NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

SECURITY SERVICE
MI5

Security Operating Procedures (SyOPs) v3.0 for Privileged Users (PUs) with access to MI5 IT Systems and Services

Document Owner:	[REDACTION]
Issuing Authority:	***Senior MI5 Official***
Issue Date:	1st April 2014
Review Date:	1st April 2015

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

Abstract

MI5 defines a Privileged User (PU) as a registered user or account holder who manages the applications, services, equipment and security defences within the IT enterprise. IT account holders who develop and test are also considered to be PUs.

MI5 assesses the security risks of PUs as part of the output of HMG's mandated technical security risk assessment methodology. For a more business focussed and contextualised assessment, MI5 further assesses a PUs level of privilege using 5 criteria (Technology, Ability, Scope, Protective Marking, Criticality) so that they can be categorised as either an

Enhanced Standard User;
Standard Privileged User;
Enhanced Privileged User.

These Security Operating Procedures (SyOPs) are a requirement of the Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0) and outline the high level security responsibilities for all PUs with access to MI5 systems (which might also host SIA information). You must read these SyOPs and e-sign them using ***the relevant site*** (if you have access to ***the relevant system***), otherwise, you will be required to read and sign the declaration at the end of these SyOPs before you can apply for a PU account and at least annually thereafter to maintain access. It contains details of what you must do in order to maintain the Confidentiality, Integrity and Availability (CIA) of MI5 Information and IT systems (which might also contain SIA information) and what you should do in the event of a security incident.

Line Managers have a responsibility to ensure that information security is embedded in the everyday IT support services provided by their teams, however it is your personal responsibility to comply with these SyOPs; any deviations from these procedures may render you liable to disciplinary action. No departure from, or amendment to these SyOPs is permitted without the explicit permission of the ***the relevant team*** lead

As Developers are considered to be PUs, this version of the PU SyOPs supersedes/subsumes the Security Operating Procedures (SyOPs) for Developers working on Security Service IT System Environments v3.0 dated January 2011

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

Purpose

1 The purpose of these SyOPs is to inform all Privileged Users (PU) with elevated or administrative access to MI5 systems (which might include SIA information) of their personal security responsibilities. Since these high level SyOPs are generic across MI5 IT systems, there may be additional system level SyOPs that will need to be read and signed in addition to this document.

PU Security Operating Procedures (SyOPs)
What is mandated under these PU SyOPs

2. Before accessing any MI5 IT system with a PU account, you must:

a. Attend any relevant MI5 security and awareness briefings for IT staff (this includes induction training and any specific training requirements identified for the role by Line Managers for example) An eLearning package has been created and users must complete this as a pre-requisite to requesting a PU role/account and annually thereafter;

b. Be qualified and/or experienced (through training and certifications) for the role you are undertaking as a PU (for instance, an Active Directory administrator is expected to have the relevant competencies to fill that role)

c Read these SyOPs and e-sign them using ***the relevant site*** (if you have access to ***the relevant system***); otherwise, you will be required to read and sign the declaration at the end of these SyOPs to confirm that you will discharge your security responsibilities relating to PU access to MI5 IT systems. The latest version of these SyOPs must then be re-read and re-signed (either on ***the relevant site*** or manually) at least annually to retain PU access (reminders will be automatically emailed to PUs via ***the relevant site*** where e-signing has been used).

d Read and abide by MI5's Code of Practice for the Use of Electronic Facilities as required by ALL users of MI5 IT systems;

e. Read and understand the requirements of the Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0);

f. Hold a current DV and be a UK National in accordance with Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0). Some PU roles will require PUs to be Sensitive Post Checked (SPC), these roles will be identified as part of the PU Management and Business Authorisation (PUMBA) workflow used to authorise PU accounts ***the relevant team*** and you should check with your Line Manager to understand whether or not it applies to any of your PU roles/accounts. The relevant team PU roles do not currently use PUMBA however some PU accounts may still require SPC and you should liaise with your Line Manager to identify whether or not SPC applies to you ;

g Ensure that any PU access is applied for through the IT Service Desk request fulfilment process (***the relevant team*** supported systems) and/or other MI5 PU account processes and procedures (***the relevant team*** supported systems) and ***the relevant site*** support team);

h. Ensure that any of your personal PU accounts no longer required follow the correct MI5 processes and procedures to have those accounts disabled. If you still have PU access that is no longer required, you have a personal responsibility to initiate the process to have such access revoked; for ***the relevant team*** provisioned PU accounts, you can use PUMBA to initiate this.

