Security Aspects Letter

CACI

Charles McKay | SIRO (Senior Information Risk Owner)

11/09/2020 | Version 1.0

DOCUMENT CONTROL

Handling Instructions

This document has been marked as OFFICIAL-SENSITIVE and the following handling caveats apply:

- This document is distributed on the basis that recipients have a valid 'need-to-know'.
- This document must not be distributed to anyone outside of the documented distribution list below without the prior and explicit documented approval from the Police ICT Company Assuror, author or Police ICT Company (the Company) authority.
- If you have received this document and are not listed on the distribution list, you must securely dispose of this document and inform the author.
- Where there is a genuine business need to print this document, the printed document must be stored in a physically secure environment with physical access to the document limited to those within the distribution list. The printed document must also be securely disposed of when no longer required.
- Where there is a genuine business need to distribute this document through email to an external party, Police ICT approved secure email must be used (PNN, CJSM, GSi or other approved domain).
- Where there is a genuine business need to distribute this document through email to an external party, standard email may be used subject to the 'need-to-know' principle. Appropriate encryption must be used where this option is utilised.

Change Record

Version	Date	Author	Change Summary
0.1	07-Aug-20	Peter Hands	Draft
0.2	08-Sept-20	Heidi Thompson	CACI review comments
1.0	11-Sept-20	Mark Grover	Baseline and issue

Distribution

Version	Date	Name/Role
0.1	07-Aug-20	Alan Riordan – Commercial Manager Police ICT Company
1.0	11-Sept-20	Alan Riordan – Commercial Manager Police ICT Company Heidi Thompson – Head of Client Services, Digital Solutions, CACI

Approvals

Name	Name/Role	Date Approved
Charles McKay	Head of Service Delivery & SIRO, Police ICT Company	11-Sept-20

TABLE OF CONTENTS

DOCUMENT CONTROL **2**

HANDLING INSTRUCTIONS 2
CHANGE RECORD 2
DISTRIBUTION 2
APPROVALS 2

1 OBJECTIVE **4**

2 PROTECTING COMPANY INFORMATION – OVERVIEW **4**

MARKINGS 4
INFORMATION TYPES 4

3 STORAGE **5**

4 DATA AGGREGATION **6**

5 TRANSMISSION **6**

6 HUMAN RESOURCES SECURITY **7**

8 SAL REVISIONS **7**

9 SHARED RESPONSIBILITY **8**

10 SUPPLIER DECLARATION **8**

NPIRMT GUIDANCE ON HANDLING OF POLICE DATA WITHIN OFFICIAL SENSITIVE **9**

GLOSSARY **10**

1 OBJECTIVE

1.1. This letter establishes the security provisions with which all suppliers shall comply in providing the services as agreed by the Police ICT Company for the design, build, implementation, and support of the Police ICT Company ITSM requirements (also known as the Technology Enhancement Support (TES) service.

1.2. The Security Aspects Letter (SAL) is not a complete and exhaustive list of requirements and conveys the spirit of information security and risk management requirements.

1.3. CACI is required to ensure a comprehensive approach to information risk management through procedural, policy, personnel, physical and technical controls while in possession of Company or its customers information.

1.4. Where CACI sub-contracts elements of their activity, they must ensure that the provisions of this Security Aspects Letter (SAL) are disseminated throughout the supply chain.

2 PROTECTING COMPANY INFORMATION – OVERVIEW

2.1. The Company and CACI will protect information in accordance with the principles of the Government Security Classification (GSC). The Police ICT Company data is classified OFFICIAL and up to OFFICIAL SENSITIVE (OS) in order to re-enforce handling requirements (such as 'need to know' principles).

2.2. Some Police platforms and services which CACI is required to support may have a requirement to follow National Policing Information Risk Management Team (NPIRMT) Guidance on Handling of Police Data within OFFICIAL SENSITIVE, guidelines can be found in appendix A. CACI will be notified on a case by case basis by the Company where this requirement is applicable.

