cyber Security Standards and the 10 Steps to Cyber Security, currently available at: <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard> and <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>;
 - (iv) comply with the Security Policy Framework, NCSC and Cabinet Office and any other relevant Government security standards;
 - (v) comply with the Baseline Security Requirements;
 - (vi) comply with the Authority's policies, including, where applicable, HMPPS Information Security Policy, Ministry of Justice IT and Cyber Security Guidance;
- (d) address any issues of incompatibility with the Contractor's organisational security policies;
- (e) address any specific security threats of immediate relevance to Information Assets and/or Authority Data;
- (f) document:
 - (i) the security incident management processes, including reporting, recording and management of information risk incidents, including those relating to the ICT environment (to the extent that this is within the control of the Contractor) and the loss of protected Personal Data, and the procedures for reducing and raising awareness of information risk;
 - (ii) incident response plans, including the role of nominated security incident response companies; and
 - (iii) the vulnerability management policy, including processes for identification of system vulnerabilities and assessment of the potential effect on the Services of any new threat, vulnerability or exploitation technique of which the Contractor becomes aware, prioritisation of security patches, testing and application of security patches and the reporting and audit mechanism detailing the efficacy of the patching policy;



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (g) include procedures for the secure destruction of Information Assets and Authority Data and any hardware or devices on which such information or data is stored; and
 - (h) be certified by (or by a person with the direct delegated authority of) the Contractor's representative appointed and/or identified in accordance with paragraph 1.3.
- 2.4 If the Contractor becomes aware of any inconsistency in the provisions of the standards, guidance and policies notified to the Contractor from time to time, the Contractor shall immediately notify the Authority of such inconsistency and the Authority shall, as soon as practicable, notify the Contractor of the provision that takes precedence.
- 2.5 The Contractor shall, upon request from the Authority or any nominated security personnel/assurer appointed by the Authority, provide sufficient design documentation detailing the security architecture of its ISMS to support the Authority's and/or assurer's assurance that it is appropriate, secure and complies with the Authority's requirements.
- 2.6 The Authority shall review the proposed ISMS submitted pursuant to paragraph 2.1 and shall, within 10 Working Days of its receipt notify the Contractor as to whether it has been Approved.
- 2.7 If the ISMS is Approved, it shall be adopted by the Contractor immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.
- 2.8 If the ISMS is not Approved, the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall, within a further 10 Working Days notify the Contractor whether the amended ISMS has been Approved. The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and, in any event, no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with clause I1 (Dispute Resolution).
- 2.9 Approval of the ISMS or any change to it shall not relieve the Contractor of its obligations under this Schedule 6.
- 2.10 The Contractor shall provide to the Authority, upon request, any or all ISMS documents.
- 3. INFORMATION SECURITY MANAGEMENT PLAN**
- 3.1 The Contractor shall, within 30 Working Days of the Commencement Date, submit to the Authority for approval a ISMP which complies with paragraph 3.2.
- 3.2 The Contractor shall effectively implement the ISMP which shall:
- (a) comply with the Baseline Security Requirements;
 - (b) identify the organisational roles for those responsible for ensuring the Contractor's compliance with this Schedule 6;
 - (c) detail the process for managing any security risks from those with access to Information Assets and/or Authority Data, including where these are held in the ICT Environment;



