DISCOVER: [redacted]
OCTOBER 2016

Privileged Users Policy

I. Introduction

1 “Privileged Users” (PUs) for the purposes of this policy are those individuals who have IT system privileges that enable them to by-pass some or all of the controls that govern the access and activity of normal users. The extent of additional privilege ranges from those who have very limited additional privilege to execute specific tasks, those with additional privileges within an application, through to those with full control or “system admin” or “root” accounts.

2 Existing PUs who have gone through the previous process will be deemed to have the level of privilege required by their current post. If they change post, responsibilities or duties, then a further PU application following this process must be submitted. This policy applies to new systems; it is also to be applied to legacy systems unless an exemption is agreed with the security accreditor.

3 There are two categories of Privileged User: PU Function and PU Data. This categorisation may only be used where infrastructure, supporting operating systems and processes provide comprehensive security controls. Where comprehensive controls are not present, the required PU level is PU Data (defined in Section III below). The security accreditor can provide advice if in doubt.

4 For the purposes of this policy, sensitive information can include, but not be limited to, ECI, HR, Finance, Legal or Commercial. Information Asset Owners (link to http://[redacted]

are responsible for determining what information is sensitive.

II. Principles

P 1. The PU process must focus on those privileged activities that give rise to greatest risk.

P 2. The PU process is owned by Security who are responsible for ensuring a corporate record is held of all PUs and their level of privilege. Elevated privileges must be reviewed once a month by system managers and removed as soon as the requirement for them ends. This is in line with the GIAS Information Security Policy, Chapter 2, System Manager Guidance .

P 3. All PUs must have a Developed Vetting (DV) clearance that has been granted or reviewed and accepted, by GCHQ. Suitability to retain PU status will be reviewed as part of the regular Security Appraisal process.

P 4. The number of PUs for any system must be kept to the smallest number consistent with business responsiveness and efficiency.

P 5. The level of additional privilege made available to any user must be kept to the minimum necessary to perform the functions required.

P 6. PUs who have full control (e.g. root access or administrator account) must have two separate accounts; the account with the additional privilege should follow User Account Authority naming conventions for distinguishing privileged accounts.

P 7. PUs must only use their privileged account for privileged functions. Those functions that require only normal levels of privilege must be performed with the "normal" account.

P 8. Projects, sponsors and security managers must identify the roles or posts that need elevated privileges and determine the required level of privilege according to Section III of this policy.

P 9. In some circumstances, PUs can impact the availability of operational systems. In such cases there must be a segregation of roles such that the PU cannot impact the system recovery process as well.

P 10. PU status is not for life - it will be removed with a change of post or responsibilities. If a PU or individual with normal privileges changes role, position or responsibility to one that requires additional privileges, the level of additional privilege must be assessed (see Section III) and an application for that PU level must be submitted. It must not be assumed that approval will be granted, particularly if individual circumstances have changed.

P 11. If new or different categories of sensitive information are introduced onto a system, individuals with PU Data status (defined below in Section III) for that system must be screened for the newly introduced sensitive information, if that has not already been done. PUs and sponsors must be aware that the sensitive information review may lead to privileged access to that system being withdrawn.

P 12. On moving post PU privileges will be removed. However, there may be a delay while the removal process takes place and individuals must not use previously held PU privileges during this time. A new application must be approved if PU privileges are required for subsequent posts.

III.Categories of Privileged User

5 Privileged Users are divided into two categories, Privileged User Data and Privileged User Function.

The PU definitions are:

a) **PU Data**: Privileged Users who routinely access sensitive data as a result of their PU role and may require ECI, HR, Finance, Legal or Commercial briefs if deemed applicable.

b) **PU Function**: Privileged Users who do not routinely have access to sensitive data and would either have to deliberately compromise system security, or breach the trust placed in PUs to deliberately search for sensitive data.

6 Owners and managers of Secure Access Groups are also to be considered as PUs with the level PU Function. The PU process is to be followed on change of owner or manager.