What is allowed or prohibited under these PU SyOPs

3. You CAN:

a. Use properly authorised privileged access and/or accounts to administer systems or services as formally defined and agreed by each assigned and authorised PU role.

4. You MUST NOT:

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

a. Share authorised personal privileged access and/or personal accounts/passwords (personal accounts are those that are accessed using your unique badge identity and password) with any other person, regardless of circumstances;

b. Share authorised access to or knowledge of generic PU accounts/passwords ('service' accounts for example) with unauthorised users, regardless of circumstances. Note: Use of generic accounts must be avoided whenever possible. MI5 uses a system called ***the relevant system*** to manage access to/password generation for generic accounts. Where ***the relevant system*** is not being used for generic account access/password management, PUs are encouraged to discuss with their Line Managers why it is not being used. Where ***the relevant system*** is not being used to store passwords/manage access, ***the relevant team*** must also be consulted.

c. Leave any terminals unattended and unlocked where PU or Normal User access is available/logged in – terminals must be locked if you leave them and logged off at the end each working day. Where there is a valid unavoidable requirement to leave accounts logged in when users are not on MI5 premises or to leave terminals logged in and unattended but not locked, approval must be sought from the IT Security Officer (ITSO) and ***the relevant team*** must be informed.

d Leave connected sessions (to touchdown servers for example) running when logged off of desktops. Sessions must be disconnected AND logged off prior to desktop log off.

e. Abuse or attempt to abuse authorised privileged access to MI5 IT systems, functionality or data/information (notwithstanding Footnote[1] below).

f. Bypass/subvert or attempt to bypass/subvert system security controls (whether physical or technical security controls) or to use them for any purpose other than that intended (notwithstanding Footnote[1] below);

g Create or attempt to create any access account (PU or otherwise) or elevate privileges thereof without proper authorisation via the PUMBA workflow (***the relevant team*** supported systems) and/or relevant PU processes and procedures (***the relevant team*** supported systems and ***the relevant site*** support teams);

h. Share data with individuals who may not be authorised to access it themselves; for example external partners (including those who may be co-located with the user for periods of time) or other MI5 colleagues from different sections / business areas;

i. Transfer any data to or from any MI5 IT system other than via the authorised import/export procedure managed by the ***the relevant system*** (corporate/investigative systems) ***the relevant site*** team local processes and procedures (***the relevant site*** only) or local ***the relevant team*** processes and procedures (operational systems). Data transfers (whether data moves or data copies) between MI5 IT systems must be authorised by the Data Transfer Process (managed by ***the relevant team***) before they are conducted.

j. Make any unauthorised modifications or configuration changes to software or hardware. All changes must be authorised through the formal change process (corporate/investigative systems) or local ***the relevant team*** local processes and procedures (operational systems);

k. Access/administer or attempt to access/administer Production ('live') system infrastructure or applications through Non-Production ('test') environments/accounts or vice versa, unless the following exceptions apply:

[1] 1 It is noted that some PU roles (Testers, ***the relevant team*** operational PU roles, [REDACTION] for example) are sometimes required to do this as part of their role and therefore will sometimes be exempt; however, such activity must still be authorised by a formal test plan and/or operational business case as appropriate and the number of people in such roles must be kept to the least amount possible. Test plans and business cases must provide time bound access constraints for such roles. It is the responsibility of each individual PU to assure themselves that such authorisation is in place through relevant Line Managers and that their access privileges are disabled when no longer required.

