

DMP SCHEDULE 19: VARIATION FORM

Variation Form No: 001

BETWEEN:

- (1) **THE MINISTER FOR THE CABINET OFFICE (“Cabinet Office”)** as represented by Crown Commercial Service (formerly Government Procurement Service), a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool, L3 9PP (**“Authority”**);
- (2) **[Insert Supplier Name]** whose offices are at **[Insert Suppliers Address]** (**“Supplier”**),

WHEREAS the SUPPLIER and the AUTHORITY entered into a Commercial Agreement for the provision of Apprenticeship Training Dynamic Marketplace DPS dated 30th April 2019 the AUTHORITY now wish to vary that Commercial Agreement as set out below.

1. This Dynamic Marketplace Agreement is varied as follows:
2. Status of this Agreement - This variation agreement is supplemental to the Commercial Agreement. Except as expressly amended by this variation agreement and any previous variation agreement, the Commercial Agreement shall remain in full force and effect. Terms defined in the Commercial Agreement shall have the same meaning in this variation agreement, unless otherwise provided by this variation agreement.
3. The variation to the DMP Schedule 23 Security Management shall be varied as follows:

Dynamic Marketplace Agreement V1, DMP Schedule 23 Security Management

Not used for the following sections:

- 5 Information Risk Management Approval of the Information System**
- 7 Security Testing**

4. This Variation must be agreed and signed by both Parties and shall only be effective from the date it is signed by the Authority.
5. Words and expressions in this Variation shall have the meanings given to them in the Dynamic Marketplace Agreement.
6. The Dynamic Marketplace Agreement, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Variation to Dynamic Marketplace Agreement

Signed for and on behalf of the AUTHORITY

Signature.....

Print Name.....

Job Title.....

Date.....

Signed for and on behalf of the SUPPLIER

Signature.....

Print Name.....

Job Title.....

Date.....

DMP SCHEDULE 23: SECURITY MANAGEMENT**1 DEFINITIONS**

In this DMP Schedule 23, the following definitions shall apply:

“Baseline Security Implementation Objectives”	Has the meaning set out in Appendix 1 of this DMP Schedule 23.
“Breach of Security”	<p>the occurrence of:</p> <p>(a) any unauthorised access to or use of the Services, the Authority’s Premises, the Sites, the Information System and/or any information or data (including the Confidential Information and the Authority Data) used by the Supplier or any Sub-Contractor in connection with this Agreement;</p> <p>(b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Supplier or any Sub-Contractor in connection with this Agreement; and/or</p> <p>any part of the Information System ceasing to be compliant with the Certification Requirements;</p> <p>in either case as more particularly set out in the security requirements in Schedule 2.1 (<i>Services Description</i>) and the Baseline Security Requirements;</p>
“Certification Requirements”	Means the requirements given in paragraph 6 of this DMP Schedule 23
“Information System”	Has the meaning given in paragraph 3.1 of this DMP Schedule 23
“COTS Products”	<p>is software that:</p> <p>(a) the licensor of that software makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the licensor save as to price; and</p> <p>has a Non-trivial Customer Base</p>
“Risk Appetite”	The security risks the Authority will accept or not accept to achieve the organizational goals
“Information Risk Management Approval”	Is the assessment of any information system by an independent information risk manager/professional which results in a statement that the risks to the information system have been appropriately

	considered and the residual risks reduced to an acceptable level
“Risk Management Approval Statement”	Sets out the information risks associated with using the “THE Information System
“Data”	All information (including pensions data) provided to the Supplier by the Authority
“Security Delivery Outcomes”	Has the meaning set out in Appendix 2 of this DMP Schedule 23.
“Statement of Information Risk Appetite”	Has the meaning given in paragraph 4.1 of this DMP Schedule 23 and Appendix 3.