7 System Managers must consider the availability risk to their system in addition to the information risk. If a PU can prevent the normal operation of the system, segregation of duties must be enforced such that the individual cannot impact the system recovery process. Any deviation from this policy must be agreed with the Information Asset Owners whose sensitive information is on the system.

IV. Requirements for Each Category

8 Before a PU takes up their duties, the processes outlined in the following table must be completed.

Process	PU Data	PU Function
Personnel Security PU Screening	Full file review (all ECIs)	Database check
PU brief and FC300/05b signed	PU Data brief must have been completed	PU Function brief must have been completed
12 month DV review (see Para 11)	Must have been completed	Need not have been completed
Review during Security Appraisal process	Must be completed	Must be completed
Sensitive post briefing & undertakings	Must have been completed	Must have been completed
ECI, HR or finance briefings	If required by data owner	If required by data owner
COI Access	If necessary for role	If necessary for role

9 Where an individual holds a DV clearance from another vetting organisation, it must be reviewed and accepted by GCHQ before PU status may be granted. As part of that process, and in light of the individual's history, personnel security may waive all or part of the requirement for time to elapse before the DV review. Where this requirement is waived completely, the initial review and acceptance by GCHQ of the existing DV clearance effectively comprises the "12 month DV review" in the table above.

10 It is GCHQ policy to carry out a review of an individual's DV after they have spent twelve months in the Department. As an exception, Personnel Security is prepared to consider bringing the review forward to six months for PU Data, if a strong business case is presented.

11 An individual may not be granted PU Data or PU Function nor have any unsupervised access to functions requiring elevated IT privileges until the relevant process in the table above has been completed. Provided that a level of audit and accounting acceptable to the accreditor is in place, they may have closely supervised access for training purposes.

12 One of the keys to managing the information risk posed by PUs is to limit the number to the minimum required while allowing the business to operate responsively and efficiently. In order to reduce the risk to system availability where a PU has the ability to negatively impact an operational system, they must not be able to impact the recovery process. Good

life-cycle management of PUs is essential risk mitigation. The process must ensure PU status is recorded and when PUs move post, or leave the department, their elevated IT privileged accesses are removed and their record updated accordingly. Fitness to retain PU status will be included as part of the annual SAF review. A great deal of trust is placed in PUs to carry out their role in accordance with GCHQ policies and this is backed up by verification from the Accounting and Audit service.

V. Compliance

13 Chapter 2 of the GIAS Information Security Policy sets out Departmental and legal liabilities:

a) All system users are subject to this policy when using Departmental IT resources and their actions may be monitored and recorded to ensure compliance. Any identified improper or unauthorised use must be reported to line management. Significant security incidents or persistent disregard of security rules on IT facilities however discovered will be investigated by Operational IT InfoSec / Security staff. In serious cases, disciplinary action will be taken and an offender's security clearance may be restricted or withdrawn.

b) Abuse of access rights on IT systems or networks (e.g. taking unauthorised copies of documents or modifying data without authorisation) is a criminal offence under the Computer Misuse Act 1990. The unlawful disclosure of any security or intelligence information by a Civil or Crown Servant, or by a contractor working for the Department, is an offence under Section 1 of the Official Secrets Act 1989. The Department must comply with data protection legislation according to the principles of the Data Protection Act (1998) unless exemption is necessary for reasons of national security as provided under section 28 of the Act. IT system operation should also be compliant with the Human Rights Act (HRA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000.

14 GCHQ's Behaviour and Conduct policy (link to http://[redacted]

sets out the standards of behaviour expected of anyone working for or at GCHQ and the policies that must be followed, including GCHQ's rules on security. Failure to comply with this security policy may result in the incident being reported to the Security Incident Management Team for appropriate investigative and disciplinary action being initiated by your management chain. In cases of gross or repeated misconduct, this could result in dismissal. The parent organisation of contractors and integrees will be notified and will be responsible for invoking any formal disciplinary action.