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (d) set out the security measures and procedures to be implemented by the Contractor, which are sufficient to ensure compliance with the provisions of this Schedule 6;
 - (e) set out plans for transition from the information security arrangements in place at the Commencement Date to those incorporated in the ISMS;
 - (f) set out the scope of the Authority System that is under the control of the Contractor;
 - (g) be structured in accordance with ISO/IEC 27001: 2013 or equivalent unless otherwise Approved;
 - (h) be written in plain language which is readily comprehensible to all Staff and to Authority personnel engaged in the Services and reference only those documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule 6; and
 - (i) comply with the Security Policy Framework and any other relevant Government security standards.
- 3.3 The Authority shall review the ISMP submitted pursuant to paragraph 3.1 and notify the Contractor, within 10 Working Days of receipt, whether it has been Approved.
- 3.4 If the ISMP is Approved, it shall be adopted by the Contractor immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.
- 3.5 If the ISMP is not Approved, the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall notify the Contractor within a further 10 Working Days whether it has been Approved.
- 3.6 The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and, in any event, no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the ISMP following its resubmission, the matter shall be resolved in accordance with clause I1 (Dispute Resolution).
- 3.7 Approval by the Authority of the ISMP pursuant to paragraph 3.3 or of any change to the ISMP shall not relieve the Contractor of its obligations under this Schedule 6.
- 4. REVISION OF THE ISMS AND ISMP**
- 4.1 The ISMS and ISMP shall be reviewed in full and tested by the Contractor at least annually throughout the Term (or more often where there is a significant change to the Contractor System or associated processes or where an actual or potential Breach of Security or weakness is identified) to consider and take account of:
- (a) any issues in implementing the Security Policy Framework and/or managing information risk;
 - (b) emerging changes in Good Industry Practice;
 - (c) any proposed or actual change to the ICT Environment and/or associated processes;



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (d) any new perceived, potential or actual security risks or vulnerabilities;
- (e) any ISO27001: 2013 audit report or equivalent produced in connection with the Certification Requirements which indicates concerns; and
- (f) any reasonable change in security requirements requested by the Authority.

4.2 The Contractor shall give the Authority the results of such reviews as soon as reasonably practicable after their completion, which shall include without limitation:

- (a) suggested improvements to the effectiveness of the ISMS, including controls;
- (b) updates to risk assessments; and
- (c) proposed modifications to respond to events that may affect the ISMS, including the security incident management processes, incident response plans and general procedures and controls that affect information security.

4.3 Following the review in accordance with paragraphs 4.1 and 4.2 or at the Authority's request, the Contractor shall give the Authority at no additional cost a draft updated ISMS and/or ISMP which includes any changes the Contractor proposes to make to the ISMS or ISMP. The updated ISMS and/or ISMP shall, unless otherwise agreed by the Authority, be subject to clause F4 (Change) and shall not be implemented until Approved.

4.4 If the Authority requires any updated ISMS and/or ISMP to be implemented within shorter timescales than those set out in clause F4, the Parties shall thereafter follow clause F4 for the purposes of formalising and documenting the relevant change for the purposes of the Contract.

5. CERTIFICATION REQUIREMENTS

5.1 The Contractor shall ensure that any systems, including the ICT Environment, on which Information Assets and Authority Data are stored and/or processed are certified as compliant with:

- (a) ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
- (b) the Government's Cyber Essentials Scheme at the Plus level unless otherwise agreed with the Authority or where ISO/IEC 27001:2013 has not been obtained;

and shall provide the Authority with evidence:
- (c) of certification before the Contractor accessed the ICT Environment and receives, stores, processes or manages any Authority Data; and
- (d) that such certification remains valid and is kept up to date while the Contractor (as applicable) continues to access the ICT Environment and receives, stores, processes or manages any Authority Data during the Term.

5.2 The Contractor shall ensure that it:



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (a) carries out any secure destruction of Information Assets and/or Authority Data at Contractor sites which are included within the scope of an existing certificate of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and
- (b) is certified as compliant with the NCSC guidance on Sanitisation Standards or equivalent unless otherwise Approved,

and the Contractor shall provide the Authority with evidence of its compliance with the requirements set out in this paragraph 5.2 before the Contractor may carry out the secure destruction of any Information Assets and/or Authority Data.

- 5.3 The Contractor shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Contractor ceases to be compliant with the certification requirements in paragraph 5.1 and, on request from the Authority, shall:

- (a) immediately cease access to and use of Information Assets and/or Authority Data; and
- (b) promptly return, destroy and/or erase any Authority Data in accordance with the Baseline Security Requirements and failure to comply with this obligation is a material Default.

