Document Title: POA Privileged Account Policy

Document Reference: SVM/SEC/POL/4538

CP/CWO Reference: N/A

Abstract: POA Privileged Account Policy covering Master & Sub-Master and Password Policy rules applicable to all privileged accounts.

Document Status: APPROVED

Author & Dept: Steven Browell and Fujitsu Enterprise & Cyber Security IDAM Consultants GRO

External Distribution: None

Information Classification: See section 0.9

Approval Authorities:

Name	Role	
Steven Browell	Management Consultant & CISO	See Dimensions for record

0 Document Control

0.1 Table of Contents

TABLES

0.2 Document History

Only integer versions are authorised for development.

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CWO, CP, CCN or PEAK Reference
0.1	14-JUL-2022	First version in POA template	Include if known
0.2	20-JUL-2022	Final draft for approval	
0.3	27-JUL-2022	Final version for approval including feedback comments	
1.0	28-JUL-2022	Approved version	
1.1	10-MAR-2023	Correct incorrect reference to 90 days instead of 30. Remove unclear term "User Service Account". Correct wording that set password length to be "exactly" instead of "at least". Added Appendix with Oracle user instructions. Clarified password rotation of SecOps managed accounts.	
1.2	15-MAR-2023	Updates based on reviewer feedback	
1.3	22-MAR-2023	Further updates based on reviewer feedback	
2.0	23-Mar-2023	Approval version	
2.1	30-NOV-2023	Amendment to section 4.1 to simplify PP01, retire PP02-PP06, and set PP08-09 to Recommended. Added instructions on how to use LastPass to comply with policy. Various grammar amendments and pagination changes. Added DEV/APP/LLD/0028 to list of referenced documents.	
2.2	11-Jan-2024	Revisions following review.	
3.0	15-Jan-2024	Approval version	
3.1	10-Apr-2024	Update to rules on password resets. Addition of sections on TESQA and iKey Exemptions. Suspension of SMP12 and SMP13. Removed optional reviewers	
3.2	14-May-2024	Updates following review comments	
4.0	23-May-2024	Approval version	

0.3 Review Details

Review Comments by:	
Review Comments to:	Steven.browell GRO + POA Document Management

Mandatory Review	
Role	**Name**
POA Security Governance Manager	Chris Stevens
POA Security Operations Manager	Farzin Denbali
POA Security Architect	Dave Haywood; Davinder Jandu

Optional Review	
Role	**Name**

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**

0.4 Associated Documents (Internal & External)

References should normally refer to the latest approved version in Dimensions; only refer to a specific version if necessary.

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 *(DO NOT REMOVE)*	See note above	See note above	POA Generic Document Template	Dimensions
PGM/DCM/ION/0001 *(DO NOT REMOVE)*			POA Document Reviewers/Approvers Role Matrix	Dimensions
Ask Security	Latest		Europe Security Master Policy	Ask Security
Ask Security	Latest		Europe Security Policy Manual	Ask Security
Ask Security	Latest		Security Toolkit – Systems Access and Passwords	Ask Security
SVM/SEC/PRO/4537	Latest		POA Privileged Account Release Procedure	Dimensions
DEV/APP/LLD/0028	Latest		Active Directory Low Level Design for HNG-X	Dimensions

0.5 Abbreviations

Abbreviation	Definition
AD	Active Directory
CIS	Center for Internet Security
ECS	Enterprise and Cyber Security
EBMS	Europe Business Management System
JML	Joiner Mover Leaver
PAM	Privileged Access Management
POA	Post Office Account
SPM	Security Policy Management
SMP	Security Master Policy

0.6 Glossary

Term	Definition
Alphabetical order please	

0.7 Changes Expected

Changes

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, while every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE).

1 Introduction

A privileged account has additional abilities to a "standard" user account. Privileged accounts may be machine accounts or accounts allocated to individual development or support staff. Privileges may include access rights to operating systems or to application software and databases.

System privileges and levels of access required to perform management functions are higher than those assigned to standard users. Therefore, the allocation and use of privileges is restricted and controlled, and the principle of least privilege is used. The principle of least privilege refers to the concept and practice of restricting access rights to only those resources required to perform the authorised activities. Individuals should not be granted unnecessary privileges.

