CPS SECURITY POLICY

Section 1: Minimum Requirements

1.1 The security requirements that apply to Government Departments and Service Providers are governed by the Government's core set of mandatory minimum measures to protect information, to apply across central Government of the United Kingdom. Details of the mandatory minimum measures can be found at the Cabinet office website at:

Government Functional Standard GovS 007: Security - GOV.UK (www.gov.uk)

1.2 The general requirement is that Service Providers shall be proactive in planning and implementing appropriate policies, processes and procedures to safeguard and protect the information entrusted to them, to enable them to deliver the Service and to demonstrate that they have understood the risks relating to that information and plan mitigating action, which is then put in place and monitored.

1.3 As a minimum Service Providers shall put in place specific measures to address the access of Staff and sub-contractors: their organisation's selection and training; systems access rights; the treatment of types of information; and processes for checking compliance.

1.4 The CPS is keen to appoint Service Providers that maintain a culture of individual accountability and awareness that encourages staff to be 'trusted stewards' of sensitive data with an obligation to protect it and addresses inappropriate behaviours arising from information mismanagement.

1.5 All contracts that require IT services or integration with CPS digital systems will require IT certification in the form of the Governmental approved Cyber Essentials scheme. The UK Government have decreed all inter-linked systems that handle sensitive data and/or hold standalone sensitive data must be accredited by Cyber Essentials as a minimum. The CPS have deemed Cyber Essentials Plus will be a requirement for IT contracts or critically dependent IT systems.

1.6 The Service Provider shall hold Cyber Essentials+ and ISO 27001 certification (or the equivalent certifications) to support the delivery of the Services, at contract award. This level of certification must be maintained throughout the duration of the contract. The certification must be submitted to the CPS annually.

Section 2: Security Classification

2.1 The security classification for the CPS's mail will generally be up to Official – with the caveat of 'Sensitive' added, as the CPS deals with sensitive material as part of its criminal investigation and prosecution process. The handling of this material may additionally be subject to specific legal requirements.

2.2 The Service Provider may be expected to handle mail items consisting of live case data as part of its contracted duties. Under the previous security classifications, the possible risks of this type of information were assessed as Impact Level 3 (IL3).

2.3 As a Government department, the CPS's' operations are also subject to the Official Secrets Act. The Service Provider shall ensure that all employed Staff engaged to deliver the goods and services sign a declaration pursuant of the Official Secrets Act.

Section 3: Staff Security Requirements

3.1 The CPS deals with criminal prosecutions and the Service Provider must be aware that Service Provider Personnel may be handling live case data. All the Service Provider Personnel connected with the delivery of Service under this Contract shall be vetted to a minimum of BPSS however heightened access is required then vetting to SC standard must be considered. Any additional Service Provider Personnel nominated to work on the Contract shall also be vetted in accordance with this standard or higher where appropriate and/or necessary.

3.2 The CPS shall carry out periodic spot checks to ensure that the Service Provider Personnel have been security cleared to the appropriate level.

3.3 All of the Service Provider Personnel that can access the CPS's information or systems holding the CPS's information shall undergo regular training on secure information management principles. Unless otherwise agreed with the CPS in writing, this training shall be undertaken annually.

3.4 The Service Provider shall ensure that all Sub-Contractors engaged to deliver the goods and services work for a company approved by the CPS and comply with all security requirements.

3.5 The Service Provider shall disclose any criminal convictions (both current and spent) to which their Staff have been subject (including motoring conviction) as part of their conditions of employment and will authorise the CPS if required to carry out checks of information provided. The CPS shall have a right to insist that Staff with criminal convictions (excluding minor motoring convictions) are excluded from working on this Contract.

Section 4: General Provisions

4.1 When OFFICIAL level information or higher is held and sorted on the Service Provider premises, the premises in which it is held must be secured. The Service Provider shall ensure that material received at their premises is handled securely, including arrangements for transferring material from the delivery vehicle to the nominated premises.

4.2 The Service Provider shall ensure that suitable security measures are used by them to always ensure the security and safekeeping of the CPS's material, including transit.

4.3 The Service Provider shall have procedures in place to ensure that any material which is entrusted to their safekeeping is always stored securely and not disclosed to unauthorised staff at any time. Applying the 'principle of least privilege' the Service Provider's staff shall only be allowed access to the CPS's mail as required to ensure service delivery.

4.4 The Service Provider shall operate an access control system at its premises, via methods such as key codes and dedicated access cards, to ensure that unauthorised

individuals cannot access the premises. The Service Provider shall ensure that all windows can be securely locked and operate an alarm system.

4.5 The Service Provider shall operate a Staff identification process whereby each employee is assigned a unique identifier clearly illustrating designated levels of access.

4.6 The Service Provider shall ensure that all material in their possession, in connection with delivery of the Services, is retained in the United Kingdom (UK) and is not stored or processed outside of the United Kingdom.