i. If you have been granted a 'core' account, the ability to access both 'live' and 'test' environments using your core account is acknowledged and permitted. However, you must ensure that you only use your core account for authorised tasks,

ii. If you are required to use ***the relevant system*** for your PU role access (which could be accessed using your credentials for ***the relevant account*** depending on how you have been given access to safe(s)), then you must only initiate onward (transparent) connections using stored accounts available in the safe(s) appropriate to the target environment. For example, ***the relevant account*** available in safe(s) must only be used to access ***the relevant account*** environments respectively.

l. Be granted physical access to infrastructure hardware (usually but not always in data centres) without proper authorisation supported by a valid business case;

m. Use privileged account access to perform non-privileged functions;

n. Auto forward material from your PU account to any other account;

o. Connect or attempt to connect any unauthorised external devices or media (such as laptop PCs, USB sticks, smart phones or personal organisers) to any MI5 network or system, regardless of circumstances.

Public Key Infrastructure - PU Responsibilities

5. As a PU, you will be able to request a Public Key Infrastructure (PKI) certificate for use on hardware devices or software applications. Devices and software applications are referred to as Non Person Entities (NPE).

6. PUs shall note that:

a. To request an NPE certificate you must be the system owner (or delegated owner) and an existing PKI subscriber. Requests must be made using your user account (not your privileged account)

b. You must only use NPE certificates within the environment/system it was issued from and for its intended use. E.g. ***The relevant system*** certificates must only be used within ***the relevant system***.

c. Any passwords/passphrases used to access key material must be defined and managed within ***the relevant system***. You must protect and secure keys and credentials in accordance with the MI5 code of practice, MI5 policies and procedures and the Certificate Practice Statement (all available on ***the intranet***)

d. You are responsible for the renewal of any NPE certificates you request and must identify a suitable secondary nominated contact and a replacement contact should you move or leave your post. You must notify the certificate manager of any changes to the nominated contacts.

Methods of enforcement of these PU SyOPs

7. PU roles, responsibilities and access controls may apply at infrastructure, system or application level. PUs are to be assigned with accounts and passwords aligned to the security requirements of each system or application and in accordance with Cyber Security Technical Policy produced by ***the relevant team*** and/or specific ***the relevant team*** local policy where there are specific and authorised operational requirements.

8. The full requirements of the Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0) must be implemented.

Compliance with these PU SyOPs - Protective Monitoring

9. MI5 reserves the right to monitor all usage of its IT systems by individuals in order to identify instances of misconduct, to support incident response and/or investigations.

10 Misconduct is defined as conduct prejudicial to the interests of MI5 and/or failure to comply with official instructions. Any misconduct may result in formal warnings recorded on your vetting file and/or disciplinary action up to and including dismissal. See Manual of General Conditions of Service (MGCS) Section 81 (available on ***the intranet***).

11 Line Managers have a duty to report matters which may constitute misconduct to ***the relevant team***, however all users should consider it their duty to report incidents as necessary either to their Line Manager or direct to ***the relevant team*** as appropriate

12. Audit logs will be generated and monitored for all system users including PUs. User actions must be attributable to individuals

13. In addition to routine Protective Monitoring, spot checks will be conducted to ensure that processes and procedures remain in place and are being properly adhered to.

Security Incident Reporting

14 Any person discovering a security incident MUST report it immediately to their Line Manager or if unavailable, the IT Service Desk (or SSDO out of hours) or (for the operational business) using local ***the relevant team*** processes and procedures, taking care to note all relevant details (e.g. time, place, persons involved, equipment involved etc). In addition, all security incidents must be reported to the MI5 IT Security Officer. Incidents may include (not exhaustive):

a. All hardware or software faults encountered within live environments where a breach of security is suspected as a cause;

b. If a security breach is encountered (including any unauthorised access attempts);

c. If any form of hardware or software tampering of any kind is suspected;

d. If anti-virus checks alert that a virus is encountered (in this instance, note any messages or alerts that are displayed, shut down the terminal and do not use it again until you are informed that it is safe to do so). Where applicable, local ***the relevant team*** processes and procedures must be followed for viruses discovered in operational environments;

e Any suspected compromise of passwords or authentication token/device;

f. Any observation of events by others that are considered to be detrimental to MI5 security

15 A relatively minor incident might develop into a more serious one if not investigated promptly and treated appropriately.