1 Introduction

- 1.1 This DMP Schedule 23 sets out the principles of protective security to be applied by the Supplier in performing its obligations under this DMP Agreement and in delivering the Services.
- 1.2 This DMP Schedule 23 also sets out:
 - 1.2.1 the process which shall apply to the Information Risk Management Approval of the Information System;
 - 1.2.2 the requirement for the Supplier to ensure that:
 - (a) each Sub-Contractor who will Process the Data; and
 - (b) any ICT system which the Supplier or its Sub-Contractors will use to store, process or transmit the Data, it is and continues to be compliant with the Certification Requirements;
 - (c) the requirements on the Supplier to conduct Security Tests; and
 - (d) each Party's obligations in the event of an actual or attempted Breach of Security.

2. Principles of Security

- 2.1 The Supplier shall have a Board level responsibility for proactively managing the information security risk associated with the service. This responsible Board member shall ensure:
 - 2.1.1 The Authorities security approval is obtained prior to the service processing any HMG data;
 - 2.1.2 The effective delivery of Security controls throughout the period of this DMP
 - 2.1.3 Agreement; and

Variation to Dynamic Marketplace Agreement

- 2.1.4 Any change to the service is subject to a security impact assessment and any which have a major impact upon the service security policy are notified to the Authority.
 - 2.2 Each Party shall provide access to members of its information assurance personnel in accordance with the Security Management Plan to facilitate the design, implementation, operation, management and continual improvement of the Risk Management Documentation and the security of the Information System and otherwise at reasonable times on reasonable notice. The Security Plan shall address the high level Security Delivery Outcomes defined in Appendix 2.
3. **The Information System**
- 3.1 The information assets, ICT systems, associated business processes and/or premises which have been agreed between the parties to constitute the system and shall be detailed in a diagram included in the Risk Management Documentation.

- 3.2 The Authority may change the scope of the Information System in accordance with the process set out in Clause 19 (Change) of this DMP Agreement.

4. **Statement of Information Risk Appetite and Baseline Security Requirements**

- 4.1 The Authority has provided the Supplier with its Statement of Information Risk Appetite for the Information System and the Services (the Statement of Information Risk Appetite – Appendix 3).
- 4.2 The Authority's Baseline Security Implementation Objectives in respect of the Information System are set out in Appendix 1.
- 4.3 The Statement of Information Risk Appetite and the Baseline Security Implementation Objectives shall inform the Information Risk Management Approval of the Information System.

5. **Information Risk Management Approval of the Information System – NOT USED**

- 5.1 The Information System shall be subject to Information Risk Management Approval in accordance with this Paragraph 5 and reviewed annually.
- 5.2 Information Risk Management Approval of the Information System shall be performed by representatives appointed by the Authority.
- 5.3 The Supplier shall prepare risk management documentation (the Risk Management Documentation") for any part of the Information System which is not subject to a separate HMG Risk Management Approval process, which shall be subject to approval by the Authority in accordance with this Paragraph 5.

Variation to Dynamic Marketplace Agreement

- 5.4 The Risk Management Documentation shall be structured in accordance with the template as agreed with the Authority and include:
- 5.4.1 an initial Security Management Plan which shall include:
- (a) define compliance with the security delivery objective described in Appendix 2.
 - (b) the dates on which each subsequent iteration of the Risk Management Documentation will be delivered to the Authority for review and staged approval;
 - (c) the date by which the Information System must achieve Risk Management Approval and acceptance of residual risks ("Approval Date");
 - (d) the tasks, milestones, timescales and any dependencies on the Authority for the security approval of the Information System.
- 5.4.2 evidence that the Supplier and each applicable Sub-Contractor is compliant with the Assurance Requirements.
- 5.5 The Authority shall, by the relevant date set out in the Security Management Plan, issue a Risk Management Approval Statement which will form part of the Risk Management Documentation ("Risk Management Approval Statement ") confirming either:
- 5.5.1 that the Authority is satisfied that the identified risks to the Information System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority.
- 5.5.2 the Authority considers that the residual risks to the Information System have not been reduced to a level acceptable by the Authority.
- 5.6 The Supplier acknowledges that it shall not be permitted to use the Information System to receive, store or Process any Data until the Board Level responsible individual has confirmed that all residual risks are being managed. The Authority shall be notified of any such decision and shall be presented within 20 days of any such decision being made an agreed set of documentation to enable independent assurance that the risk which is being managed is within the Authority's Risk Appetite. If the Authority is not content that the risks are within the stated risk appetite the supplier shall be informed in writing and shall take immediate action to put in place additional security controls as directed by the Authority.
- 5.7 The Supplier shall keep the Information System and the Risk Management Documentation under review and shall update this documentation at least annually and the Supplier shall submit each update to the Information Risk Management Documentation to the Authority for approval as appropriate.
- 5.8 The Supplier shall review each request for a Variation against the Information Risk Management Documentation to establish whether the documentation would need to be amended and should an amendment be necessary to the Information Risk Management Documentation, the Supplier shall submit the updated document for consideration and approval by the Authority.