Privileged Users Policy

I. Introduction

1 "Privileged Users" (PUs) for the purposes of this policy are those individuals who have IT system privileges that enable them to by-pass some or all of the controls that govern the access and activity of normal users. The extent of additional privilege ranges from those who have very limited additional privilege to execute specific tasks, those with additional privileges within an application, through to those with full control or "system admin" or "root" accounts.

2 Existing PUs who have gone through the previous process will be deemed to have the level of privilege required by their current post. If they change post, responsibilities or duties, then a further PU application following this process must be submitted. This policy applies to new systems; it is also to be applied to legacy systems unless an exemption is agreed with the security accreditor.

3 There are two categories of Privileged User: PU Function and PU Data. This categorisation may only be used where infrastructure, supporting operating systems and processes provide comprehensive security controls. Where comprehensive controls are not present, the required PU level is PU Data (defined in Section III below). The security accreditor can provide advice if in doubt.

4 For the purposes of this policy, sensitive information can include, but not be limited to, ECI, HR, Finance, Legal or Commercial. Information Asset Owners (link to http://[redacted]

are responsible for determining what information is sensitive.

II. Principles

P 1. The PU process must focus on those privileged activities that give rise to greatest risk.

P 2. The PU process is owned by Security who are responsible for ensuring a corporate record is held of all PUs and their level of privilege. Elevated privileges must be reviewed once a month by system managers and removed as soon as the requirement for them ends. This is in line with the GIAS Information Security Policy, Chapter 2, System Manager Guidance .

P 3. All PUs must have a Developed Vetting (DV) clearance that has been granted or reviewed and accepted, by GCHQ. Suitability to retain PU status will be reviewed as part of the regular Security Appraisal process.

P 4. The number of PUs for any system must be kept to the smallest number consistent with business responsiveness and efficiency.

P 5. The level of additional privilege made available to any user must be kept to the minimum necessary to perform the functions required.

P 6. PUs who have full control (e.g. root access or administrator account) must have two separate accounts; the account with the additional privilege should follow User Account Authority naming conventions for distinguishing privileged accounts.

P 7. PUs must only use their privileged account for privileged functions. Those functions that require only normal levels of privilege must be performed with the "normal" account.

P 8. Projects, sponsors and security managers must identify the roles or posts that need elevated privileges and determine the required level of privilege according to Section III of this policy.

P 9. In some circumstances, PUs can impact the availability of operational systems. In such cases there must be a segregation of roles such that the PU cannot impact the system recovery process as well.

P 10. PU status is not for life - it will be removed with a change of post or responsibilities. If a PU or individual with normal privileges changes role, position or responsibility to one that requires additional privileges, the level of additional privilege must be assessed (see Section III) and an application for that PU level must be submitted. It must not be assumed that approval will be granted, particularly if individual circumstances have changed.

P 11. If new or different categories of sensitive information are introduced onto a system, individuals with PU Data status (defined below in Section III) for that system must be screened for the newly introduced sensitive information, if that has not already been done. PUs and sponsors must be aware that the sensitive information review may lead to privileged access to that system being withdrawn.

P 12. On moving post PU privileges will be removed. However, there may be a delay while the removal process takes place and individuals must not use previously held PU privileges during this time. A new application must be approved if PU privileges are required for subsequent posts.

III.Categories of Privileged User

5 Privileged Users are divided into two categories, Privileged User Data and Privileged User Function.

The PU definitions are:

a) **PU Data**: Privileged Users who routinely access sensitive data as a result of their PU role and may require ECI, HR, Finance, Legal or Commercial briefs if deemed applicable.

b) **PU Function**: Privileged Users who do not routinely have access to sensitive data and would either have to deliberately compromise system security, or breach the trust placed in PUs to deliberately search for sensitive data.

6 Owners and managers of Secure Access Groups are also to be considered as PUs with the level PU Function. The PU process is to be followed on change of owner or manager.

