Strategic
Command

UK Strategic Command

Defence Support Transformation (SpTx)

Business Modernisation for Support (BMfS)

BMFS SECURITY MANAGEMENT PLAN v1

Version date: 14/07/2021

BMfS Concept Phase - Security Management Plan
August 2020

DOCUMENT CONTROL

Issue	Issue Date	Author(s)	Changes	Approved by
0.1	Feb 19	[Redacted]	Draft	Dir DSN(T)
1.0	Aug 20	[Redacted]	Updated to encompass Concept Phase deliverables.	Dir BMfS
1.1	Jul 21	[Redacted]	Formatting and removal of SIRO risk appetite section	DD BMfS

Authority: The BMfS Security Management Plan is issued by UKStratCom staffs on the authority of Director Support Transformation following endorsement by Dir BMfS.

Sponsor: Any queries or comments about this publication, including errors or omissions, should be addressed to the BMfS PMO, MOD Abbey Wood, NH2, Maple 1A.

Status/Maintenance: All hard copies of the BMfS Security Management Plan are uncontrolled. This document will be reviewed annually and/or after significant policy/guidance changes and programme milestones. The BMfS PMO continually monitors HMG/MOD security policy sources and will publish interim guidance if required to key stakeholders and delivery agents.

TABLE OF CONTENTS

Contents

INTRODUCTION

1.1 The BMfS Security Management Plan (SMP) is a source of policy and guidance that covers mandatory controls, processes and behaviours deemed essential to protect Defence assets including data and information during the delivery of the BMfS programme. The SMP explains how Ministry of Defence expects people to act in order to protect themselves, and the security of the Armed Forces and the department more generally. The rules in this SMP apply to everyone who works in the BMfS Programme, whether employed directly in the military or civil service, or working with our information or assets as a contractor or in industry.

1.2 The information in this document therefore needs to be understood by everyone involved in the delivery of BMfS – regardless of grade, rank or status. This document is supplementary to the Governments Security Policy Framework and Defence Manual of Security (JSP440). In the event of conflict these documents have primacy.

SCOPE

2.1 The SMP covers general business, Information Assurance (IA) & security policies, processes, and procedures implemented by the BMfS Programme within SpTx covering:

a. Information Security

b. Use of corporate-provided GFX information systems, Defence networks, and software applications (e.g. MoDNET, MOSS, HRMS, etc);

c. Personnel Security;

d. Physical building/site security.

PURPOSE

3.1 The purpose of the SMP is to improve overall business resilience by providing security context and guidance to BMfS staffs, Delivery Agents and suppliers delivering elements of the BMfS Programme. It is intended to help the BMfS programme survive and maintain the delivery of Support INFORM capability, outputs and objectives by ensuring it has the ability to anticipate, prepare for, respond and adapt to security threats and risks. The SMP outlines the security principles, process, controls essential to ensure:

a. Defence information assurance;

b. Defence reputational assurance;

c. protection against counter intelligence & counter crime;

d. information integrity and availability is maintained;

e. information access controls & accountability are maintained;

BENEFITS

4.1 The key benefits of compliance with the approach outlined in the SMP to BMfS, its Customers and MOD Authorities are:

a. Clear direction on IA, RA and Cyber Security standards that need to be addressed to ensure compliance with MOD and UK Government policy and legislation.

b. Security processes can be conducted in a consistent manner enabling greater standardisation of the process across the Operating Centre.

c. The right people will be involved at the right time and individual responsibilities are understood.

d. Expectations and results from employing IA, RA and Cyber Security processes are clear and understood.

e. System security processes are consistently & accurately documented, executed in a controlled manner, are measurable and auditable, and support the accreditation process.

f. That IA, RA and Cyber Security is considered throughout the delivery of the BMfS Programme of work, and that changes to delivery approach, strategy and deliverables are suitably and sufficiently considered to align with the Senior Information Owner's stated risk appetite.

STANDARDS REGULATIONS AND LEGISLATION

5.1 Protection of information and the related obligations placed on the MoD are covered in the following Acts of Parliament:

a. Official Secrets Act 1989

b. Data Protection Act 1998

c. Freedom of Information Act 2000

d. Defence and Security Public Contracts Regulations 2011

5.2 These set the statutory framework within which the Authority and contractors working on behalf of the Authority operate.

PRINCIPLES

6.1 The protection of Government information is governed by the principle that unauthorised disclosure of information:

a. damages defence;

b. may lead to criminal prosecution; and

c. is a disciplinary offence for certain categories of information under Ministry of Defence (MoD) Personnel Policy, Rules and Guidance.