16 Failure to report a security incident is a disciplinary offence. Admitting to an honest mistake will be treated more favourably than trying to cover up an incident.

17. ***The relevant team's*** Cyber Security Policy [REDACTION] – IT Security Incident Management Policy must be adhered to.

Exemptions and Waivers to these PU SyOPs

18. Requests for exemptions and/or waivers for anything covered in these SyOPs should be submitted to the ***the relevant team*** with a full business justification. ***The relevant team*** will advise the details of the process when contacted.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

Review Criteria

19 Any changes to related internal MI5 policies will result in a review of these SyOPs Otherwise, these SyOPs will be reviewed on an annual basis

NOTE. REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

DOCUMENTCONTROL

Document History

Version	Date	Summary of Changes	Changed By
0.1	08/11/2010	Initial draft.	***MI5 Official***
0.2	08/02/2011	Updated following review meeting with ***MI5 Official***	***MI5 Official***
1.0	16/02/2011	Updated following final review comments prior to issue.	***MI5 Official***
1.2	18/09/2012	Document reviewed in line with the new version of the PU Policy version 1.4	***MI5 Official***
2.0	27/9/2012	Version number to 2.0 Issued for publication.	***MI5 Official***
2.1	05/12/2013	Updates to bring into line with v3.0 of PU Policy and routine annual review.	***MI5 Official***
2.2	25/02/2014	Updates to v2.1 following wide business review	***MI5 Official***
3.0	01/04/2014	Version 3.0 issued for publication as latest version.	***MI5 Official***

GLOSSARY

Term	Definition
Availability	The property of information being accessible and usable upon demand by an authorised entity
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Integrity	The property of safeguarding the accuracy and completeness of information – this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later
Privileged User	In line with HMG's technical security risk assessment framework's Information Assurance Standard No.1 (IAS1) definition, a Privileged User (PU) is a registered user or account holder who manages the applications, services, equipment and security defences within the IT enterprise. MI5's PU Policy also includes those account holders who develop and test. PUs can usually not be constrained in the same way as a Normal (Standard) User and as such are represented as a separate threat actor type. MI5 considers the security risks from PUs as part of the output of HMG's mandated IAS1 technical security risk assessment. For a more business focussed and contextualised assessment, MI5 further applies the security risk assessment method described in Annex A of the PU Policy to assess a PUs level of privilege using 5 criteria (Technology, Ability, Scope, Protective Marking, Criticality) so that they can be categorised as either an;

	- Enhanced Standard User; - Standard Privileged User; - Enhanced Privileged User.	
	Risk	The potential that a given threat will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to the organisation
	Risk Management	Process of coordinating activities to direct and control an organisation with regard to risk
	Risk Tolerance	Risk tolerance is closely related to risk appetite, whereas appetite refers to risk at the corporate level, risk tolerance allows for variations in the amount of risk an organisation is prepared to accept for a particular project or programme.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

DECLARATION

You must sign these SyOPs on ***the relevant site*** agreeing to the terms and requirements detailed in these PU SyOPs (Version 3.0). If you are not able to e-sign these SyOPs on ***the relevant site*** because you do not have access then you must complete the declaration below
The declaration must be completed and returned to ***the relevant team***. ***the relevant team*** PUs and ***the relevant team*** for ***the relevant team*** PUs.

A Privileged User account cannot be issued until this form has been received by the ***the relevant team*** along with a completed PU Account Request Form.

Declaration
I have attended all relevant MI5 security and awareness briefings for PUs with access to MI5 IT systems and have full DV clearance.

I have read these PU SyOPs and understand my responsibilities as detailed within them.

I undertake to observe these SyOPs and take all reasonable precautions to ensure that I do not breach the security requirements detailed therein

I will inform my Line Manager, the ***the relevant team*** and IT Service Desk (***the relevant team***) or follow local ***the relevant team*** or ***the relevant site*** team processes and procedures when I no longer need PU access for specific systems.

I understand that if I fail to observe these SyOPs, I may be subject to disciplinary action.

Name: ..... Pass (***the relevant site***) No: .....

Signature: ..... Date: .....