- 5.9 The Supplier shall be solely responsible for the costs associated with developing and updating the Information Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Information Risk Management Approval process.

6. Certification Requirements

- 6.1 The Supplier shall ensure at all times during the DMP Period the Services are compliant with Cyber Essentials requirement and shall provide the Authority with a copy of each such Certificate of compliance. Unless otherwise agreed with the Authority the Supplier shall not be permitted to operate the Information System to receive, store or Process any Authority Data unless such certification is in place.
- 6.2 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, should it cease to be compliant with the Certification Requirements and, on request from the Authority:
- 6.2.1 immediately ceases using the Data; and
 - 6.2.2 promptly returns, destroys and/or erases the Data in accordance with Baseline Security Requirements.

7. Security Testing – NOT USED

- 7.1 The Supplier shall, at its own cost and expense, when it Processing Authority Data:
- 7.1.1 undertake the security assurance activities as defined in the “Authority’s” Security Assurance Framework to evidence that the risk is within the Authority’s risk tolerance. The Supplier can propose alternative security testing not defined in the Security Assurance Framework but shall need to demonstrate to the satisfaction of the “Authority’s” security assurance lead that the proposed Security test delivers comparable level of assurance to test defined in the security assurance framework.
 - 7.1.2 procure a Security Test of the Information System by a NCSC approved member of the CHECK Scheme once every 12 months during the DMP Period unless additional IT Health Checks are required by Paragraph 7.2;
 - 7.1.3 commission external vulnerability scanning of the “Information System monthly;
 - 7.1.4 conduct such other tests as are required by:
 - (a) any Vulnerability Correction Plans;
 - (b) the Information Risk Management Documentation; and
 - (c) the Authority following a Breach of Security or a significant change to the components or architecture of the Information System, (each a "Security Test").
- 7.2 In relation to each Security Test, the Supplier shall promptly, following receipt of each Security Test report:
- 7.2.1 provide the Authority with a copy of the Security Test report;
 - 7.2.2 in the event that the Security Test identifies any issues, the Supplier shall define a remedial plan by the Authority (each a "Vulnerability Correction Plan") which sets out in respect of each issue identified in the Security Test report:
- 7.3 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier’s ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

- 7.4 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including security tests by CHECK certified company) as it may deem necessary in relation to the Service, the Information System and/or the Supplier's compliance with the Information Risk Management Documentation. The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Security Tests to the extent that it is reasonably practicable for it to do so taking into account the nature of the Security Test.
- 7.5 The Authority shall notify the Supplier of the results of such Security Tests after completion of each such test.
- 7.6 The Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If such Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance to the extent directly arising as a result of the Authority and/or its authorised representatives carrying out such Security Tests.
- 7.7 Without prejudice to the provisions of Paragraph 7.2.2, where any Security Test carried out pursuant to this Paragraph 7 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Information System and/or the Information Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness.
- 7.8 Where the Supplier shall implement such changes to the Information System and/or the Information Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.
- 7.9 For the avoidance of doubt, where a change to the Information System and/or the Information Risk Management Documentation is required to remedy non-compliance with the Information Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.
- 7.10 If any repeat Security Test carried out pursuant to Paragraph 7.7 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.
- 7.11 On each anniversary of the DMP Commencement Date, the Supplier shall provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:
- 7.11.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this DMP Agreement; and