6.2 All information that HMG collects, stores, processes, generates or shares to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

6.3 Everyone who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked with a classification or not. BMfS has adopted the following key principles to ensure appropriate safeguarding of government data and information:

a. Everyone is responsible for security

b. Protective security should follow national security guidance and ensure that HMG's assets are robustly protected.

c. Security must enable the effective delivery of BMfS and the Senior Responsible Owner's (SRO) strategic intent. It should be framed to support the Programme objectives, to work transparently and openly, and to deliver outcomes efficiently and effectively.

d. Risk management is key and should be driven from The SpTx Steering Group. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level. This process will take full account of relevant statutory obligations and protections, including data protection legislation, the Freedom of Information Act, the Official Secrets Act, Equality Act, and the Serious Organised Crime and Police Act.

e. Attitudes and behaviours are fundamental to good security. The right security culture, proper expectations and effective training are essential.

f. Policies and processes will be in place for reporting, managing and resolving any security incidents. Where systems have broken down or individuals have acted improperly, the appropriate action will be taken.

g. Weakest Link Principle - a chain is only as strong as its weakest link. Risk will be assessed holistically with all elements including processes, people and technology considered to identify potential threats.

h. Reputational Risk by Association Principle – The programme will consider all risks to delivery of the BMfS Programme of work to impact on Programme reputation even where threats impact external to the authority.

POLICY

7.1 The BMfS Security Management Plan is derived from and compliant with the policies and standards in the following Joint Service Publications (JSPs):

a. JSP 440: The Defence Manual of Security.

b. JSP 441: Managing Information in Defence.

c. JSP 490: Defence Crypto-security Operating Instructions.

d. JSP 525: Corporate Governance.

e. JSP 604: The Defence Manual for ICT.

f. JSP 740 – Acceptable Use Policy for ICT

g. JSP 892: Risk Management.

h. JSP 903: Defence Top Secret Information Handling Model (SECRET).

i. The Defence Security Handbook

ROLES

8.1 Everyone is responsible for security, but within the account there are a number of security roles formally held;

8.1.1 **Senior Security Risk Co-ordinators (SSRCs)** UKStratCom as a TLB has appointed a Senior Security Risk Co-ordinator (SSRC) to provide advice and direction regarding balancing business needs and security requirements.

8.1.2 **Senior Responsible Owner (SRO) -** The SpTx SRO is ultimately accountable for developing and delivering Support Capabilities into service. The role of SRO extends to accountability for all SpTx programmes and integral projects ensuring they meet their objectives, deliver required outcomes and realise required benefits within an agreed performance, cost and time envelope. The SRO is responsible and accountable for all aspects of governance including risk and threat management and programme Security processes. The SRO is the ultimate point of escalation and decision maker for threats to the Programme including those arising from security.

8.1.3 **Support Chief Information Officer - Information Owner for Support on behalf of Defence -** The Sp CIO role is delegated responsibility by Chief of Defence Logistics and Support to own Defence Support Information on behalf of Defence. They are responsible for information and data assurance

practices, risk management and compliance reporting capabilities relating to use of Defence information and data. The Sp CIO delivers three critical functions;