6. SECURITY TESTING

- 6.1 The Contractor shall, at its own cost, carry out relevant Security Tests from the Commencement Date and throughout the Term, which shall include:

- (a) a monthly vulnerability scan and assessment of the Contractor System and any other system under the control of the Contractor on which Information Assets and/or Authority Data are held;
- (b) an annual IT Health Check by an independent CHECK qualified company of the Contractor System and any other system under the control of the Contractor on which Information Assets and/or Authority Data are held and any additional IT Health Checks required by the Authority and/or any assurer. The Contractor shall remediate risks identified by IT Health Check reports in a timely manner and provide the vulnerability correction plan to the Authority;
- (c) an assessment as soon as reasonably practicable following receipt by the Contractor of a critical vulnerability alert from a provider of any software or other component of the Contractor System and/or any other system under the control of the Contractor on which Information Assets and/or Authority Data are held; and
- (d) such other tests as are required:
 - (i) by any Vulnerability Correction Plans;
 - (ii) by ISO/IEC 27001:2013 certification requirements or equivalent Approved;
 - (iii) after any significant architectural changes to the ICT Environment;



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (iv) after a change to the ISMS (including security incident management processes and incident response plans) or the ISMP; and
- (v) following a Breach of Security.

6.2 In relation to each IT Health Check, the Contractor shall:

- (a) agree with the Authority the aim and scope of the IT Health Check;
- (b) promptly, following receipt of each IT Health Check report, give the Authority a copy of the IT Health Check report; and
- (c) if the IT Health Check report identifies any vulnerabilities:
 - (i) prepare a Vulnerability Correction Plan for Approval which sets out in respect of each such vulnerability:
 - (A) how the vulnerability will be remedied;
 - (B) the date by which the vulnerability will be remedied;
 - (C) the tests which the Contractor shall perform or procure to be performed (which may, at the Authority's discretion, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (ii) comply with the Vulnerability Correction Plan; and
 - (iii) conduct such further Security Tests as are required by the Vulnerability Correction Plan.

6.3 Security Tests shall be designed and implemented by the Contractor so as to minimise any adverse effect on the Services and the date, timing, content and conduct of Security Tests shall be agreed in advance with the Authority.

6.4 The Authority may send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of Security Tests (in a form to be Approved) as soon as practicable and in any event within 5 Working Days after completion of each Security Test.

6.5 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority and/or its authorised representatives, including any assurer, may at any time to carry out Security Tests (including penetration tests) as it may deem necessary as part of any accreditation process and/or to verify the Contractor's compliance with the ISMS and the ISMP:

- (a) upon giving reasonable notice to the Contractor where reasonably practicable to do so; and
- (b) without giving notice to the Contractor where, in the Authority's view, the provision of such notice may undermine the Security Tests to be carried out



Contract for the Provision of Learning and Skills at HMP & YOI Parc

and, where applicable, the Authority shall be granted access to the Contractor's premises for the purpose of undertaking the relevant Security Tests.

- 6.6 If the Authority carries out Security Tests in accordance with paragraphs 6.5(a) or 6.5(b), the Authority shall (unless there is any reason to withhold such information) notify the Contractor of the results of the Security Tests as soon as possible and in any event within 5 Working Days after completion of each Security Test.
- 6.7 If any Security Test carried out pursuant to paragraphs 6.1 or 6.4 reveals any:
- (a) vulnerabilities during any accreditation process, the Contractor shall track and resolve them effectively; and
 - (b) actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Contractor shall promptly notify the Authority of any proposed changes to the ICT Environment (to the extent that this is under the control of the Contractor) and/or to the ISMS and/or to the ISMP (and the implementation thereof) which the Contractor intends to make in order to correct such failure or weakness. Subject to Approval and paragraphs 4.3 and 4.4, the Contractor shall implement such changes to the ICT Environment (to the extent that this is under the control of the Contractor) and/or the ISMS and/or the ISMP and repeat the relevant Security Tests in accordance with an Approved timetable or, otherwise, as soon as reasonably practicable.
- 6.8 If the Authority unreasonably withholds its approval to the implementation of any changes to the ICT Environment and/or to the ISMS and/or to the ISMP proposed by the Contractor in accordance with paragraph 6.7, the Contractor is not in breach of the Contract to the extent that it can be shown that such breach:
- (a) has arisen as a direct result of the Authority unreasonably withholding Approval to the implementation of such proposed changes; and
 - (b) would have been avoided had the Authority Approved the implementation of such proposed changes.
- 6.9 If a change to the ISMS or ISMP is to address any non-compliance with ISO/IEC 27001:2013 requirements or equivalent, the Baseline Security Requirements or any obligations in the Contract, the Contractor shall implement such change at its own cost and expense.
- 6.10 If any repeat Security Test carried out pursuant to paragraph 6.7 reveals an actual or potential breach of security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.
- 6.11 On each anniversary of the Commencement Date, the Contractor shall provide to the Authority a letter from the individual appointed or identified in accordance with paragraph 1.3 confirming that having made due and careful enquiry:
- (a) the Contractor has in the previous year carried out all Security Tests in accordance with this Schedule 6 and has complied with all procedures in relation to security matters required under the Contract; and