7.11.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

8. Breach of Security – General Principles

- 8.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Information Risk Management Documentation.
- 8.2 Without prejudice to the security incident management process set out in the Information Risk Management Documentation, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:
- 8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to:
- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
 - (b) remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security;
 - (c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and
 - (d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;
- 8.2.2 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 of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.
- 8.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance of the Information System and/or the Information Risk Management Documentation with the Baseline Security Requirements and/or this DMP Agreement, then such action and any required change to the Information System and/or Information Risk Management Documentation shall be at no cost to the Authority.

9. Breach of Security – IT Environment

Variation to Dynamic Marketplace Agreement

- 9.1 The Supplier shall, as an enduring obligation throughout the DMP Period, use its reasonable endeavours to prevent any Breach of Security for any reason including as a result of malicious, accidental or inadvertent behaviour. In accordance with the patching policy (which shall form part of the Information Risk Management Documentation and which shall be agreed with the Authority), this shall include an obligation to use the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.
- 9.2 Notwithstanding Paragraph 9.1, if a Breach of Security is detected in the Authority System or the Information System, the Parties shall co-operate to reduce the effect of the Breach of Security and, particularly if the Breach of Security causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any losses and to restore the Ordered Services to their desired operating efficiency.
- 9.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraphs 8 and 9.2 shall be borne by the Parties as follows:
 - 9.3.1 by the Supplier where the Breach of Security originates from defeat of the Supplier's or any Sub-Contractor's security controls, the Supplier Software, the Third Party Software or the Data (whilst the Data was under the control of the Supplier);
 - 9.3.2 by the Authority if the Breach of Security originates from defeat of the Authority's security controls or the Data (whilst the Data was under the control of the Authority); and
 - 9.3.3 in all other cases each Party shall bear its own costs.

10. Vulnerabilities and Corrective Action

- 10.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information System will be discovered which unless mitigated will present an unacceptable risk to the Data.
- 10.2 The severity of threat vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Information Risk Management Documentation and using the appropriate vulnerability scoring systems including:
 - 10.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and
 - 10.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 10.3 The Supplier shall procure the application of security patches to vulnerabilities in the Information System within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 7 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:
 - 10.3.1 the Supplier can demonstrate that a vulnerability in the Information System is not exploitable within the context of the Services (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of the Services must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Services;
 - 10.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or
 - 10.3.3 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Information Risk Management Documentation.
- 10.4 The Information Risk Management Documentation shall include provisions for major version upgrades of all Supplier Software and Third Party Software which are COTS Products to be kept up to date such that all Supplier Software and Third Party Software which are COTS Products are always in mainstream support throughout the DMP Period unless otherwise agreed by the Authority in writing.
- 10.5 The Supplier shall:
 - 10.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

Variation to Dynamic Marketplace Agreement

- 10.5.2 promptly notify GovCertUK of any actual or sustained attempted Breach of Security;
- 10.5.3 ensure that the Information System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
- 10.5.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Information System by actively monitoring the threat landscape during the DMP Period;
- 10.5.5 pro-actively scan the Information System for vulnerable components and address discovered vulnerabilities through the processes described in the Information Risk Management Documentation;
- 10.5.6 ensure that the Board person responsible shall ensure that the service is patched in accordance with the timescales specified to achieve the security outcomes
- 10.5.7 propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
- 10.5.8 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Information System); and
- 10.5.9 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 Information System and provide initial indications of possible mitigations.
- 10.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Supplier shall immediately notify the Authority.
- 10.7 A failure to comply with Paragraph 10.3 shall constitute a material Default.

11 Service Decommissioning

- 11.1 On termination of the DMP Agreement or where an Authority ceases to use the DMP agreement the Supplier shall:
 - 11.1.1 on demand, provide: the Authority with all Data in an agreed open format;
 - 11.1.2 have documented processes to guarantee availability of Data in the event of the Supplier ceasing to trade;
 - 11.1.3 securely erase any or all Data held by the Supplier when requested to do so by the Authority; and
 - 11.1.4 securely destroy all media that has held Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, in accordance with Good Industry Practice.