Markings

2.3. This SAL has been developed under the premise that all information assets will be classified OFFICIAL under the UK Government Security Classifications Policy (GSCP). Some Police ICT Company information assets will attract a classification level of OS and these are listed within the information types section below.

2.4. All information must be considered OFFICIAL whether it bears a marking or not.

Information Types

2.5. To assist in the understanding of what constitutes Company/police information with that of information used by CACI in the delivery of their service, the following should be applied:

- Information relating to designs, operations, Company policies and procedures and specific police business should be treated as OFFICIAL SENSITIVE content and should not be stored or processed on non-corporate systems or devices.
- Service metadata, i.e. data/information used for the purposes of CACI to support their contractual obligation (i.e. such as data/information relating to service and project management such as project plans, status reports, TES process information and service reports), can be stored and processed on CACI Laptops and Systems hosted within the CACI corporate infrastructure.

2.6. CACI's staff, and any contractors employed on behalf of CACI will adhere to any handling instructions allocated to the Police ICT Company Information Assets. Table 1 below details handling obligations specific to the Company delivery.

Aspect	GSC – Handling Instructions
Generic Customer data such as contact names	OFFICIAL – no restrictions
Documentation that details contractual matters relevant to the service	OFFICIAL - no restrictions
General system description documentation with no specific details of the aspects listed in the fields below.	OFFICIAL - no restrictions
All other Documentation such as High- and Low-Level Design documents	OFFICIAL SENSITIVE
Details of Software used in the development or operational environment	OFFICIAL SENSITIVE
Firewalls, Switches, Routers	OFFICIAL SENSITIVE
System Administration services	OFFICIAL SENSITIVE
Hosting Platforms	OFFICIAL SENSITIVE
Auditing	OFFICIAL SENSITIVE

Table 1 Handling Instructions applied to Service Aspects

2.7. It is possible that other sensitive matters will be identified during the development and support of this service. When such matters are identified, CACI's employees will be instructed on the handling instructions required, including any restrictions relevant to its dissemination and use. At all times, if there is any lack of clarity about appropriate Handling instructions, this should be raised with the Police ICT Company Information Security and Assurance team.

2.8. OFFICIAL information may be sufficiently sensitive to warrant additional security controls to protect it during transmission or storage. Handling instructions should clarify what additional security controls are required. The term OFFICIAL SENSITIVE is not always applied to sensitive information and it should not be assumed that OFFICIAL (including non-marked documents) information can be readily shared. Information that is unmarked, should be assumed to be OFFICIAL SENSITIVE.

3 STORAGE

3.1. Company specific information, i.e. any information or artefacts relating to this service, in electronic form should only be stored on corporate systems. All devices and data storage devices must be encrypted.

3.2. The CACI's employees are permitted to transfer non-sensitive information onto CACI's issued laptops for business needs. CACI's laptops must have Bitlocker encrypted hard drives. Company information must not be stored on any other device without prior approval from the Company SIRO or Information Security team. Live data that FCN Xchange processes, should not be stored locally on any corporate device.

Storage	GSC – Handling Instructions
Document Storage	All Company information should be protected by one barrier (e.g. locked container in a secure building). Particularly sensitive information (OFFICIAL SENSITIVE) should be protected by 2 barriers (locked container in a locked room in a secure building).
Electronic Storage	All Company information can be stored on CACI Corporate or Police ICT issued laptops in accordance with Company policy.
Disposal - paper	All Company OS information should be destroyed in a secure manner and as a minimum should be crosscut shred and placed in secure waste sacks.
Disposal – digital storage	Must be securely destroyed in accordance with Company policy. CACI's Laptops and desktops that have been used to process Company information (service metadata) are to be destroyed in line with commercial best practice. The Police ICT Company Information Security team should be contacted if clarification is required.

Table 2 Handling Instructions applied to Storage of the Police ICT Company Information

4 DATA AGGREGATION

5.1. In aggregation, the impact of a breach of any of these Security Aspects may be higher than the individual records or documents. CACI should ensure that aggregated or accumulated collections of information assets are protected appropriately.