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

SECURITY SERVICE
MI5

Security Operating Procedures (SyOPs) v3.0 for Privileged Users (PUs) with access to MI5 IT Systems and Services

Document Owner:	[REDACTION]
Issuing Authority.	***Senior MI5 Official***
Issue Date:	1st April 2014
Review Date:	1st April 2015

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

Abstract

MI5 defines a Privileged User (PU) as a registered user or account holder who manages the applications, services, equipment and security defences within the IT enterprise IT account holders who develop and test are also considered to be PUs.

MI5 assesses the security risks of PUs as part of the output of HMG's mandated technical security risk assessment methodology For a more business focussed and contextualised assessment, MI5 further assesses a PUs level of privilege using 5 criteria (Technology, Ability, Scope, Protective Marking, Criticality) so that they can be categorised as either an:

Enhanced Standard User;
Standard Privileged User;
Enhanced Privileged User.

These Security Operating Procedures (SyOPs) are a requirement of the Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0) and outline the high level security responsibilities for all PUs with access to MI5 systems (which might also host SIA information) You must read these SyOPs and e-sign them using ***the relevant site*** (if you have access to ***the relevant system***); otherwise, you will be required to read and sign the declaration at the end of these SyOPs before you can apply for a PU account and at least annually thereafter to maintain access. It contains details of what you must do in order to maintain the Confidentiality, Integrity and Availability (CIA) of MI5 Information and IT systems (which might also contain SIA information) and what you should do in the event of a security incident.

Line Managers have a responsibility to ensure that information security is embedded in the everyday IT support services provided by their teams, however it is your personal responsibility to comply with these SyOPs, any deviations from these procedures may render you liable to disciplinary action No departure from, or amendment to these SyOPs is permitted without the explicit permission of the ***the relevant team*** lead.

As Developers are considered to be PUs, this version of the PU SyOPs supersedes/subsumes the Security Operating Procedures (SyOPs) for Developers working on Security Service IT System Environments v3.0 dated January 2011.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

Purpose

1 The purpose of these SyOPs is to inform all Privileged Users (PU) with elevated or administrative access to MI5 systems (which might include SIA information) of their personal security responsibilities. Since these high level SyOPs are generic across MI5 IT systems, there may be additional system level SyOPs that will need to be read and signed in addition to this document.

PU Security Operating Procedures (SyOPs)
What is mandated under these PU SyOPs

2. Before accessing any MI5 IT system with a PU account, you must:

a. Attend any relevant MI5 security and awareness briefings for IT staff (this includes induction training and any specific training requirements identified for the role by Line Managers for example). An eLearning package has been created and users must complete this as a pre-requisite to requesting a PU role/account and annually thereafter;

b. Be qualified and/or experienced (through training and certifications) for the role you are undertaking as a PU (for instance, an Active Directory administrator is expected to have the relevant competencies to fill that role).

c. Read these SyOPs and e-sign them using ***the relevant site*** (if you have access to ***the relevant system***); otherwise, you will be required to read and sign the declaration at the end of these SyOPs to confirm that you will discharge your security responsibilities relating to PU access to MI5 IT systems. The latest version of these SyOPs must then be re-read and re-signed (either on ***the relevant site*** or manually) at least annually to retain PU access (reminders will be automatically emailed to PUs via ***the relevant site*** where e-signing has been used).

d. Read and abide by MI5's Code of Practice for the Use of Electronic Facilities as required by ALL users of MI5 IT systems.

e. Read and understand the requirements of the Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0);

f Hold a current DV and be a UK National in accordance with Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0) Some PU roles will require PUs to be Sensitive Post Checked (SPC); these roles will be identified as part of the PU Management and Business Authorisation (PUMBA) workflow used to authorise PU accounts ***the relevant team*** and you should check with your Line Manager to understand whether or not it applies to any of your PU roles/accounts. The relevant team PU roles do not currently use PUMBA however some PU accounts may still require SPC and you should liaise with your Line Manager to identify whether or not SPC applies to you ;

g Ensure that any PU access is applied for through the IT Service Desk request fulfilment process (***the relevant team*** supported systems) and/or other MI5 PU account processes and procedures (***the relevant team*** supported systems) and ***the relevant site*** support team).

h. Ensure that any of your personal PU accounts no longer required follow the correct MI5 processes and procedures to have those accounts disabled If you still have PU access that is no longer required, you have a personal responsibility to initiate the process to have such access revoked, for ***the relevant team*** provisioned PU accounts, you can use PUMBA to initiate this.