12 Audit and Monitoring

- 12.1 The Supplier shall collect audit records which relate to security events in the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should be made available to the Authority, within 5 days, when requested
- 12.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Information System.
- 12.3 The Supplier shall retain audit records collected in compliance with this provision until the Service.

Appendix 1 - Baseline Security Requirements

1.1 Data Security Outcomes

The Security Policy defines the security characteristics of the Service supplied under the Contract. The Supplier shall assert, and evidence compliance, of the Service Supplied under the Contract against the Data Security Outcomes defined at Annex 1. The Security Policy describes the required security outcomes which the service shall need to achieve, in order to provide the Contracting Authority with the assurance and confidence that the Security Risk is being appropriately managed.

The Supplier shall also be cognisant of the need to support the Contracting Authorities compliance with EU data protection legislation throughout the life of the Contract.

1.2 Handling, Processing and Storage of OFFICIAL-SENSITIVE information

Where the Supplier is going to handle, process and store OFFICIAL-SENSITIVE information, the Supplier shall implement additional measures to secure data of this type throughout the lifecycle of the Contract. The measures defined herein are in addition to the Supplier delivering a Service where the residual risk associated with the Service Supplied under the Contract is acceptable to the Contracting Authority. For a Supplier Service to handle OFFICIAL-SENSITIVE data the residual risk associated with the additional measures defined below shall be considered acceptable to the Contracting Authority. The additional measures have been cross referenced to the relevant Security Principle headline defined within the Security Policy.

Serial	Security Principle Headline	Additional Measures
1.	Asset Protection and Resilience	<p>The Supplier shall provide evidence that the infrastructure devices storing any bulk Authority data shall not be directly accessible from a device hosted on the internet. The Supplier shall assure the protection afforded to bulk data addresses the NCSC guidance https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-introduction</p>
2.	Governance	<p>The Supplier shall provide evidence of robust handling processes throughout the lifecycle of all information held on the system which conforms to the definition of personal data defined within the Data Protection Act 1998 or other UK regulatory requirements. The robust handling procedures will need to specify the procedural measures implemented to ensure:</p> <ul style="list-style-type: none"> • There are clearly defined roles associated with any access to bulk Authority data. • Where a role is identified as having access to bulk Authority data there shall be defined responsibilities which detail any actions which can be performed in support of maintaining Service availability. • There shall be a process defined which authorises

Variation to Dynamic Marketplace Agreement

		<p>Supplier staff to be able access to bulk Authority data for purposes of delivering and maintaining the Service availability.</p> <ul style="list-style-type: none"> Any individual being given access to bulk Authority data is aware of the HMG requirements for data protection. The Supplier nominates an individual within its organisation who is independent from the programme delivery team and is responsible for ensuring the enforcement of the measures defined above.
3.	Operational security	<p>This Supplier incident reporting process shall include reporting security incidents to the Data Controller and ICO</p> <p>The supplier shall agree with Authority triggers and timescales for sharing such incidents with service Contracting Authority (s) which have compromised OFFICIAL-SENSITIVE data.</p> <p>The Supplier shall publish and agreed with the Authority the content and format of security incident notifications for sharing information involving OFFICIAL SENSITIVE. The Supplier shall agree with the Authority a restricted distribution group with individuals who have a “need to know” for incident involving OFFICIAL SENSITIVE data.</p>

ANNEX 1: SECURITY POLICY**Data Security Principles/Implementation Objectives Matrix**

	Headline	Principle	Sub-points	Implementation Objectives
1	Data in transit protection	OFFICIAL data transiting from a Contracting Authority service consumer across untrusted networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected between the Contracting Authority's end user devices and the service.
		OFFICIAL data transiting the Supplier's internal networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected internally within the service.
		OFFICIAL data transiting untrusted networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected between the service and other services (e.g. where APIs are exposed).
2	Asset protection and resilience	Contracting Authority or Contracting Authority data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or	Physical location and legal jurisdiction	Suppliers shall ensure that the following information is made available to the Contracting Authorities: The geographic locations where Contracting Authority data is stored, processed or managed

