**Security Requirements Document**

**Contents**

[Notes 3](#_Toc461692463)

[1 Purpose 4](#_Toc461692470)

[2 Introduction 4](#_Toc461692474)

[3 Classification of Information 5](#_Toc461692486)

[4 Organisation Security Controller 6](#_Toc461692494)

[5 Vetting and Staff Clearance Requirements for Individuals Accessing College of Policing Data and Information 6](#_Toc461692497)

[6 Physical Security of College of PolicingData when held by Service Providers 7](#_Toc461692506)

[7 Computing Device Security 7](#_Toc461692511)

[8 Accreditation 8](#_Toc461692520)

[9 Offshoring 8](#_Toc461692525)

[10 Retention and Destruction of Classified Material 9](#_Toc461692538)

[11 Loss of or Unauthorised Access to Classified Material 9](#_Toc461692540)

[12 Quality Control Checks 9](#_Toc461692545)

[13 Sub-contractors 9](#_Toc461692548)

[14 Fraud and Corruption during the Contract Period 10](#_Toc461692550)

[15 Business Continuity and Disaster Recovery 10](#_Toc461692555)

 [Signatories 11](#_Toc461692583)

**Notes**

Security standards must meet the College of Policing Procurement Policy which should encompass Crown Commercial Services (CCS) Security Standards and HMG Security Policy Framework (SPF) as issued by the Cabinet Office who set out mandatory requirements that Departments, Agencies and third party suppliers must adhere to.

In addition, where the College deems it appropriate, enhanced or additional College security policies, guidelines or procedures will apply. The terms “data, information and assets” and “classified material” will be used interchangeably throughout this document.

This Security Requirements Document (SRD) has been prepared taking into account the minimum security vetting requirements for access to College data, information, assets or estate.

Vetting level requirements will differ depending on the type and sensitivity of the data and information as well as site access requirements.

**NB:** Vetting requirements may include both Police and National Security Vetting.

This SRD must be supported by appropriate commercial terms and conditions.

1 **Purpose**

1.1 The purpose of this Security Requirements Document (SRD) is to outline the security requirements and security classification guidelines that apply to contractors and internal and external stakeholders delivering services to/for the College of Policingas well as their advisors, consultants and appointed professionals who store or process existing College of Policing data andinformation for College purposes – for clarity the term “service provider” will be utilised throughout this document instead. In addition, specific guidance is given on College of Policing data andinformation assets which are created as part of the College’sprocesses.

1.2 The security requirements and classification guidance are drawn from the College’s security policies which are formulated from the HMG Security Policy Framework (SPF). Specific reference is made within this SRD to the Colleges Government Security Classifications (GSC) Mandatory Policy Guidelines which provide the necessary guidance.

1.3 Any queries, updates or issues relating to this document should be referred to the College Security Unit (CSU).

2 **Introduction**

2.1 All records created, used or held by Government Departments are deemed Public Records under the Public Records Acts and must be compliant with the relevant legislation and handled in accordance with appropriate information management principles.

2.2 In addition, College data, information and assets must be protected to prevent unauthorised disclosure, loss, theft or compromise. The GSC scheme comprises three levels, OFFICIAL, SECRET and TOP SECRET. A copy of the College GSC Mandatory Policy Guidelines should accompany this letter and contains the necessary detail around the creating, handling, transmitting/transferring, sharing, storage and disposal requirements – you are expected to adhere to all guidelines detailed when dealing with College data and information.

2.3 The GSC is designed to indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. The typical threat profile for College OFFICIAL data and information is broadly similar to that faced by a large UK private company, with valuable data, information and services, in terms of compromise by an attack by determined outsiders including hacktivists, single issue pressure groups, investigative journalists, and the majority of criminal gangs and individuals.

2.4 Applying a classification to an asset indicates its sensitivity, or confidentiality, and thus the level of protection required. The ‘consequence of compromise’ must be considered, to determine the asset value, the necessary security controls and therefore the classification.

2.5 When assessing the value of an asset it will be necessary to consider both the direct and indirect consequences of compromise in relation to a breach or loss of:

* Confidentiality: Ensuring only properly authorised persons can access data and information and that effective controls are in place to prevent unauthorised access.
* Integrity: Ensuring that data cannot be modified in an unauthorised or undetected manner.
* Availability: Ensuring that authorised people can access that data and information when they need to, at the right time and in the right way.

2.6 Each classification involves safeguards which must be adopted whatever the subject matter - documents classified because of their political or economic content require the same safeguards as criminal justice information.

2.7 In relation to any contract with the College of Policingthere is potential to create, handle, transmit/transfer, share, store and dispose of large amounts of data and information in both paper and electronic format. All information – however it is recorded - needs to be managed properly to ensure that it provides the greatest benefit as well as being protected from loss or unauthorised alteration or disclosure. The classification appropriate to an asset may alter through the passage of time.