What is allowed or prohibited under these PU SyOPs

3. You CAN:

a. Use properly authorised privileged access and/or accounts to administer systems or services as formally defined and agreed by each assigned and authorised PU role

4 You MUST NOT:

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

a. Share authorised personal privileged access and/or personal accounts/passwords (personal accounts are those that are accessed using your unique badge identity and password) with any other person, regardless of circumstances;

b. Share authorised access to or knowledge of generic PU accounts/passwords ('service' accounts for example) with unauthorised users, regardless of circumstances. Note: Use of generic accounts must be avoided whenever possible. MI5 uses a system called ***the relevant system*** to manage access to/password generation for generic accounts. Where ***the relevant system*** is not being used for generic account access/password management, PUs are encouraged to discuss with their Line Managers why it is not being used. Where ***the relevant system*** is not being used to store passwords/manage access, ***the relevant team*** must also be consulted.

c. Leave any terminals unattended and unlocked where PU or Normal User access is available/logged in – terminals must be locked if you leave them and logged off at the end each working day. Where there is a valid unavoidable requirement to leave accounts logged in when users are not on MI5 premises or to leave terminals logged in and unattended but not locked, approval must be sought from the IT Security Officer (ITSO) and ***the relevant team*** must be informed,

d. Leave connected sessions (to touchdown servers for example) running when logged off of desktops. Sessions must be disconnected AND logged off prior to desktop log off.

e. Abuse or attempt to abuse authorised privileged access to MI5 IT systems, functionality or data/information (notwithstanding Footnote[1] below);

f. Bypass/subvert or attempt to bypass/subvert system security controls (whether physical or technical security controls) or to use them for any purpose other than that intended (notwithstanding Footnote[1] below);

g. Create or attempt to create any access account (PU or otherwise) or elevate privileges thereof without proper authorisation via the PUMBA workflow (***the relevant team*** supported systems) and/or relevant PU processes and procedures (***the relevant team*** supported systems and ***the relevant site*** support teams),

h. Share data with individuals who may not be authorised to access it themselves; for example external partners (including those who may be co-located with the user for periods of time) or other MI5 colleagues from different sections / business areas.

i. Transfer any data to or from any MI5 IT system other than via the authorised import/export procedure managed by the ***the relevant system*** (corporate/investigative systems), ***the relevant site*** team local processes and procedures (***the relevant site*** only) or local ***the relevant team*** processes and procedures (operational systems). Data transfers (whether data moves or data copies) between MI5 IT systems must be authorised by the Data Transfer Process (managed by ***the relevant team***) before they are conducted;

j. Make any unauthorised modifications or configuration changes to software or hardware. All changes must be authorised through the formal change process (corporate/investigative systems) or local ***the relevant team*** local processes and procedures (operational systems),

k. Access/administer or attempt to access/administer Production ('live') system infrastructure or applications through Non-Production ('test') environments/accounts or vice versa, unless the following exceptions apply:

---

[1] It is noted that some PU roles (Testers, ***the relevant team*** operational PU roles, [REDACTION] for example) are sometimes required to do this as part of their role and therefore will sometimes be exempt; however, such activity must still be authorised by a formal test plan and/or operational business case as appropriate and the number of people in such roles must be kept to the least amount possible. Test plans and business cases must provide time bound access constraints for such roles. It is the responsibility of each individual PU to assure themselves that such authorisation is in place through relevant Line Managers and that their access privileges are disabled when no longer required.