4.7 The Service Provider shall agree any change in location of data storage, processing, and administration with the Contracting Body in advance of any proposed move. Contracting Body data shall not be stored outside of the UK unless agreed with the CPS's Senior Security Advisor.

4.8 The Service Provider shall allow premises to be inspected by the CPS as required, subject to advance notification, to verify the suitability of security protocols.

4.9 Should any of the material relating to the CPS's' business be unaccounted for whilst in the care of the Service Provider, the Service Provider shall trace this material within forty-eight (48) hours. Loss of any material shall be treated as a serious breach of security. Any such loss should be reported within twenty-four (24) hours to the CPS's Operational Security Team.

4.10 The Service Provider shall appreciate that public sector document provenance and data sharing security may, on occasion, be of interest to various sectors of the media. Under no circumstances should any of the CPS's' information be disclosed to external sources.

4.11 The Service Provider shall provide staff and documentation at the discretion of the CPS to demonstrate that document provenance and data sharing is robustly managed and is secure.

4.12 The Service Provider shall ensure that normal security standards are maintained in the event of a business continuity issue.

4.13 If the Service Provider receives a Right of Access (ROAR) application under the Data Protection Act (DPA) and/or the Freedom of Information (FOI) Act any such application must be notified to the CPS Representative and referred to the CPS Information Access Team's inbox before any response is made. All other DPA rights requests should be referred to the Data Protection Officer's inbox.

Section 5: Information Security Protocols

5.1 If any CPS information is held and accessed within Service Provider systems, the Service Provider shall comply with at least the minimum set of security measures and standards as determined by the Government Functional Standard GovS007 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachm

ent_data/file/1016424/GovS_007-_Security.pdf as well as any additional protections as needed as a result of their risk assessment.

5.2 Should any service provider utilise Cloud Services in the IT deliverables then they must conform the requirements in line with NCSC's 14 Cloud Principles.

The cloud security principles - NCSC.GOV.UK

5.3 Unless otherwise agreed with the CPS in writing, all Service Provider devices used to access or manage CPS information are expected to meet the set of security requirements set out in the NCSC End User Devices Security Guidance or its successor:

Device Security Guidance - NCSC.GOV.UK

5.4 Wherever possible, such information shall be held and accessed on ICT systems on secure premises. This means Service Provider shall avoid use of removable media (including laptops, portable hard drives, CDs, USB memory sticks, tablets, and media card formats) for storage or access to such data where possible.

5.5 Where it is not possible to avoid the use of removable media, Service Provider shall apply all the following conditions:

- The information transferred to the removable media shall be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held. Where possible, only anonymised information shall be held;

- user rights to transfer data to removable media shall be carefully considered and strictly limited to ensure that this is only provided where necessary for business purposes and subject to monitoring by managers, and

- The individual responsible for the removable media shall handle it – themselves or if they entrust it to others – as if it were the equivalent of a large amount of their own cash.

- The data shall be encrypted to a UK Government standard appropriate for handling data up to and including OFFICIAL-SENSITIVE, or FIPS 140-2, using software that does not require a software download onto the recipient's device.

- The data contained on the media shall be securely erased as soon as it has been transferred to a secure source.

5.6 When CPS data is held on mobile, removable, or physically uncontrolled devices or portable media, such as laptops or tablets, it shall be stored and encrypted to a UK

Government standard appropriate for handling data up to and including OFFICIAL-SENSITIVE, such as FIPS 140-2 or NCSC approved methods.

5.7 Where the Service Provider grants increased IT privileges or access rights to its Staff or Sub-contractors, those persons shall be granted only those permissions necessary for them to carry out their duties and be subject to appropriate monitoring. When Staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

5.8 Service Provider shall recognise the need for the Contracting Body's information to be safeguarded under the UK Data Protection regime. To that end, Service Provider shall be able to state to the CPS the physical locations in which data may be stored, processed and managed from, and to confirm that all relevant legal and regulatory frameworks authority are complied with.

5.9 Service Provider shall agree any change in location of data storage, processing, and administration with the CPS in advance of any proposed move to the extent that such move has any impact upon the Service and relates specifically to the CPS Data. CPS Data shall not be stored outside of the UK unless agreed with the CPS's Senior Security Advisor.

5.10 The CPS requires that any information up to Official Sensitive transmitted electronically shall be sent via the Criminal Justice Secure Email (CJSM) system. The CPS will sponsor and pay for Service Provider's subscription to this system. The CJSM service is an important part of the process of joining up the Criminal Justice System (CJS) in England and Wales. It allows people working in the CJS to send emails containing information up to OFFICIAL SENSITIVE in a secure way. CJSM uses a dedicated server to securely transmit emails between connected criminal justice practitioners. Once connected, users can use CJSM to send secure emails to each other and to criminal justice organisations. As the ICT infrastructure of the CPS is updated during the Contract, Service Provider may be required to transmit data via other electronic systems, such as the 'Egress' system, but this should be agreed with the CPS Senior Security Advisor.