7 System Managers must consider the availability risk to their system in addition to the information risk. If a PU can prevent the normal operation of the system, segregation of duties must be enforced such that the individual cannot impact the system recovery process. Any deviation from this policy must be agreed with the Information Asset Owners whose sensitive information is on the system.

IV. Requirements for Each Category

8 Before a PU takes up their duties, the processes outlined in the following table must be completed.

Process	PU Data	PU Function
Personnel Security PU Screening	Full file review (all ECIs)	Database check
PU brief and FC300/05b signed	PU Data brief must have been completed	PU Function brief must have been completed
12 month DV review (see Para 11)	Must have been completed	Need not have been completed
Review during Security Appraisal process	Must be completed	Must be completed
Sensitive post briefing & undertakings	Must have been completed	Must have been completed
ECI, HR or finance briefings	If required by data owner	If required by data owner
COI Access	If necessary for role	If necessary for role

9 Where an individual holds a DV clearance from another vetting organisation, it must be reviewed and accepted by GCHQ before PU status may be granted. As part of that process, and in light of the individual's history, personnel security may waive all or part of the requirement for time to elapse before the DV review. Where this requirement is waived completely, the initial review and acceptance by GCHQ of the existing DV clearance effectively comprises the "12 month DV review" in the table above.

10 It is GCHQ policy to carry out a review of an individual's DV after they have spent twelve months in the Department. As an exception, Personnel Security is prepared to consider bringing the review forward to six months for PU Data, if a strong business case is presented.

11 An individual may not be granted PU Data or PU Function nor have any unsupervised access to functions requiring elevated IT privileges until the relevant process in the table above has been completed. Provided that a level of audit and accounting acceptable to the accreditor is in place, they may have closely supervised access for training purposes.

12 One of the keys to managing the information risk posed by PUs is to limit the number to the minimum required while allowing the business to operate responsively and efficiently. In order to reduce the risk to system availability where a PU has the ability to negatively impact an operational system, they must not be able to impact the recovery process. Good

life-cycle management of PUs is essential risk mitigation. The process must ensure PU status is recorded and when PUs move post, or leave the department, their elevated IT privileged accesses are removed and their record updated accordingly. Fitness to retain PU status will be included as part of the annual SAF review. A great deal of trust is placed in PUs to carry out their role in accordance with GCHQ policies and this is backed up by verification from the Accounting and Audit service.

V. Compliance

13 Chapter 2 of the GIAS Information Security Policy sets out Departmental and legal liabilities:

a) All system users are subject to this policy when using Departmental IT resources and their actions may be monitored and recorded to ensure compliance. Any identified improper or unauthorised use must be reported to line management. Significant security incidents or persistent disregard of security rules on IT facilities however discovered will be investigated by Operational IT InfoSec / Security staff. In serious cases, disciplinary action will be taken and an offender's security clearance may be restricted or withdrawn.

b) Abuse of access rights on IT systems or networks (e.g. taking unauthorised copies of documents or modifying data without authorisation) is a criminal offence under the Computer Misuse Act 1990. The unlawful disclosure of any security or intelligence information by a Civil or Crown Servant, or by a contractor working for the Department, is an offence under Section 1 of the Official Secrets Act 1989. The Department must comply with data protection legislation according to the principles of the Data Protection Act (1998) unless exemption is necessary for reasons of national security as provided under section 28 of the Act. IT system operation should also be compliant with the Human Rights Act (HRA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000.

14 GCHQ's Behaviour and Conduct policy (link to http://[redacted]
[redacted]

sets out the standards of behaviour expected of anyone working for or at GCHQ and the policies that must be followed, including GCHQ's rules on security. Failure to comply with this security policy may result in the incident being reported to the Security Incident Management Team for appropriate investigative and disciplinary action being initiated by your management chain. In cases of gross or repeated misconduct, this could result in dismissal. The parent organisation of contractors and integrees will be notified and will be responsible for invoking any formal disciplinary action.