i. If you have been granted a 'core' account, the ability to access both 'live' and 'test' environments using your core account is acknowledged and permitted. However, you must ensure that you only use your core account for authorised tasks;

ii. If you are required to use ***the relevant system*** for your PU role access (which could be accessed using your credentials for ***the relevant account*** depending on how you have been given access to safe(s)), then you must only initiate onward (transparent) connections using stored accounts available in the safe(s) appropriate to the target environment. For example, ***the relevant account*** available in safe(s) must only be used to access ***the relevant account*** environments respectively

l. Be granted physical access to infrastructure hardware (usually but not always in data centres) without proper authorisation supported by a valid business case;

m. Use privileged account access to perform non-privileged functions;

n Auto forward material from your PU account to any other account;

o. Connect or attempt to connect any unauthorised external devices or media (such as laptop PCs, USB sticks, smart phones or personal organisers) to any MI5 network or system, regardless of circumstances.

Public Key Infrastructure - PU Responsibilities

5 As a PU, you will be able to request a Public Key Infrastructure (PKI) certificate for use on hardware devices or software applications. Devices and software applications are referred to as Non Person Entities (NPE)

6. PUs shall note that:

a. To request an NPE certificate you must be the system owner (or delegated owner) and an existing PKI subscriber Requests must be made using your user account (not your privileged account)

b. You must only use NPE certificates within the environment/system it was issued from and for its intended use E.g. ***The relevant system*** certificates must only be used within ***the relevant system***.

c. Any passwords/passphrases used to access key material must be defined and managed within ***the relevant system***. You must protect and secure keys and credentials in accordance with the MI5 code of practice, MI5 policies and procedures and the Certificate Practice Statement (all available on ***the intranet***).

d You are responsible for the renewal of any NPE certificates you request and must identify a suitable secondary nominated contact and a replacement contact should you move or leave your post. You must notify the certificate manager of any changes to the nominated contacts.

Methods of enforcement of these PU SyOPs

7 PU roles, responsibilities and access controls may apply at infrastructure, system or application level PUs are to be assigned with accounts and passwords aligned to the security requirements of each system or application and in accordance with Cyber Security Technical Policy produced by ***the relevant team*** and/or specific ***the relevant team*** local policy where there are specific and authorised operational requirements.

8 The full requirements of the Policy for Privileged User (PU) and Enhanced Standard User IT Accounts (Version 3.0) must be implemented

Compliance with these PU SyOPs - Protective Monitoring

9. MI5 reserves the right to monitor all usage of its IT systems by individuals in order to identify instances of misconduct, to support incident response and/or investigations.

10 Misconduct is defined as conduct prejudicial to the interests of MI5 and/or failure to comply with official instructions. Any misconduct may result in formal warnings recorded on your vetting file and/or disciplinary action up to and including dismissal. See Manual of General Conditions of Service (MGCS) Section 81 (available on ***the intranet***).

11 Line Managers have a duty to report matters which may constitute misconduct to ***the relevant team***, however all users should consider it their duty to report incidents as necessary either to their Line Manager or direct to ***the relevant team*** as appropriate

12. Audit logs will be generated and monitored for all system users including PUs. User actions must be attributable to individuals.

13. In addition to routine Protective Monitoring, spot checks will be conducted to ensure that processes and procedures remain in place and are being properly adhered to.

Security Incident Reporting

14. Any person discovering a security incident MUST report it immediately to their Line Manager or if unavailable, the IT Service Desk (or SSDO out of hours) or (for the operational business) using local ***the relevant team*** processes and procedures, taking care to note all relevant details (e.g. time, place, persons involved, equipment involved etc). In addition, all security incidents must be reported to the MI5 IT Security Officer. Incidents may include (not exhaustive):

a. All hardware or software faults encountered within live environments where a breach of security is suspected as a cause;

b. If a security breach is encountered (including any unauthorised access attempts);

c. If any form of hardware or software tampering of any kind is suspected;

d. If anti-virus checks alert that a virus is encountered (in this instance, note any messages or alerts that are displayed, shut down the terminal and do not use it again until you are informed that it is safe to do so). Where applicable, local ***the relevant team*** processes and procedures must be followed for viruses discovered in operational environments,

e. Any suspected compromise of passwords or authentication token/device;

f. Any observation of events by others that are considered to be detrimental to MI5 security

15. A relatively minor incident might develop into a more serious one if not investigated promptly and treated appropriately

16. Failure to report a security incident is a disciplinary offence. Admitting to an honest mistake will be treated more favourably than trying to cover up an incident.