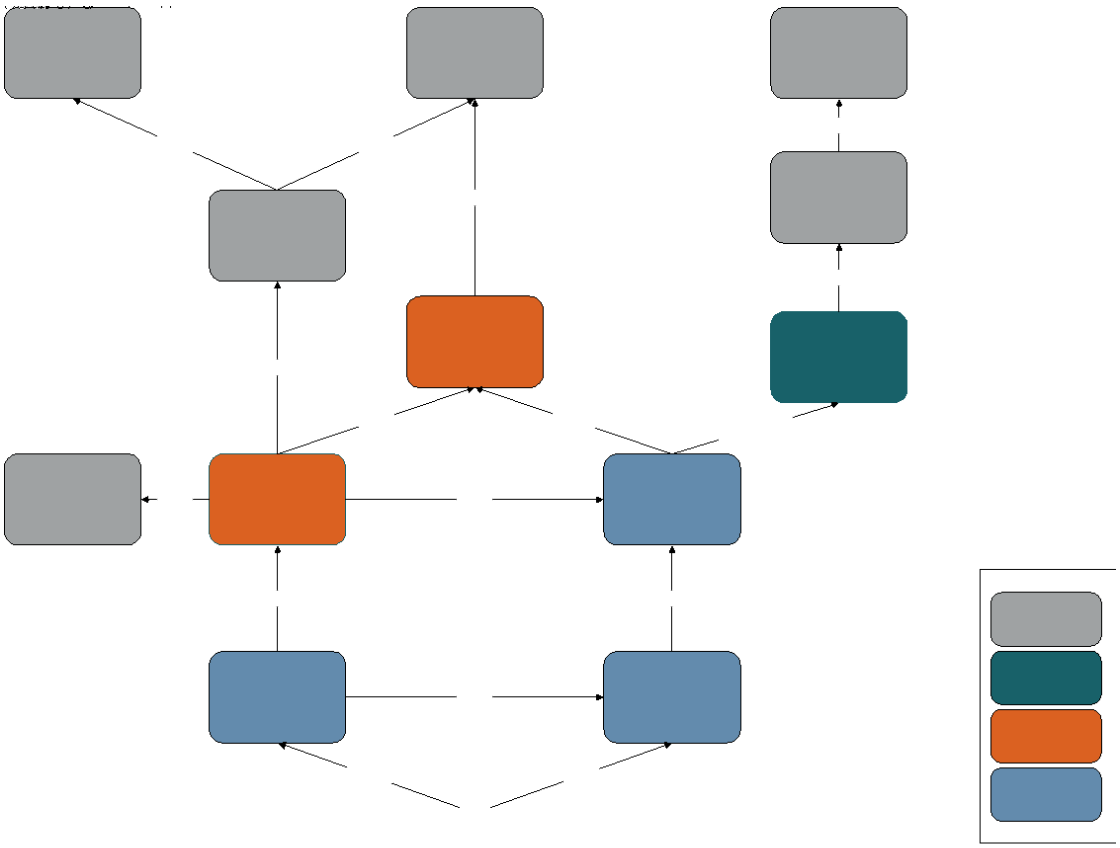
- An “Information Risk Management” function, aggregating all management and reporting activities across the Defence Support Organisation (DSpO).
- An “IT Security” function, focused on the architecture of functional and technical controls.
- A “Security Operations” function, focused on driving the implementation of controls through the application of technical standards and procedures designed in accordance with MoD policy to protect Defence assets and reputation

8.1.4 **SpTx Principal Security Advisor (PSyA)** –The senior security specialist for SpTx who advises management on all aspects of security. Within SpTx this role is combined with the role of Establishment Sy Officer (ESyO) as outlined in JSP 440 guidance and includes providing advice to the management chain on all aspects of security and coordination of resources allocated to security. The PSyA is best placed to understand: the establishment’s mission/operational outputs and therefore critical capabilities, infrastructure and assets; the local threat; the vulnerabilities and local profile of the establishment and is able to reflect the SRO’s and line managers’ Risk Appetites; and the effect on outputs if security incidents occur and impinge on operations or business outputs.

8.1.5 **Branch SyO (BSyO) – This role is the individual tasked with managing basic** security functions within BMfS. This is an additional tasking rather than a full time post. The BSyO has received security training and is able to provide limited advice. They have a good knowledge of the programme’s objectives and planned outputs and are able to assess the positive or negative impact of security procedures on individual Areas of Responsibility (AORs).

GOVERNANCE

9.1 Governance and points of escalation follow the model detailed in the Defence Security handbook and is detailed below:



THE GOVERNMENT SECURITY CLASSIFICATION SYSTEM

10.1 The MoD like the rest of HMG uses the Government Security Classification (GSC) System. In addition to being classified all information must be correctly and clearly labelled so that users understand how it must be handled, following handling instructions, national caveats and compartments, outlined in Cabinet Office guidance on Government Security Classifications and within JSP 440 Part 2 and JSP 441. The following classifications are defined in those documents:

10.1.1 OFFICIAL - The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or disclosed inappropriately, but are not subject to a heightened risk profile. This includes the information relating to the routine operation of Defence.

10.1.2 OFFICIAL SENSITIVE - A special subset of OFFICIAL has also been specified and has been named OFFICIAL SENSITIVE. Under government guidance, OFFICIAL SENSITIVE broadly covers information classified within the legacy system as RESTRICTED and CONFIDENTIAL. There are certain concessions for OFFICIAL SENSITIVE information which means that its treatment differs from that of RESTRICTED and CONFIDENTIAL under exceptional circumstances.