The purpose of this Privileged Account Policy is to set a standard for creating, protecting, and managing all privileged accounts within Post Office Account (POA).

The privileged account types on the POA are as follows:

- **Personal Privileged** – Individual privileged accounts
- **Shared Privileged** – Privileged account used by more than one individual
- **Local Administrator** – Local host admin access accounts
- **Domain Administrator** – Domain admin access accounts
- **Database Administrator** – Database admin accounts
- **Network Administrator** – Network admin accounts
- **Application Administrator** – Admin accounts for specific applications or appliances
- **Built-in Administrator** – Vendor default admin accounts that must be retained
- **Service Accounts** – Local or domain non-interactive system accounts (including MSAD Service Accounts)

Note: Some accounts may meet the definition of more than one type e.g. a Built-in Administrator account that is also Shared Privileged as it is needed by a team that manage the applicable system.

The Master Policy rules set a vision for POA. If POA deployed Privileged Access Management (PAM) toolsets, then these rules would be integral to that solution. POA does not have such a toolset, so some of the Master Policy rules are challenging, or impractical to achieve. Every effort must be made when changes are implemented in any parts of the solutions on POA to move towards compliance with the Master Policy. Compliance with the Master Policy is considered highly desirable for all privileged accounts in use on POA.

The Sub-Master Policy rules, however, are deemed to be achievable within the POA solutions deployed despite the absence of PAM toolsets. Although they may incur additional manual processes they should be operated and complied with. Complying with the Sub-Master Policy is mandatory on POA and ensures a significant alignment with the Master Policy.

The Password Policy is referred to in both the Master and Sub-Master Policies and compliance is considered mandatory for all privileged accounts within POA.

POA SecOps maintain a Privileged Account Register of all privileged accounts which includes their compliance to the Master Policy, Sub-Master Policy and Password Policy. Exceptions are recorded on the Privileged Account Register along with the reason for non-compliance. This allows POA SecOps to decide if it is necessary to challenge the non-compliance or accept the reason as appropriate and thereby agree to the exception to compliance.

2 Master Policy (information only)

The Master Policy rules set a vision for POA. If POA deployed Privileged Access Management (PAM) toolsets, then these rules would be integral to that solution. POA does not have such a toolset, so some of the Master Policy rules are challenging, or impractical to achieve. Every effort must be made when changes are implemented in any parts of the solutions on POA to move towards compliance with the Master Policy. The Master Policy is shown in Appendix A for reference only.

3 Sub-Master Policy

The Sub-Master Policy rules are deemed to be achievable within the POA solutions deployed despite the absence of PAM toolsets. Although they may incur additional manual processes they must be operated and complied with. Complying with the Sub-Master Policy is mandatory on POA and ensures a significant alignment to the Master Policy.

3.1 Sub-Master Policy Rules

The table below details the Sub-Master Policy references and associated policy rules. Items marked with an asterisk in the Mandatory column are not applicable to Service Accounts.

All privileged accounts that are held on the POA SecOps Register record the compliance to these policy references.

Sub-Master Policy Ref	Sub-Master Policy Rule	Mandatory
SMP01	The privileged account has a clearly stated named owner	Yes
SMP02	The privileged account owner must ensure the password complies with the Password Policy rules	Yes
SMP03	Privileged accounts must be created, changed, and disabled following the POA JML processes	Yes
SMP04	All privileged accounts must have their access clearly defined within the POA JML forms so that access levels are documented	Yes
SMP05	Shared privileged accounts must be stated on the POA JML forms so that users requiring access to use them can be recorded centrally	Yes
SMP06	All privileged accounts must be recorded on the POA SecOps Privileged Account Register, so they are centrally recorded and subject to the POA SecOps periodic verification processes	Yes
SMP07	The privileged account, if a Service Account, must not permit human interactive logon	Yes
SMP08	Privileged account owners must respond to verification process checks every 90 days - and failure to respond within the designated time stated on the verification will mean that the privileged account will be disabled or will have its access removed	Yes
SMP09	Privileged accounts that are used less than once a week are to be handed over to POA SecOps for central ownership and management under the Privileged Account Release Procedure	Yes*
SMP10	Superseded by SMP11. Ignore	
SMP11	Changes made to the Live system using a privileged account must be documented under Change Control, be part of a defined service obligation, or be documented by a formally operated processes such as APPSUP	Yes