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (b) the Contractor is confident that its security and risk mitigation procedures in relation to Information Assets and Authority Data remain effective.

7. SECURITY AUDITS AND COMPLIANCE

- 7.1 The Authority and its authorised representatives may carry out security audits as it reasonably considers necessary in order to ensure that the ISMS is compliant with the principles and practices of ISO 27001: 2013 or equivalent (unless otherwise Approved), the requirements of this Schedule 6 and the Baseline Security Requirements.
- 7.2 If ISO/IEC 27001: 2013 certification or equivalent is provided; the ISMS shall be independently audited in accordance with ISO/IEC 27001: 2013 or equivalent. The Authority and its authorised representatives shall, where applicable, be granted access to the Contractor Sites and Sub-Contractor premises for this purpose.
- 7.3 If, on the basis of evidence resulting from such audits, it is the Authority's reasonable opinion that ISMS is not compliant with any applicable principles and practices of ISO/IEC 27001: 2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements is not being achieved by the Contractor, the Authority shall notify the Contractor of this and provide a reasonable period of time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) for the Contractor to implement any necessary remedy. If the Contractor does not ensure that the ISMS is compliant within this period of time, the Authority may obtain an independent audit of the ISMS to assess compliance (in whole or in part).
- 7.4 If, as a result of any such independent audit as described in paragraph 7.3 the Contractor is found to be non-compliant with any applicable principles and practices of ISO/IEC 27001:2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements the Contractor shall, at its own cost, undertake those actions that are required in order to ensure that the ISMS is compliant and shall reimburse the Authority in full in respect of the costs obtaining such an audit.

8. SECURITY RISKS AND BREACHES

- 8.1 The Contractor shall use its reasonable endeavours to prevent any Breach of Security for any reason, including as a result of malicious, accidental or inadvertent behaviour.
- 8.2 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall act in accordance with the agreed security incident management processes and incident response plans as set out in the ISMS.
- 8.3 Without prejudice to the security incident management processes and incident response plans set out in the ISMS and any requirements to report incidents in accordance with PSI 24/2014 if applicable, upon becoming aware of any Breach of Security or attempted Breach of Security, the Contractor shall:
- (a) immediately notify the Authority and take all reasonable steps (which shall include any action or changes reasonably required by the Authority) that are necessary to:
 - (i) minimise the extent of actual or potential harm caused by any Breach of Security;



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (ii) remedy any Breach of Security to the extent that is possible and protect the integrity of the ICT Environment (to the extent that this is within its control) and ISMS against any such Breach of Security or attempted Breach of Security;
 - (iii) mitigate against a Breach of Security or attempted Breach of Security; and
 - (iv) prevent a further Breach of Security or attempted Breach of Security in the future resulting from the same root cause failure;
 - (b) provide to the Authority and/or the Computer Emergency Response Team for UK Government ("GovCertUK") or equivalent any data that is requested relating to the Breach of Security or attempted Breach of Security within 2 Working Days of such request; and
 - (c) as soon as reasonably practicable and, in any event, within 2 Working Days following the Breach of Security or attempted Breach of Security, provide to the Authority full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis if required by the Authority and the Contractor recognises that the Authority may report significant actual or potential losses of Personal Data to the Information Commissioner or equivalent and to the Cabinet Office.
- 8.4 If any action is taken by the Contractor in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the ISMS with any ISO/IEC 27001: 2013 requirements or equivalent (as applicable), the Baseline Security Requirements and/or the requirements of this Schedule 6, any such action and change to the ISMS and/or ISMP as a result shall be implemented at the Contractor's cost.

