**DYNAMIC FRAMEWORK**

**SCHEDULE 2.3**

**STANDARDS**

|  |  |  |
| --- | --- | --- |
| **VERSION** | **DATE** | **COMMENT** |
| 1.0 | 10 June | Initial Release |
|  |  |  |
|  |  |  |

**SCHEDULE 2.3**

**STANDARDS**

1. Introduction
	1. Throughout the Call-Off Term the Supplier shall comply with each of the Standards identified below in accordance with the level of Security Requirements set out in the Call-Off Contract, as more particularly described in Schedule 2.4 (Information Security and Assurance).
	2. Any deviation or amendment to Standards (as may be required by a Customer) shall be expressly set out in the Call-Off Order Form for the relevant Call-Off Contract.
2. GENERAL
	1. Throughout the Call-Off Term of any Call-Off Contract, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Customer's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.
	2. Where a new or emergent standard is to be developed or introduced by the Customer, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Customer's receipt, of the Services is explained to the Customer (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
	3. Where Standards referenced conflict with each other or with Market Practice then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Customer of the relevant Call-Off Contract and shall be implemented within an agreed timescale.
3. STANDARDS, GUIDANCE AND POLICIES

The list below is a non-exhaustive list of standards and guidance location(s) with which the Supplier, Supplier System and the Services shall, as applicable to each element of the Services (and in accordance with the level of security requirements identified in accordance with Schedule 2.4 (Information Security and Assurance) as being relevant to the Call-Off Contract), comply at all times throughout a Call-Off Term. This list is supplementary to, in support of or may be superseded by other published commercial best practices/guidance. This list is correct at the time of issue and may be iterated from time to time.

|  |  |  |
| --- | --- | --- |
|  |  | **Level of Standards applicable** |
| Guidance & Policies | Location | **Basic** | **Normal** | **Enhanced** |
| Ministry of Justice Data Sharing Principles | <https://mojdigital.blog.gov.uk/2016/10/06/data-principles-the-right-ingredients-to-solving-the-data-spaghetti-problem/> |  |  | X |
| APIs and System Integration Standard | <https://www.gov.uk/guidance/gds-api-technical-and-data-standards> |  |  | X |
| Email Security Standard | <https://www.gov.uk/government/publications/email-security-standards> | X | X | X |
| Digital Service Standard | <https://www.gov.uk/service-manual/service-standard> |  | X | X |
| Open Standards for Government | <https://www.gov.uk/government/publications/open-standards-for-government> |  |  | X |
| UK HMG Technology Code of Practice | <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice> |  |  | X |
| Minimum Cyber Security Standard | <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard> | Cyber Essentials Basic | Cyber Essential PLUS  | Cyber Essential PLUS |
| ISO/IEC 20000 (Information Technology Service Management) | <http://www.iso.org> |  |  | X |
| ISO/IEC 27001 (Information Security Management) | <https://www.iso.org/isoiec-27001-information-security.html> |  | (as applicable) | X |
| [MoJ Security Guidance](https://ministryofjustice.github.io/security-guidance/#moj-security--guidance) | [https://ministryofjustice.github.io/security-guidance/#moj-security—guidance](https://ministryofjustice.github.io/security-guidance/%23moj-security%E2%80%94guidance) | X | X | X |
| eNational Cyber Security Centre (guidance) | <https://www.ncsc.gov.uk/guidance> |  |  | X |
| National Cyber Security Centre (risk management) | <https://www.ncsc.gov.uk/guidance/risk-management-collection> |  |  | X |
| National Cyber Security Centre (CHECK Green scheme) | <https://www.ncsc.gov.uk/scheme/penetration-testing> |  | X | X |
| NCSC Cloud Security Principles | [www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles](http://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles) |  | X | X |
| Government Security Classifications | <https://www.gov.uk/government/publications/government-security-classifications> | X | X | X |
| Security Policy Framework | <https://www.gov.uk/government/collections/government-security#security-policy-framework> |  | X | X |
| ISO 10007 (Quality Management – Guidelines for Configuration Management) | <http://www.iso.org> |  |  | X |
| ISO/IEC 22301 (Security and Resilience - Business Continuity Management Systems - Requirements) | <http://www.iso.org> | X | X | X |
| ISO/IEC 44001 (Collaborative Business Relationship Management Systems – Requirements and Framework) | <http://www.iso.org> |  |  | X |
| UK Government Baseline Personnel Security Standards and the relevant Probation Instructions (the "**Baseline Security Requirements**") | <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf> |  |  | X |
| HMPPS Security Documents (HMPPS Incident Management Policy, and where relevant HMPPS SyOPS/AUP) |  | X | X | X |
| HM Prison & Probation Service – Records, Information Management and Retention Policy | <https://www.justice.gov.uk/downloads/offenders/psipso/psi-2018/psi-04-2018-records-information-management-retention-policy.pdf> | X | X | X |
| HM Prison & Probation Service Information Security Policy Framework  | <https://www.gov.uk/government/publications/information-security-policy-framework>  | X | X | X |
| HM Prison & Probation Service – Information Risk Management Policy  | <https://www.justice.gov.uk/downloads/offenders/psipso/psi-2016/PSI-06-2016-PI-08-2016-AI-08-2016-Information-Risk-Management-Policy.docx>  |  | X | X |
| HM Prison & Probation Service – IT Security Policy | <https://www.justice.gov.uk/downloads/offenders/psipso/psi-2014/psi-25-2014-it-security-policy.pdf> |  |  | X |
| HM Prison & Probation Service – The Data Protection Act 2018 and General Data Protection regulation, The Freedom of Information Act 2000 and Environmental Information Regulations 2004 instruction | <https://www.justice.gov.uk/downloads/offenders/psipso/psi-2018/psi-03-2016-dpa-foi-eir.pdf>  |  |  | X |

1. ENVIRONMENTAL STANDARDS
	1. The Supplier warrants that it has either obtained ISO 14001 (Environmental Management Systems – Requirements for Guidance and Use) (or equivalent) certification for its environmental management and shall comply with and maintain certification requirements throughout any Call-Off Term or shall follow a sound environmental management policy, ensuring that any Goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.
	2. The Supplier shall, as appropriate, (when designing, procuring, implementing and delivering the Services) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.
	3. The Supplier shall work within the Customer's and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document Greening Government: ICT Strategy issue (March 2011) at https://www.gov.uk/government/publications/greening-government-ict-strategy.
2. SAFETY STANDARDS

The Supplier shall comply with those British Standards or other standards relevant to the provision of the Services and any new hardware required for the delivery of the Services.

1. Sub-Contractors

The Supplier will ensure that all Sub-contractors, Sub-processors and supply-chain of the Supplier adhere to the Standards and policies set out in this Schedule (Standards).