10.1.3 OFFICIAL SENSITIVE classified information can be combined with descriptors to indicate that common sense is needed to limit access appropriately. The approved descriptors are;

10.1.3.1 COMMERCIAL – To identify commercial or market-sensitive information, including that which is subject to statutory or regulatory obligations that may be damaging to HMG or to a commercial partner if improperly accessed.

10.1.3.2 PERSONAL – To identify Personal Data (as defined by the Data Protection Act) whose release or loss could cause harm, distress or detriment to the individual(s) to whom it relates. MoD must ensure that it fulfils its obligations under the Data Protection Act.

10.1.4 SECRET - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime. There is a significant step up between OFFICIAL and SECRET.

10.1.5 TOP SECRET - HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

HANDLING INFORMATION SECURELY BY ALL DEFENCE PERSONNEL

11.1 Information needs to be assessed and managed so that the Department may make informed, practical and effective decisions. This requires a mature understanding of the security risks, arrangements to determine and apply cost-effective controls to mitigate identified risks and assurance processes to ensure mitigations remain effective. When managing information, the following processes should be followed:

11.1.1 Apply good information security behaviours in order to prevent and identify potential information or cyber security incidents and events.

11.1.2 Handle information with care to avoid loss, damage or inappropriate access.

11.1.3 Use appropriate Information and Communications Technology (ICT) systems and follow guidance on specific sensitivities and handling requirements.

11.1.4 Store assets securely when not in use, e.g. implement clear desk policies and screen locking when ICT is left unattended.

11.1.5 Appropriately protect data in transit and at rest.

11.1.6 Appropriately protect assets taken outside the work environment, ensuring they are protected in transit, not left unattended and stored securely.

11.1.7 Take precautions to prevent overlooking or inadvertent access to information when working remotely or in public places.

11.1.8 Exercise appropriate discretion when discussing Departmental business in public or by telephone, and keeping details of sensitive material to a minimum.

11.1.9 Take particular care when sharing information with external partners or the public.

11.1.10 Ensure that information that is not freely available in the public domain is destroyed in a way that makes reconstitution unlikely. More sensitive assets should be returned to the office for secure disposal where appropriate.

11.1.11 Use all ICT equipment in accordance with Security Operating procedures (SyOPs) and JSP 740 (Acceptable Use Policy).

11.1.12 Ensure passwords, PINs and other authentication devices (including smartcards and access tokens) are appropriately protected and not shared, and that any passwords are strong.

11.1.13 Apply requirements relating to Information Protection Zones, including the use of Portable Electronic Devices (PEDs).

11.1.14 Follow requirements for processing of bulk and/or personal data.

11.2 The policy of the BMfS Programme is that information classified OFFICIAL SENSITIVE and above will not be sent over the internet and will not be taken off site unless this has been explicitly agreed by the BMfS PMO who will ensure appropriate controls have been applied.

11.3 The more widely information is circulated, the greater the difficulty in protecting it. Consequently, you may disclose official information only to those who require the knowledge for the conduct of their official duty. Unauthorised disclosures of official information be it protectively marked or unclassified, in any form, is an offence under the Official Secrets Act and is a disciplinary matter. Staffs are generally security cleared to have access to SECRET material, with the occasional viewing of TOP SECRET (TS). Staff who require regular access to TS and Caveated material will require a Developed Vetting (DV) clearance.

SYOPS

12.1 All MoD employees, contractors or suppliers accessing the Defence Local Area Network (LAN) or MoDnet, are required to act in accordance with the MoDnet official user Security Operating Procedures (SyOPs). Details of the SyOPs can be found at MoDnet official user SyOPs

12.2 All staffs are required maintain an up to date SyOPs agreement and abide by all instructions and guidance.

GFX AND USE OF PERSONAL DEVICES

13.1 Classified MoD material (above OFFICIAL) should only be stored and processed on Authority devices, in accordance with JSP 440 guidance. Any exception to this rule must to be agreed with the PSyO and permission must be provided in writing, specifying limitations on the material, devices, and what handling protocols will apply.

Note: OFFICIAL (unmarked) information shall not, under any circumstances, be sent to unsecured personal email addresses. When working on OFFICIAL (unmarked) information, corporate IT equipment must be used, not personal devices unless with the express permission of the BSyO or PSyO.

13.2 All protectively marked material will be stored on MoDNet unless storage on an appropriate secure system has been agreed in writing by the with the PSyO. Any storage of Defence information and data can be subject to audit by the BSyO or PSyO at any time.