IT Environment

- 8.5 The Contractor shall ensure that the Contractor System:
- (a) functions in accordance with Good Industry Practice for protecting external connections to the internet;
 - (b) functions in accordance with Good Industry Practice for protection from malicious code;
 - (c) provides controls to securely manage (store and propagate) all cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Authority's Cryptographic Policy as made available to the Contractor from time-to-time;
 - (d) is patched (and all of its components are patched) in line with Good Industry Practice, any Authority patching policy currently in effect and notified to the Contractor and any Contractor patch policy that is agreed with the Authority; and
 - (e) uses the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.
- 8.6 Notwithstanding paragraph 8.5, if a Breach of Security is detected in the ICT Environment, the Parties shall co-operate to reduce the effect of the Breach of Security and, if the Breach of Security causes loss of operational efficiency or loss or corruption of Information Assets and/or Authority Data, assist



Contract for the Provision of Learning and Skills at HMP & YOI Parc

each other to mitigate any losses and to recover and restore such Information Assets and Authority Data.

8.7 All costs arising out of the actions taken by the Parties in compliance with paragraphs 8.2, 8.3 and 8.6 shall be borne by:

- (a) the Contractor if the Breach of Security originates from the defeat of the Contractor's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Contractor or its Sub-Contractor; or
- (b) the Authority if the Breach of Security originates from the defeat of the Authority's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Authority

and each Party shall bear its own costs in all other cases.

9. VULNERABILITIES AND CORRECTIVE ACTION

9.1 The Parties acknowledge that from time-to-time vulnerabilities in the ICT Environment and ISMS will be discovered which, unless mitigated, will present an unacceptable risk to Information Assets and/or Authority Data.

9.2 The severity of any vulnerabilities shall be categorised by the Contractor as '*Critical*', '*Important*' and '*Other*' according to the agreed method in the ISMS and using any appropriate vulnerability scoring systems.

9.3 The Contractor shall procure the application of security patches to vulnerabilities categorised as '*Critical*' within 7 days of public release, vulnerabilities categorised as '*Important*' within 30 days of public release and vulnerabilities categorised as '*Other*' within 60 days of public release, except where:

- (a) the Contractor can demonstrate that a vulnerability is not exploitable within the context of the Services being provided, including where it resides in a software component which is not being used, provided that, where those vulnerabilities become exploitable, they are remedied by the Contractor within the timescales in paragraph 9.3;
- (b) the application of a security patch in respect of a vulnerability categorised as '*Critical*' or '*Important*' adversely affects the Contractor's ability to deliver the Services, in which case the Contractor shall be granted an extension to the timescales in paragraph 9.3 of 5 days, provided that the Contractor continues to follow any security patch test plan agreed with the Authority; or
- (c) the Authority agrees a different timescale after consultation with the Contractor in accordance with the processes defined in the ISMS.

9.4 The ISMS and the ISMP shall include provision for the Contractor to upgrade software throughout the Term within 6 months of the release of the latest version unless:



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (a) upgrading such software reduces the level of mitigation for known threats, vulnerabilities or exploitation techniques, provided always that such software is upgraded by the Contractor within 12 months of release of the latest version; or
- (b) otherwise agreed with the Authority in writing.

9.5 The Contractor shall:

- (a) implement a mechanism for receiving, analysing and acting upon threat information provided by GovCertUK, or any other competent central Government Body;
- (b) ensure that the ICT Environment (to the extent that this is within the control of the Contractor) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
- (c) ensure that it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment (to the extent that this is within the control of the Contractor) by actively monitoring the threat landscape during the Term;
- (d) pro-actively scan the ICT Environment (to the extent that this is within the control of the Contractor) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS;
- (e) from the Commencement Date and within 5 Working Days of the end of each subsequent month during the Term provide a report to the Authority detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that this is within the control of the Contractor) and any elapsed time between the public release date of patches and either the time of application or, for outstanding vulnerabilities, the time of issue of such report;
- (f) propose interim mitigation measures in respect of any vulnerabilities in the ICT Environment (to the extent this is within the control of the Contractor) known to be exploitable where a security patch is not immediately available;
- (g) remove or disable any extraneous interfaces, services or capabilities that are no longer needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment to the extent this is within the control of the Contractor); and
- (h) inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment (to the extent this is within the control of the Contractor) and provide initial indications of possible mitigations.