2.8 Each individual and organisation processing data and information in relation to College of Policing is personally responsible for ensuring that it is used properly, kept up to date, shared only with those who have a right to see it (‘need to know’ principle), stored in accordance with its sensitivity and classification and only retained for as long as it is actually needed, or in accordance with any specific retention schedule or legal requirement.

3 **Classification of Information**

3.1 The service provider is responsible for being aware of all existing College of Policing information assets in their possession which have been classified: OFFICIAL (public domain), OFFICIAL (secure), OFFICIAL – SENSITIVE, SECRET and TOP SECRET, and for maintaining that protection in accordance with stated requirements and supplied mandatory guidelines. Legacy data and information may exist that will be marked under the former Government Protective Marking Scheme (GPMS).

3.2 The service provider is responsible for ensuring that any new data or information created is classified in accordance with the GSC Mandatory Policy Guidance.

3.3 The vast majority of College data, information and interaction with service providers is expected to occur at OFFICIAL. Should the service provider believe any data or information requires a classification of SECRET or TOP SECRET they **must** seek immediate guidance for the CSU.

3.4 In the event the service provider disputes the classification of any College data or information this should firstly be brought to the attention of the relevant College Information Asset Owner who may wish to consult the CSU.

3.5 It is not a requirement to mark OFFICIAL information. However, if in certain circumstances it would help avoid any doubt as to the classification, the owner or originator can apply the OFFICIAL (public domain) or OFFICIAL (secure) handling guidance such as ‘for your use only’ or ‘not for onward transmission’ and so on.

For detailed guidance please refer to the GSC Mandatory Policy Guidelines document.

**SERVICE PROVIDER SECURITY AND STAFF VETTING REQUIREMENTS**

4 **Organisation Security Controller**

4.1 The service provider must nominate a Security Controller, with responsibility for day to day aspects of security, together with a board level[[1]](#footnote-1) contact who accepts responsibility for security on behalf of the service provider and to whom the Security Controller reports.

4.2 The Security Controller shall establish processes to ensure the full implementation of this SRD and referenced documents, and that any breach or attempted breach of the requirements set out in this document, including attempts at manipulation or deliberate erasure or modification of records, must be reported within 24 hours or earlier time if possible, to the CSU.

5 **Vetting and Staff Clearance Requirements for Individuals Accessing College of Policing Data and Information**

5.1 Vetting standards required of the service provider will be identified and communicated during the SAL / Contract / Project initiation phase.

5.2 The service provider’s Security Controller must report to CSU any changes that my call into question an individual’s vetting/security clearance eligibility e.g. poor finances, cautions, arrest, county court judgements.

5.3 Individuals with access to College of Policing data andinformation assets shall have identity and immigration history checks carried out by the College or other authority as appropriate. The information gathered by these checks may be used for the investigation of potential corruption and criminal activity.

5.4 Access to live policing data, information and premises in most cases will require Non-Police Personnel Vetting (NPPV) clearance. In addition National Security Vetting (government clearances) may also be required.

5.5 The College reserves the right to approve the vetting of all individuals involved with College data and information. Confirmation of clearance must be passed to the College who reserve the right to validate or refuse it. The College also reserves the right to review and assess vetting levels and apply them retrospectively where required.

5.6 Individuals with any adverse outcomes, such as an adverse immigration history, convictions whether spent or not, may only have access to College of Policing data and information assets with the prior written approval of the CSU. Such approval, if provided, shall be at the College’s sole discretion.

5.7 To gain or maintain continued access, any queries from College Security Clearances in respect to the individual's clearance must be resolved by the individual within 5 working days. In addition, any relevant business visa conditions for non-EEA nationals must be met before the individual starts work in the UK.

5.8 The Security Controller must inform/warn individuals permitted access to classified material against divulging information to any unauthorised person, and must be informed that the Official Secrets Acts 1911-1989 applies to them.

6 **Physical Security of College of PolicingData when held by Service Providers**

6.1 A layered approach to physical security should be adopted on a risk assessed basis to prevent unauthorised access to sites and/or classified material (and other valuable assets) putting in place integrated and proportionate control measures to prevent, deter, detect and/or delay attempted “physical attacks”, and to trigger an appropriate response.

6.2 Physical security measures should complement other technical, personnel and procedural controls as part of a “layered” or “defence in depth” approach to security that effectively balances prevention, detection, protection and response.

6.3 When not in use data and information assets which are OFFICIAL including OFFICIAL - SENSITIVE must be protected by at least one physical barrier e.g. a locked cabinet within a secure location. Mechanisms used must be deemed adequate for such classification by CSU.