13.3 The following instructions relate to the use of non-Authority issued laptops:

13.3.1 Only material that is unmarked or OFFICIAL can be held on non-Authority issued devices.

13.3.2 Having encryption on a device does not mean that material higher than OFFICIAL can be stored without prior authorisation by the BSyO/PSyO.

13.3.3 When Authority Information and data is stored on non-Authority devices the same SyOps rules will apply to their use, carriage and storage.

DATA TRANSFER

14.1 Authority data must only be transferred to an appropriate Authority device unless approval is granted by the PSyO to transfer data to a non-Authority device with appropriate encryption and access controls.

14.2 Removable media containing protectively marked material must be treated according to the highest protective marking applied to any contained document.

14.3 The generation of hard copy material should be minimised. All hard copy material must be appropriately marked with the appropriate government classification. In all cases, the individual has responsibility for the material in their possession. Any loss of documents outside of the client location must be treated as a breach and the reporting procedures followed at the earliest opportunity.

14.4 Printing hard copy should only be done if essential. When printing all staffs must ensure that they collect all print jobs in a timely fashion to ensure that the data is not accessed by anyone who should not do so. Where network printers operate a ‘secure print’ function, this should be used by default for protectively marked or sensitive material.

14.5 The policy of the BMfS Programme is that OFFICIAL SENSITIVE information will not be sent over the internet and will not be taken off site unless this has been explicitly agreed by the BMfS PMO who will ensure appropriate controls have been applied.

PHYSICAL SECURITY/SITE SECURITY

15.1 The MoD is at risk from a number of sources such as International and Domestic Terrorism, Extremist Groups, Espionage, Subversion, Protest activity, Investigative Journalism and Sabotage to name just a few. It is therefore vital we have in place effective methods of security that we are all familiar with in order to counteract the threats we face.

15.2 The MoD Guard Service (MGS) have responsibility for the securing and protection of MoD sites. The MGS have the authority to search the contents of any vehicle, package, or container entering or leaving the establishment, with the consent of the owner, and where there are reasonable grounds for such actions, deny entry or exit until authorised by a responsible officer. These are the condition of entry and condition of service searches. Refusal to agree to being searched is a disciplinary offence. The MGS have authority to remove any out of date MoD Site Access Passes and pass them to the ESyO team. The MGS have the authority to make a citizen's arrest.

MGS contact details:
Internal – [REDACTED]
External – [REDACTED]

15.3 The MoD Police (MDP) is a statutory force of civilian police officers, whose authority is granted in the Ministry of Defence Police Act 1987. Their duty is to provide an effective police service to the MoD. In the event of a significant breach that amount to the level of criminality the MDP have further powers of investigation additional to those of the MGS.

MoD Police contact details:
Internal – [REDACTED]
External – [REDACTED]

15.4 All MoD establishments have site security instructions and Site Administration and Operating Procedures (SAOPs) that provide specific instructions around access and conduct when on site. Most MoD sites employ a system of photographic Site Access Passes which grant entry to and from MoD sites on production. All personnel are responsible for the Safety of any issued MoD Site Access Passes. The loss, or suspected theft, of a MoD pass must be immediately reported to the BMfS BSO and the pass issuing office for further advice. If you believe you have lost your pass off site you must inform your local police force or report the loss on line at www.reportmyloss.com.

SOCIAL MEDIA AND PERSONAL ONLINE SECURITY

16.1 Personnel who use social networking sites are reminded that they are not to divulge they work for the MoD and are to be careful of any mention of the area they are working in. Government guidance on how to keep safe online is provided at the following sites:

Think before you share
Social networking and security
Personal online security

DISCLOSURE TO MEDIA AND ELECTED OFFICALS

17.1 No member of staff or person engaged by BMfS should allow themselves to be interviewed by a representative of the Media or Member of Parliament on official matters, or communicate with them on official matters, without authorisation to do so. The PSyA should be advised of the initial approach in these cases.

17.2 All staff must be particularly on their guard against disclosing official information in public places, at commercial exhibitions, receptions, non-official conferences, staff parties etc.

PASSING CLASSIFIED INFORMATION OVER TELEPHONES - VULNERABILITIES

18.1 No telephone system is fully secure, vulnerabilities include the following:

18.1.1 Casual overhearing - is overhearing by people near the telephone being used, or those who may have access to the exchange, such as technicians. If the matter overheard is interesting enough, this may encourage deliberate eavesdropping.