9.6 If the Contractor is unlikely to be able to mitigate any vulnerability within the timescales in paragraph 9.3, the Contractor shall notify the Authority immediately.

9.7 Any failure by the Contractor to comply with paragraph 9.3 shall constitute a material Default.



Contract for the Provision of Learning and Skills at HMP & YOI Parc

10. SUB-CONTRACTS

- 10.1 The Contractor shall ensure that all Sub-Contracts with Sub-Contractors who have access to Information Assets and/or Authority Data contain equivalent provisions in relation to information assurance and security that are no less onerous than those imposed on the Contractor under the Contract.



Contract for the Provision of Learning and Skills at HMP & YOI Parc

ANNEX 1 – BASELINE SECURITY REQUIREMENTS

1. Security Classifications and Controls

- 1.1 The Contractor shall, unless otherwise Approved by the Authority in writing, only have access to and handle Information Assets and Authority Data that are classified under the Government Security Classifications Scheme as OFFICIAL.
- 1.2 There may be a specific requirement for the Contractor in some instances on a limited 'need to know basis' to have access to and handle Information Assets and Authority Data that are classified as 'OFFICIAL-SENSITIVE.'
- 1.3 The Contractor shall apply the minimum security controls required for OFFICIAL information and OFFICIAL-SENSITIVE information as described in Cabinet Office guidance, currently at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.
- 1.4 The Contractor shall be able to demonstrate to the Authority and any assurer that it has taken into account the "Technical Controls Summary" for OFFICIAL (in the above guidance) in designing and implementing the security controls in the Contractor System, which shall be subject to assurance to Government standards.
- 1.5 Additional controls may be required by the Authority and any assurer where there are aspects of data aggregation.

2. End User Devices

- 2.1 Authority Data shall, wherever possible, be held and accessed on paper or in the ICT Environment on secure premises and not on removable media (including laptops, removable discs, CD-ROMs, USB memory sticks, PDAs and media card formats) without Approval. If Approval is sought to hold and access data by other means, the Contractor shall consider the second-best option and third best option below and record the reasons why a particular approach should be adopted when seeking Approval:
 - (a) second best option means: secure remote access so that data can be viewed or amended over the internet without being permanently stored on the remote device, using products meeting the FIPS 140-2 standard or equivalent, unless Approved;
 - (b) third best option means: secure transfer of Authority Data to a remote device at a secure site on which it will be permanently stored, in which case the Authority Data and any links to it shall be protected at least to the FIPS 140-2 standard or equivalent, unless otherwise Approved, and noting that protectively marked Authority Data must not be stored on privately owned devices unless they are protected in this way.
- 2.2 The right to transfer Authority Data to a remote device should be carefully considered and strictly limited to ensure that it is only provided where absolutely necessary and shall be subject to monitoring by the Contractor and Authority.