 If holding data or information at SECRET or above prior explicit detailed agreement and approval must be reached with CSU regarding processes, containers, locks etc.

7 **Computing Device Security**

7.1 Data and information assets which are classified OFFICIAL (secure) or OFFICIAL – SENSITIVE must not be created, handled, transmitted/transferred, shared, stored on/from any computer system and/or network unless it has been approved by the College to handle data of the relevant classification. Consideration must be given to the protection of classified data whether on removable media or within the machine or network. In general OFFICIAL:-

* May be held on any computer system or network suitable for sensitive.
* Information that has been accredited to hold OFFICIAL data and information.
* May also be held on laptops/desktops that are accredited to hold OFFICIAL and are equipped with government approved whole disk encryption. A list of serial numbers of these laptops must be maintained by the service provider and made available to the College on request.
* May be held on a USB storage portable devices which are suitably encrypted.
* Must be kept to the minimum amount of date necessary for the purpose.

7.2 The minimum encryption standard for memory sticks or other removable media is commercial encryption to FIPS-140-2 or equivalent for OFFICIAL; other classifications require the prior written approval of the CSU.

7.3 Appropriate safeguard, management and systems controls and audits must be in place to prevent the loss or theft of College of Policing data, information and assets. In the event of such a loss, the audits must clearly identify the complete audit trail in relation to that asset – for example, audits must include details as to whom, where and when a person has access to the data, has viewed it, printed it, copied it or sent it by email.

8 **Accreditation**

8.1 It is a Mandatory requirement of the SPF and/or PSN Code of Connection that:

* All ICT systems that handle, store and process classified information or business critical data, or that are interconnected to cross-government or police networks or services e.g. the Public Services Network (PSN), must undergo a formal risk assessment to identify and understand relevant technical risks; and
* Must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.

8.2 To gain accreditation the service provider must ensure that the solution is appropriately accredited in accordance with the SPF using an appropriate risk assessment & mitigation process for Government/Police data. Service provider’s will maintain the solution in accordance with the latest versions of the SPF, HMG standards and supporting Cabinet Office and Police policies and documents.

9 **Offshoring**

9.1 “Offshoring” means any arrangement where data handling services or an element of services are performed outside the UK, as well as the more traditional offshore outsourcing arrangements (where whole business functions are carried out outside the UK).

9.2 If there is the potential for personal or other sensitive non-personal information to be held, processed or otherwise transferred outside the UK you must:

* Comply with the mandatory Cabinet Office Approvals Process for Offshoring proposals.
* Comply with the minimum mandatory measures HMG IA Standard No. 60 set out in the data handling review.
* Comply with the data Protection Act and Information Commissioner’s Office (ICO) guidance.
* Provide the College‘s Senior Information Risk Owner’s (SIRO) with written assurance that adequate information risk assessment and protection is in place and be in receipt of their prior written approval.

9.3 For personal data which is sensitive you must:

* Show evidence of a robust risk assessment of information risk.
* Take specific account of the legislative framework of the hosting country, particularly overriding provisions which may create tensions and potential conflicts with UK laws, such as the Patriots Act in relation to the United States.
* Ensure that access, and the ability to copy or store records, is strictly limited to that required by business need; ensure that vetting of employees is appropriate for the data being handled; and that mitigation is in place for any other risks around employees of the offshored site.
* Have robust independent assessment of compliance with all arrangements contractual or otherwise.

9.4 For all College data, information and assets, irrespective of classification, appropriate safeguards, management and systems controls – including division and oversight of responsibility and audits must be in place to prevent the loss, theft or leak of personal data. In the event of such a loss. There must be sufficient reporting and audit in place to clearly identify the complete audit trail in relation to that data –for example, audits must include details as to whom, where and when data has been accessed, viewed, printed, copied it or sent by email. In the event that an individual cannot show the audit, they become culpable for future handling of that data and document register.

10 **Retention and Destruction of Classified Material**

10.1 The service provider shall agree classified material retention and disposal arrangements at the outset of the contract – in the absence of agreement College standards will be deemed to apply.

11 **Loss of or Unauthorised Access to Classified Material**

11.1 The service provider is required to comply with the SPF and the College’s policy in relation to leaks, breaches and data incidents. Any such incidents must be immediately reported to the CSU.

11.2 Any loss of College data or information, or the suspicion of unauthorised access to such material, must be reported without delay by the Security Controller, who will liaise with the CSU and the Home Office and/or Police Service as appropriate.

11.3 If there is any doubt as to whether there has been a breach the incident or suspicion of such must be reported immediately to the CSU and every effort to confine and resolve – address the breach and remedial actions undertaken.

11.4 The service provider will co-operate with the College in any investigation that is considered necessary as a result of any breach of security in relation to College classified data or information.