18.1.2 Deliberate interception - is intentional, planned interception by Foreign Intelligence Services (FIS), subversive organisations or militant members of protest groups, nationalist organisations, and members of the press. The techniques involved include the use of covert eavesdropping devices and hacking into telephone switch software.

18.1.3 Microwave and Satellite links can be intercepted from numerous places including foreign diplomatic premises both within the UK and overseas. Due to the inappropriate sitting of telephones there are also Radiation Security (RADSEC) vulnerabilities.

18.2 Use of Public Switched Telephone Networks (PSTN), including the Government Telephone Networks (GTN) (for inter-governmental department communications) and Mobile Telephones, may only be used for conversations at OFFICIAL (which includes OFFICIAL-SENSITIVE). The table below gives full details of appropriate controls when communicating sensitive information:

EQUIPMENT	AREA	PROTECTIVE MARKING
Telephone Networks (Public and DFTS)	UK & Overseas	[REDACTED]
Secure Telephone Network (Cryptographically protected as appropriate e.g. Brent)	UK & Overseas	[REDACTED]
Digital Mobile Telephones	UK & Overseas	[REDACTED]
Voicemail (Fixed or mobile networks)	UK & Overseas	[REDACTED]
Voice Over IP1	UK & Overseas	[REDACTED]
Short Message Service (SMS)	UK & Overseas	[REDACTED]
Multi-media Message Service (MMS)	UK & Overseas	[REDACTED]
Video/Tele Conferencing (VTC) - insecure VTC, i.e. not cryptographically protected and including public and DFTS telephone services i.e. Zoom & MS Teams	UK & Overseas	[REDACTED]
Video/Tele Conferencing (VTC) Secure, i.e. cryptographically protected as appropriate	UK & Overseas	[REDACTED]

INCIDENT REPORTING PROCEDURE

19.1 This section details the incident handling procedure. A security incident includes any breach of security, any loss of protected information, any potential loss of protected information, any breach of data handling requirements or any near miss. All security incidents must be reported to the BSyO and recorded in the Programme Security log, owned by the BSyO.

19.2 In the event of a security incident the following procedure will be used:

19.2.1 Step 1: Immediate action by individual experiencing the theft or loss
Make an immediate inventory of compromised material(s) identifying any loss or possible compromised items including:

- Documents/electronic media,
- Devices, Laptops, removable media, mobile phones or other data storage or communications devices
- Site security passes
- Personal and Sensitive information including names and contact details

19.2.2 Step 2: In the event of a loss or if you suspect a document has been compromised report the incident to the BSyO informing them of all sensitive material lost, stolen or potentially compromised.

19.2.3 Step 3: The BSyO will provide immediate advice and guidance to secure or re-secure any protected information assets.

19.2.4 Step 4: The BSyO will assess severity and impact before escalating to the PSyA when appropriate.

19.2.5 Step 5: The BSyO will complete a security investigation identifying route cause and impact resulting from the security incident details of which will be shared with the PSyO and the WARP. The BSyO can impose penalties including loss of access privileges and removal of any GFx. The BSyO can also seek to escalate the incident in the case of a serious breach with penalties available up to instant dismissal for Gross Misconduct and Criminal Prosecution where warranted.

BMfS	Business Modernisation for Support
BSyO	Branch Security Officer
DV	Developed Vetting
FIS	Foreign Intelligence Services
GCS	Government Classification System
GFX	Government Furnished Equipment
GTN	Government Telephone Networks
HMG	Her Majesties Government
HRMS	Human Resources Management System
IA	Information Assurance
ICT	Information and Communications Technology
JSP	Joint Services Publication
LAN	Local Area Network
MDP	MoD Police
MGS	MoD Guard Service
MMS	Multi-media Message Service
MoD	Ministry of Defence
MoDnet	The MoD intranet and internal network
MOSS	Microsoft SharePoint site
PEDs	Portable Electronic Devices
PMO	Project Management Office
PSTN	Public Switched Telephone Networks
PSyA	Principal Security Advisor
RA	Risk Assessment
SAOPs	Site Administration and Operating Procedures
SC	Security Clearance
SMP	Security Management Plan
SMS	Short Message Service
Sp CIO	Support Chief Information Officer
SpTx	Support Transformation
SRO	Senior Responsible Owner
SSRC	Senior Security Risk Co-ordinators
SyOPs	Security Operating procedures
TS	Top Secret
UKStratCom	Strategic Command
VTC	Video/Tele Conferencing