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- 2.3 Unless otherwise Approved, when Authority Data resides on a mobile, removable or physically uncontrolled device, it shall be:
- (a) the minimum amount that is necessary to achieve the intended purpose and should be anonymised if possible;
 - (b) stored in an encrypted form meeting the FIPS 140-2 standard or equivalent and using a product or system component which has been formally assured through a recognised certification process of NCSC to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("**CPA**") or equivalent, unless otherwise Approved;
 - (c) protected by an authentication mechanism, such as a password; and
 - (d) have up to date software patches, anti-virus software and other applicable security controls to meet the requirements of this Schedule 6.
- 2.4 Devices used to access or manage Authority Data shall be under the management authority of the Contractor and have a minimum set of security policy configurations enforced. Unless otherwise Approved, all Contractor devices shall satisfy the security requirements set out in the NCSC End User Devices Platform Security Guidance ("**NCSC Guidance**") (<https://www.gov.uk/government/collections/end-user-devices-security-guidance--2>) or equivalent.
- 2.5 Where the NCSC Guidance highlights shortcomings in a particular platform the Contractor may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. If the Contractor wishes to deviate from the NCSC Guidance, this should be agreed in writing with the Authority on a case-by-case basis.
- 3. Data Storage, Processing, Management, Transfer and Destruction**
- 3.1 The Parties recognise the need for Authority Data to be safeguarded and for compliance with the Data Protection Legislation. To that end, the Contractor shall inform the Authority the location within the United Kingdom where Authority Data is stored, processed and managed. The import and export of Authority Data from the Contractor System must be strictly controlled and recorded.
- 3.2 The Contractor shall inform the Authority of any changes to the location within the United Kingdom where Authority Data is stored, processed and managed and shall not transmit, store, process or manage Authority Data outside of the United Kingdom without Approval from the Authority.
- 3.3 The Contractor shall ensure that the Contractor System provides internal processing controls between security domains to prevent the unauthorised high domain exporting of Authority Data to the low domain if there is a requirement to pass data between different security domains.
- 3.4 The Contractor shall ensure that any electronic transfer of Authority Data:
- (a) protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data;
 - (b) maintains the integrity of the Authority Data during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data; and



Contract for the Provision of Learning and Skills at HMP & YOI Parc

- (c) prevents the repudiation of receipt through accounting and auditing.

3.5 The Contractor shall:

- (a) protect Authority Data, including Personal Data, whose release or loss could cause harm or distress to individuals and ensure that this is handled as if it were confidential while it is stored and/or processed;
- (b) ensure that any OFFICIAL-SENSITIVE information, including Personal Data is encrypted in transit and when at rest when stored away from the Contractor's controlled environment;
- (c) on demand, provide the Authority with all Authority Data in an agreed open format;
- (d) have documented processes to guarantee availability of Authority Data if it ceases to trade;
- (e) securely destroy all media that has held Authority Data at the end of life of that media in accordance with any requirements in the Contract and, in the absence of any such requirements, in accordance with Good Industry Practice;
- (f) securely erase any or all Authority Data held by the Contractor when requested to do so by the Authority;
- (g) ensure that all material used for storage of Confidential Information is subject to controlled disposal and the Contractor shall:
 - (i) destroy paper records containing Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and
 - (ii) dispose of electronic media that was used for the processing or storage of Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.

4. Networking

- 4.1 Any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA or through the use of Public Sector Network ("PSN") compliant encrypted networking services or equivalent unless none are available in which case the Contractor shall agree the solution with the Authority.
- 4.2 The Contractor shall ensure that the configuration and use of all networking equipment in relation to the provision of the Services, including equipment that is located in secure physical locations, shall be at least compliant with Good Industry Practice.
- 4.3 The Contractor shall ensure that the ICT Environment (to the extent this is within the control of the Contractor) contains controls to maintain separation between the PSN and internet connections if used.

Contract for the Provision of Learning and Skills at HMP & YOI Parc**5. Security Architectures**

- 5.1 When designing and configuring the ICT Environment (to the extent that this is within the control of the Contractor) the Contractor shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills for all bespoke or complex components.
- 5.2 The Contractor shall provide to the Authority and any assurer sufficient design documentation detailing the security architecture of the ICT Environment and data transfer mechanism to support the Authority's and any assurer's assurance that this is appropriate, secure and compliant with the Authority's requirements.
- 5.3 The Contractor shall apply the '*principle of least privilege*' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of the ICT Environment used for the storage, processing and management of Authority Data. Users should only be granted the minimum necessary permissions to access Information Assets and Authority Data and must be automatically logged out of the Contractor System if an account or session is inactive for more than 15 minutes.

6. Digital Continuity

The Contractor shall ensure that each Information Asset is held in an appropriate format that is capable of being updated from time to time to enable the Information Asset to be retrieved, accessed, used and transferred to the Authority, including in accordance with any information handling procedures set out in PSI 24/2014 (Information Assurance) if applicable.