Variation to Dynamic Marketplace Agreement

		<p>seizure.</p> <p>OFFICIAL data shall be protected to a level which is comparable with that required under UK legislation</p>		<p>from.</p> <p>The applicable legal jurisdictions that the Suppliers operates within and how it provides comparable controls to those required under UK legislation.</p> <p>The Contracting Authority (where applicable) shall be informed of any changes to the above.</p>
		<p>OFFICIAL data shall physical protection against unauthorised access, tampering, theft and /or reconfiguration of data processing services.</p>	<p>Datacentre security</p>	<p>Data processing locations used to deliver the service are adequately protected.</p>
		<p>OFFICIAL data when stored on any type of removable media or storage within a service shall not be accessible by local unauthorised parties.</p>	<p>Data at rest protection</p>	<p>The Contracting Authority has confidence that removable storage media containing their data is adequately protected from unauthorised access.</p>
		<p>The process of provisioning, migrating and de-provisioning resources shall not result in unauthorised access to the Contracting Authority's data.</p>	<p>Data sanitisation - retention period</p>	<p>The Suppliers shall inform Contracting Authority's how long it will take to securely erase Contracting Authority data (including from any backups) from the Services.</p>
			<p>Data sanitisation - Contracting Authority on-boarding and off-</p>	<p>The Supplier shall securely erase Contracting Authority data when components are moved or re-provisioned, upon request by the Contracting Authority or when the Contracting Authority</p>

Variation to Dynamic Marketplace Agreement

			boarding	leaves the service. The Supplier shall sanitise media in accordance with NCSC guidance https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
		Once equipment used to deliver the service reaches the end of its useful life it should be disposed of in a way that does not compromise the security of the service or Contracting Authority's data	Equipment Disposal	All equipment potentially holding Contracting Authority data, credentials, or configuration information for the service shall be identified. Storage media which has held Contracting Authority data shall be appropriately sanitised or securely destroyed at the end of its lifecycle. Accounts or credentials specific to the redundant equipment are revoked.
		The service shall have the ability to operate normally in the event of failures, incidents or attacks	Physical resilience and availability	The Supplier shall clearly articulate the availability capabilities and commitments of the service. The service has adequate resiliency measures in place.
3	Separation between tenants	Separation should exist between Contracting Authority (s) of a service to prevent a malicious or compromised Contracting Authority from affecting the confidentiality, integrity or availability of another Contracting Authority of the service.		The Contracting Authority should be informed of any other Contracting Authority they share the platform or service with Separation between Contracting Authority (s) shall be enforced at all points within the service where the service is exposed to Contracting Authority (s). One Contracting Authority shall not be able to affect the confidentiality, integrity or availability of another Contracting Authority.

Variation to Dynamic Marketplace Agreement

4	Governance	The Supplier has a security governance framework that co-ordinates and directs the provider's overall approach to the management of ICT systems, services and information.	IA Risk Management Processes	<p>A clearly identified, and named, board representative (or a person with the direct delegated authority of) shall be responsible for the security of the cloud service. This is typically someone with the title Chief Security Officer, Chief Information Officer or Chief Technical Officer.</p> <p>The Supplier's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service.</p> <p>Information security is incorporated into the Supplier's financial and operational risk reporting mechanisms for the service.</p> <p>The Supplier has defined roles and responsibilities for information security within the service and allocated them to named individuals. This includes a named individual with responsibility for managing the security aspects of the service.</p> <p>The Supplier has processes in place to identify and ensure compliance with applicable legal and regulatory requirements relating to the service.</p>
			IA Organisational Maturity	The Supplier can demonstrate a sufficient degree of IA Maturity.
5	Operational security	The Supplier has processes and procedures in place to ensure the operational	Configuration and change management	The status, location and configuration of service components (including hardware and software components) shall be tracked to ensure they can

Variation to Dynamic Marketplace Agreement

		security of the service.		be effectively managed and remain securely configured. Changes to the service shall be assessed for potential security impact. They shall be managed and tracked through to completion.
			Vulnerability management	Potential new threats, vulnerabilities or exploitation techniques which could affect the service are assessed and corrective action is taken.