17 ***The relevant team's*** Cyber Security Policy [REDACTION] – IT Security Incident Management Policy must be adhered to.

Exemptions and Waivers to these PU SyOPs

18. Requests for exemptions and/or waivers for anything covered in these SyOPs should be submitted to the ***the relevant team*** with a full business justification. ***The relevant team*** will advise the details of the process when contacted.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

Review Criteria

19. Any changes to related internal MI5 policies will result in a review of these SyOPs Otherwise, these SyOPs will be reviewed on an annual basis.

DOCUMENTCONTROL

Document History

Version	Date	Summary of Changes	Changed By
0.1	08/11/2010	Initial draft	***MI5 Official***
0.2	08/02/2011	Updated following review meeting with ***MI5 Official***	***MI5 Official***
1.0	16/02/2011	Updated following final review comments prior to issue.	***MI5 Official***
1.2	18/09/2012	Document reviewed in line with the new version of the PU Policy version 1.4	***MI5 Official***
2.0	27/9/2012	Version number to 2.0 Issued for publication	***MI5 Official***
2.1	05/12/2013	Updates to bring into line with v3.0 of PU Policy and routine annual review	***MI5 Official***
2.2	25/02/2014	Updates to v2.1 following wide business review	***MI5 Official***
3.0	01/04/2014	Version 3.0 issued for publication as latest version.	***MI5 Official***

GLOSSARY

Term	Definition
Availability	The property of information being accessible and usable upon demand by an authorised entity
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Integrity	The property of safeguarding the accuracy and completeness of information – this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later
Privileged User	In line with HMG's technical security risk assessment framework's Information Assurance Standard No 1 (IAS1) definition, a Privileged User (PU) is a registered user or account holder who manages the applications, services, equipment and security defences within the IT enterprise. MI5's PU Policy also includes those account holders who develop and test. PUs can usually not be constrained in the same way as a Normal (Standard) User and as such are represented as a separate threat actor type. MI5 considers the security risks from PUs as part of the output of HMG's mandated IAS1 technical security risk assessment. For a more business focussed and contextualised assessment, MI5 further applies the security risk assessment method described in Annex A of the PU Policy to assess a PUs level of privilege using 5 criteria (Technology, Ability, Scope, Protective Marking, Criticality) so that they can be categorised as either an;

	- Enhanced Standard User; - Standard Privileged User; - Enhanced Privileged User.	
	Risk	The potential that a given threat will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to the organisation.
	Risk Management	Process of coordinating activities to direct and control an organisation with regard to risk
	Risk Tolerance	Risk tolerance is closely related to risk appetite, whereas appetite refers to risk at the corporate level, risk tolerance allows for variations in the amount of risk an organisation is prepared to accept for a particular project or programme.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

DECLARATION

You must sign these SyOPs on ***the relevant site*** agreeing to the terms and requirements detailed in these PU SyOPs (Version 3.0) If you are not able to e-sign these SyOPs on ***the relevant site***. because you do not have access then you must complete the declaration below
The declaration must be completed and returned to ***the relevant team***, ***the relevant team*** PUs and ***the relevant team*** for ***the relevant team*** PUs.

A Privileged User account cannot be issued until this form has been received by the ***the relevant team*** along with a completed PU Account Request Form.

Declaration
I have attended all relevant MI5 security and awareness briefings for PUs with access to MI5 IT systems and have full DV clearance.

I have read these PU SyOPs and understand my responsibilities as detailed within them.

I undertake to observe these SyOPs and take all reasonable precautions to ensure that I do not breach the security requirements detailed therein

I will inform my Line Manager, the ***the relevant team*** and IT Service Desk (***the relevant team***) or follow local ***the relevant team*** or ***the relevant site*** team processes and procedures when I no longer need PU access for specific systems.

I understand that if I fail to observe these SyOPs, I may be subject to disciplinary action.

Name: ..... Pass (***the relevant site***) No: .....

Signature: ..... Date .....