5 TRANSMISSION

6.1. CACI's employees should have due regard to the sensitive nature of the Police ICT Company information and its customers and partners that is being transmitted and afford it an appropriate level of security. Table 3 details the transmission security that should be applied when transmitting information:

Transmission method	GSC – Handling Instructions
Mail	By post or courier, in a sealed envelope. Do not show protective marking on the envelope. For more sensitive information (OS and above), recorded delivery, double enveloped, both fully addressed. Any classification and

	descriptor to be on the inner envelope only. Return address on outer envelope.
Electronic Mail	Non-sensitive information (i.e. general correspondence, etc.) can be transmitted over insecure email (i.e. @The Supplier.com email address). Information of more sensitive nature (i.e. anything relating to Company security or similar) should be over secure email (e.g. @The Supplier.cjsm.net) or encrypted and password protected with the password being sent via another channel, for example SMS (where practical).
Telephone	Any telephone system can be used; care should be taken when discussing more sensitive data.
Internet	Transferring data via cloud storage devices (Google cloud, Drop Box) should not be used. Only Company accredited cloud services should be used as a means of transfer (e.g. O365) Some examples of satisfactory approaches include, but are not limited to: • Email systems meeting the 'Securing government email' guidance • Transport Level Encryption (TLS) version 1.2 and above aligned to NCSC recommended configuration(s) • Internet Protocol Security (IPSec) aligned to NCSC recommendation configuration(s) • NCSC and Company approved products or services for data transfer <CACI> should discuss with the Company where deviations from NCSC recommendations may be required due to technological limitations.

Table 3 Transmission requirements for Company Information

6 HUMAN RESOURCES SECURITY

7.1. CACI shall have, or be able to obtain, a level of vetting commensurate to the sensitivity of their work activity. As a minimum, all CACI's employed staff or contractors should have NPPV Level 3 issued by Warwickshire Police. As a temporary measure, the Company will accept NPPV2/3 clearances and SC while Warwickshire vetting is underway.

7.2. Employed staff or contractors who do not meet the vetting requirements stated in 7.1 must not work on Company development, build or operation without a policy exception agreed in writing by the Company SIRO (or their delegate).

8 SAL REVISIONS

8.1. The Authority reserves the right to issue a revised SAL at any time.

8.2. You are requested to acknowledge receipt of this letter and your acceptance of its terms as incorporated into your contract and binding within 14 days.

8.3. You are requested to confirm that the details of this SAL have been brought to the attention of the personnel directly responsible for the security of the services provided to, or in support of, the Company, that they are fully understood, and that the security and information assurance requirements set out in the contract schedules can and will be taken to safeguard the material concerned within 28 days.

8.4. You agree to provide a SAL in similar form to all subcontractors, obtain their acknowledgement and provide a copy to the Company within 28 days.

9 SHARED RESPONSIBILITY

9.1. The following provisions apply to items which are the responsibility of the Company, CACI or are shared between them.

9.2. Primary responsibility for the security of Company personnel, premises, and assets lies with the Company.

9.3. CACI shall comply with all current and future legislation appropriate to the secure operation and use of IT systems in providing the service / system to the Company.

9.4. The Company requires CACI, as appropriate, to comply with or follow the guidance contained in the latest versions of the following documents:

- ISO27001: 2017
- Applicable Company Information Security Management System Security Policies as determined by the Company Information Security Forum.

9.5. CACI shall make copies of its ISO27001 policy set available to the Company as required. All documents are subject to amendment or addition at Company discretion. Changes to documents must be notified to CACI, and both parties should consider the implications of those changes.

9.6. Any difficulty in interpreting the meaning of the above aspects or in safeguarding the materials should be raised with the Company Information Assurance immediately and send a copy of your letter to your Security Adviser.