Variation to Dynamic Marketplace Agreement

				<p>Protective monitoring</p> <p>The service shall collect data events from all relevant Contractor devices to support effective identification that all implementation objectives are operating effectively. There shall be effective automated analysis systems in place, supported by adequately trained staff, which identify and prioritise indications in the data that may be related to malicious activities. The Supplier shall provide Contracting Authority's with alerts resulting from protective monitoring which impact the implementation objectives within 24 hours. NCSC Security Operation Centre provides recommended Good Practice for the implementation of a protective monitoring solution.</p>
--	--	--	--	--

Variation to Dynamic Marketplace Agreement

-	-		Incident management	<p>A defined process and contact route shall exist for reporting of security incidents by Contracting Authority (s) and external entities.</p> <p>A definition of a security incident shall be published for the service and the triggers and timescales for sharing such incidents with service Contracting Authority (s).</p> <p>The content and format of security incident notifications for sharing information with Contracting Authority (s) shall be published.</p> <p>The Supplier shall initiate investigations into incidents within five hours.</p>
6	Personnel security	Supplier staff should be subjected to adequate personnel security screening and security education for their role.	Contracting Authority	Supplier staff that have logical or physical access to the service shall be subjected to adequate personnel security screening for their role. At a minimum these checks shall include identity, unspent criminal convictions, and right to work checks.

 Variation to Dynamic Marketplace Agreement

7	Secure development	Services should be designed and developed to identify and mitigate threats to their security.		<p>The Supplier shall have a process in place to review new and evolving threats regularly and have development plans in place to progressively improve and reinforce the security of their service against these threats.</p> <p>Software development is carried out in line with industry good practice.</p> <p>Configuration management processes are in place to ensure the integrity of the components of any software.</p> <p>NCSC guidance on Security Design Principles for Digital Services provides best practice advice.</p>
8	Supply chain security	The Supplier should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to deliver.		<p>The Supplier shall clearly define information is shared with or accessible by its third party Contractors (and their supply chains).</p> <p>The Supplier's procurement processes shall ensure that the minimum relevant security requirements for all third party Contractors and delivery partners are explicitly documented.</p> <p>The risks to the Supplier from Sub-Contractors and delivery partners shall be regularly assessed and appropriate security controls implemented.</p> <p>The Supplier shall monitor its potential Sub-Contractor's compliance with security requirements and initiate remedial action where necessary.</p>

 Variation to Dynamic Marketplace Agreement

				<p>The Supplier's procurement process shall ensure that following contract termination all assets are returned, removed (or appropriately destroyed) and any Sub-Contractors' access rights to the Supplier's internal systems or information are removed.</p> <p>The Supplier shall categorise each Sub-Contractor as one of the following:</p> <p>Type 1 - access to aggregated Contracting Authority Consumer data Type 2 – access to limited number (less than 10) individual Contracting Authority Consumer records Type 3 – access to only part of an individual Contracting Authority Consumer records Type 4 – no access to Contracting Authority Consumer records</p>
9	Contracting Authority management	The Contracting Authority should be provided with tools to enable them to securely manage their service.	Authentication of Contracting Authority to management interfaces	<p>Only properly authorised individuals from the Contracting Authority organisation can authenticate to, and access management tools for the service.</p> <p>Only authorised individuals from the Contracting Authority are able to perform actions affecting the service through support channels</p>