12 **Quality Control Checks**

12.1 The service provider shall provide for the College’sprior written approval, a suitable programme for the quality control of the information and the work completed on behalf of the College.

12.2 To reassure the Collegethat services are being undertaken in a manner consistent with the contract, an acceptable programme is likely to entail the service provider undertaking a regular dip sample of letters and phone calls made and casework undertaken. The service provider shall provide key personnel to be responsible for this quality control work. The Collegeshall be entitled to request all information relating to this quality control work at any time during or after the duration of the Contract and the service provider shall provide a response within one week.

13 **Sub-contractors**

13.1 The requirements above apply equally to sub-contractors used by the main service provider in relation to the College’sbusiness. Where the contract with the College allows their use, service providers must ensure the appropriate integrity measures are in place in relation to their sub-contractor and they must follow the general requirements listed in these paragraphs, in addition the College may require an audit.

14 **Fraud and Corruption during the Contract Period**

14.1 All service providers are required to put in place appropriate counter fraud and security management arrangements prior to the commencement date of the contract.

14.2 Allegations of corrupt activity received by the service provider in relation to the service delivered for the College must be copied immediately to the CSU. The service provider must appoint a single point of contact in relation to any investigation matters.

14.3 Independent systems must be in place to report whistle blowing allegations.

14.4 The service provider’s staff are required to co-operate fully with any investigation into fraud or corruption. Any fraud investigators appointed by the College of Policingmust be given full and immediate access to all systems and records held by the service provider, any sub-contractors and their staff. The College of Policingshall have the power at any time during the provision of the services to give the service provider immediate notice requiring the removal from the service provider’s premises of any equipment, documentation or other evidence which, in the reasonable opinion of the College of Policing is required as evidence of part of an investigation.

15 **Business Continuity and Disaster Recovery**

15.1 An effective and up-to-date Business Continuity Management (BCM) system should be put in place to maintain or else quickly resume provision of key services in the event of a disruption. BCM arrangements must follow industry best practice (BS25999 or equivalent standard). This includes disaster recovery policies for key ICT systems, along with appropriate arrangements to minimise the impact of a terrorist attack or other critical incidents.

15.2 The service provider is required to produce, prior to the Contract Effective Date, a comprehensive Business Continuity Plan (BCP), including Disaster Recovery procedures which meets the British Standard for Business Continuity Management, ISO22301. The BCP shall be agreed by the College DSO, which shall not unreasonably withhold its approval.

15.3 The BCP should be written to complement the phases of the contract which are:

* Mobilisation.
* Delivery and execution.
* Exit and handover.

15.4 The situations in which the BCP can be utilised should include as a minimum:

* General disruption.
* Loss of site.
* Denial of access to premises.
* Loss of communications systems, recording systems.
* Denial of access to personnel including such instances as a serious adverse weather event or travel disruption.
* Resourcing of the contract (staff, systems and all premises including but not limited to outlets).
* IT and Security.
* Loss of College data and or information.
* Breach of IT and security requirements.

15.5 The BCP shall include the critical activities to be recovered and the key representatives responsible, including but not limited to:

* Procedures for invocation of the plan including those with College to invoke.
* Key contact details for both the service provider and the College.
* The timescales in which the critical activities are to be recovered.
* The recovery levels needed for each critical activity.
* The resources required to achieve the defined recovery levels.
* Strategies for recovery.

15.6 The service provider shall ensure that its staff and its sub-contractor staff have access to a copy of the BCP and are trained in these emergency procedures and understand their roles and responsibilities if the plan is to be invoked.

15.7 The service provider shall ensure that all of its staff, whether directly employed or via a sub-contractor, understand the manual back up of the systems in place to ensure that, in the event of any failure to its IT systems used in the delivery of the services, it is able to carry out the services with minimal disruption.

15.8 The service provider shall ensure that the risk assessments which inform the BCP and the BCP itself are regularly refreshed and updated as appropriate and no less than once every six months. Any changes to the BCP need to be approved by the CSU as part of the strategic review meetings which form part of the contract management regime.

15.9 The service provider shall ensure the BCP is subject to regular testing, at a minimum this should occur annually or following a significant change in processes, staff or technology. The service provider should issue a report to the CSU highlighting any failures in the BCP revealed by the test and proposals for remedying any failures. The service provider shall promptly implement any actions or remedial measures which the College considers necessary as a result of those tests.

**Signatories**

**College of Policing - Procurement Manager**

**Name: Bea Wilkinson**

**Date: 05th January 2022**

**Signature:**

**Signed and agreed on behalf of <Service Provider>**

**Name:**

**Date:**

**Signature:**

1. A board level member who has responsibility and accountability for Information Risk within the service provider organisation. [↑](#footnote-ref-1)