7. Personnel Vetting and Security

- 7.1 All Staff shall be subject to pre-employment checks that include, as a minimum, their employment history for at least the last 3 years, identity, unspent criminal convictions and right to work (including nationality and immigration status) and shall be vetted in accordance with:
- (a) the BPSS or BS7858 or equivalent; and
 - (b) PSI 07/2014, if applicable, based on their level of access to Information Assets and/or Authority Data.
- 7.2 If the Authority agrees that it is necessary for any Staff to have logical or physical access to Information Assets and/or Authority Data classified at a higher level than OFFICIAL (such as that requiring 'SC' clearance), the Contractor shall obtain the specific Government clearances that are required for access to such Information Assets and/or Authority Data.
- 7.3 The Contractor shall prevent Staff who are unable to obtain the required security clearances from accessing Information Assets and/or Authority Data and/or the ICT Environment used to store, process and/or manage such Information Assets or Authority Data.
- 7.4 The Contractor shall procure that all Staff comply with the Security Policy Framework and principles, obligations and policy priorities stated therein, including requirements to manage and report all security risks in relation to the provision of the Services.



Contract for the Provision of Learning and Skills at HMP & YOI Parc

7.5 The Contractor shall ensure that Staff who can access Information Assets and/or Authority Data and/or the ICT Environment are aware of their responsibilities when handling such information and data and undergo regular training on secure information management principles. Unless otherwise Approved, this training must be undertaken annually.

7.6 If the Contractor grants Staff access to Information Assets and/or Authority Data, those individuals shall be granted only such levels of access and permissions that are necessary for them to carry out their duties. Once Staff no longer require such levels of access or permissions or leave the organisation, their access rights shall be changed or revoked (as applicable) within 1 Working Day.

8. Identity, Authentication and Access Control

8.1 The Contractor shall operate a robust role-based access control regime, including network controls, to ensure all users and administrators of and those maintaining the ICT Environment are uniquely identified and authenticated when accessing or administering the ICT Environment to prevent unauthorised users from gaining access to Information Assets and/or Authority Data. Applying the '*principle of least privilege*', users and administrators and those responsible for maintenance shall be allowed access only to those parts of the ICT Environment they require. The Contractor shall retain an audit record of accesses and users and disclose this to the Authority upon request.

8.2 The Contractor shall ensure that Staff who use the Authority System actively confirm annually their acceptance of the Authority's acceptable use policy.

9. Physical Media

9.1 The Contractor shall ensure that all:

- (a) OFFICIAL information is afforded physical protection from internal, external and environmental threats commensurate with the value to the Authority of that information;
- (b) physical components of the Contractor System are kept in secure accommodation which conforms to the Security Policy Framework and NCSC standards and guidance or equivalent;
- (c) physical media holding OFFICIAL information is handled in accordance with the Security Policy Framework and NCSC standards and guidance or equivalent; and
- (d) Information Assets and Authority Data held on paper are:
 - (i) kept secure at all times, locked away when not in use on the premises on which they are held and secured and are segregated if the Contractor is co-locating with the Authority; and
 - (ii) only transferred by an approved secure form of transfer with confirmation of receipt obtained.



Contract for the Provision of Learning and Skills at HMP & YOI Parc

10. Audit and Monitoring

- 10.1 The Contractor shall implement effective monitoring of its information assurance and security obligations in accordance with Government standards and where appropriate, in accordance with NCSC Guidance.
- 10.2 The Contractor shall collect audit records which relate to security events in the ICT Environment (where this is within the control of the Contractor), including those that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such Contractor audit records shall include:
- (a) logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent it is within the control of the Contractor). To the extent, the design of the ICT Environment allows, such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers;
 - (b) regular reports and alerts giving details of access by users of the ICT Environment (to the extent that it is within the control of the Contractor) to enable the identification of changing access trends any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data; and
 - (c) security events generated in the ICT Environment (to the extent it is within the control of the Contractor) including account logon and logoff events, start and end of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
- 10.3 The Parties shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 10.4 The Contractor shall retain audit records collected in compliance with paragraph 10.1 for at least 6 months.