10 SUPPLIER DECLARATION

10.1. You are requested to acknowledge receipt of this letter and to confirm that the levels of protective marking associated with the requirements listed above have been brought to the attention of the individuals directly responsible for the provision of the various services associated with this contract. Additionally, that they are fully understood, and that the required security controls can and will be taken to safeguard the material concerned.

Signed _____ Dated_____

Name Position

For and on behalf of (CACI)

NPIRMT GUIDANCE ON HANDLING OF POLICE DATA WITHIN OFFICIAL SENSITIVE

In 2015, the Police Chief's Council decided to adopt Government classifications, but agreed with Police Information Assurance Board (PIAB) that the OFFICIAL classification is insufficiently granular to adopt for policing purposes.

The CACI should be aware of the generic handling instructions used by NPIRMT:

- OFFICIAL SENSITIVE LOW - business support information including data on Facilities, Fleet and Property Management, and Supplier details
- OFFICIAL SENSITIVE MEDIUM - the majority of POLICE data for day to data operations; most information on staff; and information on most non-serious crime
- OFFICIAL SENSITIVE HIGH - information on areas such as Evidence and Forensics; Offender and suspect information; and Operation Planning

The CACI should further be aware of the NPIRMT guidance which states that:

- For systems/services designed to process data at MEDIUM and HIGH gradation. The full set of Candidate Control Set for Services (CCSS) controls needed for HIGH should be considered and, if appropriate, applied
- For systems/services designed to process data at HIGH. The full set of controls needed for HIGH should be considered and, if appropriate, applied

Table 4 details marking and handling instructions for systems subject to NPIRMT handling instructions. For clarity, a 'corporate device' is a supplier owned device that meets the standards defined in the NCSC End User Device Guidance.[1]

Data Handling classification	What data is it	Who can have it	How can it get there	What device can it use
Official These are the handling instructions for all data for the SUPPLIER to perform their day to day operations	Financial Data, Commercial Data, Equipment Registers, Supplier Details and Supplier operational data	No restrictions	Any email domain Normal postal methods	No restrictions
Official Sensitive Medium	Police designs, operations, policies and procedures and specific police business	CACI workers on a need to know basis	All data transmitted via VPN or TLS1.2 All mobile devices must have MDM installed Data to hosted in the UK and supported from an approved location	Only corporately owned devices Full hard disc encryption – this should be CAPS approved Log in as a minimum via unique username and password Privileged users 2FA only

[1] https://www.ncsc.gov.uk/collection/end-user-device-security

				Remote access via 2FA only Current anti-malware, anti-virus installed on all devices
Official Sensitive High These handling instructions are unlikely to apply before services are in live operations	Victim & Witness data, manage intelligence, Identity & Access Management, Manage Evidence (due to aggregation), Manage Forensics (due to aggregation), Prosecution planning	CACI staff on a named basis	All data transmitted via VPN or TLS1.2 Endpoints should mutually authenticate All mobile devices must have MDM installed Data must be hosted in UK only and supported from an approved location (which includes working from home) No Bluetooth connectivity shall be allowed	Only corporately owned devices Full hard disc encryption – this should be CAPS approved Remote access via minimum 2FA Current anti-malware, anti-virus installed on all devices Data encrypted at rest as well as in transit

Table 4 Company's Generic Handling Instructions

GLOSSARY

Name	Meaning
BPSS	Baseline Personnel Security Standard
CCSS	Candidate Control Set for Services
CIA	Confidentiality, Integrity, and/or Availability
CJSM	Criminal Justice Secure email service
GSC	Government Security Classifications
IA	Information Assurance
NCSC	National Cyber Security Centre
NPCC	The National Police Chiefs Council
NPIRMT	National Policing Information Risk Management Team
NPPV	Non-Police Personnel vetting
NPTC	National Police Technology Council
OS	OFFICIAL SENSITIVE
PIAB	Police Information Assurance Board
The Company	The Police ICT Company
PNN	Police National Network (synonymous to PSN4P)
SAL	Security Aspects Letter
SC	Security Clearance - one of the National Security Vetting clearance levels
SIRO	Senior Information Risk Owner