 Variation to Dynamic Marketplace Agreement

			Separation of Contracting Authority within management interfaces	<p>No other Contracting Authority service consumer can access management tools for the service.</p> <p>The contracting shall be able to constrain permissions granted to authorised individuals from the Contracting Authority to perform actions affecting the service.</p>
			Secure Contracting Authority Service Change Authorisation	A Supplier support procedures shall identify when a support action is security related (such as altering a user's access permissions, or changing user credentials) and ensure appropriate authorisation is in place for this change.
10	Identity and Authentication	Contracting Authority and Supplier access to all service interfaces should be constrained to authenticated and authorised individuals.		The Supplier shall implement controls which provide confidence that a user has authorisation to access a specific interface.
11	External interface protection	All external interfaces of the service should be identified and have appropriate protections to defend against attacks through them.		The service controls and protects access to elements of the service by Contracting Authority (s) and outsiders.
12	Secure service administration	The methods used by the Supplier's administrators to manage the operational service (monitor system health, apply patches, update configuration etc.) should be designed to mitigate any risk		<p>The networks and devices used to perform administration /management of the service shall be appropriate to protect the Contracting Authority 's data</p> <p>End user devices used for administration shall be enterprise managed assets and shall be securely</p>

Variation to Dynamic Marketplace Agreement

		of exploitation which could undermine the security of the service.		<p>configured. CESG's EUD Security Guidance provides recommended good practice for configuration of a range of different end user device platforms which can be used to inform the configuration of these devices.</p> <p>NCSC guidance on implementation of system administration architectures provides best practice.</p>
13	Audit information for tenants	Contracting Authority (s) should be provided with the audit records they need in order to monitor access to their service and the data held within it.		<p>Audit information shall be retained for a minimum of two years or until the Contracting Authority leaves the service. The audit information shall be accessible online for a minimum of six months from the point of event collection.</p> <p>The Supplier shall make tenants aware of:</p> <p>The audit information that will be provided.</p> <p>The format of the data and the schedule by which it will be provisioned (e.g. on demand, daily etc.).</p>
14	Security use of the Service by the consumer	Service consumers are clear on their responsibilities when accessing the service.		<p>The Service consumer understands any service configuration options available to them and the security implications</p> <p>The Service consumer understands the security requirements on their processes, uses and infrastructure related to use of the service.</p> <p>The Contracting Authority is able to educate its privileged users in how to use it safely and securely.</p>



Appendix 2 – Security Delivery Objectives

Security Governance

- Security Working Group
- Security Management Plan
- Security Risk Register

Security Risk Acceptance

- Risk Management Document
- Privacy Impact Assessment

Security Assurance

- Security Assurance Plan
- Cyber Essential Scheme Certification

Operational Security

- Operational Security Management Report

Appendix 3 – The Statement of Information System Risk Appetite

- 1.1. The data held by the system (once fully operational) will consist of:
- Personal Data
 - Commercial Information
 - Departmental Corporate Information
- 1.2. The risk appetite is applicable to the Information System service and the provision of the Ordered Services.
- 1.3. The Information System will hold a large amount of aggregated with potentially SENSITIVE personal data sets. There is also assessed to be a risk from an integrity perspective of these data sets and user access controls need to be put in place to ensure that there are strict control over who is able to access these. This intent should be satisfied by the Supplier of the System adequately applying the controls from a competent supplier who has been certified under an appropriate security governance regime; ISO27001, Cyber Essential or equivalent standard, and putting additional controls around any potential download and transmission of aggregated data from The Information System. In addition, a robust Protective Monitoring regime should be in place to detect any attempt to download data and export it.
- 1.4. In addition, the programme will implement appropriate and proportionate controls to maintain the integrity and accuracy of data help on the service and supporting systems. Good practice and proportionate baseline security controls will be implemented including the segregation of roles and access to update/amend data.
- 1.5. While these measures will be put in place to mitigate any risk to the confidentiality of the service data where appropriate. The service shall also ensure appropriate protection in in place to mitigate the risk associated with a compromise of the availability as well as the Integrity of the data.
- 1.6. The risk appetite for the service is **CAUTIOUS** (see the treasury definitions on GOV.UK) as accepted by the service Senior Programme Executive, the service SRO and the HMG Department Office Senior Information Risk Owner (SIRO).