Sub-Master Policy Ref	Sub-Master Policy Rule	Mandatory
~~SMP12~~	~~Whenever practical, changes made to the Live system using a privileged account should be witnessed by another Fujitsu user and the witness name must be recorded in a Fujitsu service management toolset (TfSNow or Peak)~~	~~No*~~
~~SMP13~~	~~When using a privileged account to make changes to the Live system, the actions being performed must, where possible, be logged to a local system log that is also stored centrally and also stored in the Audit Archive~~	~~No~~
SMP14	The owner of privileged accounts that are shared must always record who has access to use the privileged account (it must be provided to POA SecOps when requested)	Yes
SMP15	The owner of privileged accounts that are shared must maintain records of who has used the accounts and when it was used (it must be provided to POA SecOps when requested)	Yes
SMP16	Privileged account credentials must be securely stored (e.g. in a Password Manager/encrypted file) or not stored at all	Yes
SMP17	Privileged accounts must require the use of Multi-Factor Authentication	Yes*

Table 1 – Sub-Master Policy Rules

April 2024 – SMP12 and SMP13 have been suspended due to operational impracticalities to achieve in the absence of tooling.

4 Password Policy

The Password Policy is referred to in both the Master and Sub-Master Policies and compliance is mandatory for all privileged accounts in use on POA.

4.1 Password Policy Rules

The table below details the Password Policy references and associated policy rules.

All privileged accounts that are held on the POA SecOps Register record the compliance to these policy references.

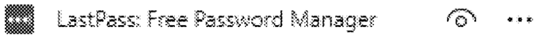
Password Policy Ref	Password Policy Rule	Mandatory
PP01	IRRELEVANT	Yes See Note 1
PP02-PP06		
PP07		Yes See Note 1
PP08		Recommended
PP09		Recommended

Table 2 – Password Policy Rules

Note 1 – The corporate password generating tool (LastPass), which is deployed to all corporate laptops, provides a Generator that can be used to create strong passwords. To generate a strong password, open your browser and select the LastPass icon near the navigation bar,

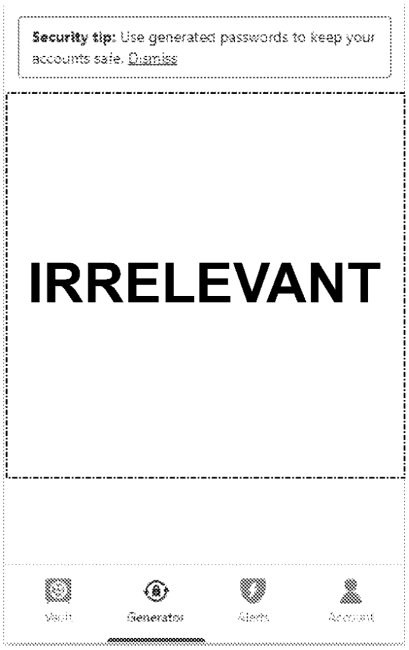
Or from the drop-down list of extensions

, select the LastPass: Free Password Manager entry…



LastPass: Free Password Manager

This presents a screen with an option Generator at the bottom:



Security tip: Use generated passwords to keep your accounts safe. Dismiss

IRRELEVANT

IRRELEVANT

When the password appears, compare it to the PP01 rules above. If the password is compliant, you can copy it and use it. If it is not compliant, click on refresh and check the updated password shown.

You can also store the password in your LastPass Vault.

Whilst it is acknowledged that current advice for human passwords is that they are not rotated regularly (i.e. do not expire), that they do not have these types of complexity rules, and that longer passwords are more secure than complex passwords and more importantly are easier to remember, there are constraints within the POA deployed solutions that would make this difficult to deploy unilaterally.

See https://pages.nist.gov/800-63-3/sp800-63b.html#appA for additional information.

It is recommended, particularly for human accounts, that long passwords are used.

4.2 MSAD Account Password Policy

POA Password Policy is managed by POA SecOps and the following minimum criteria, extracted from DEV/APP/LLD/0028 Section 13 Group Policy, should be followed where the system allows:

Policy	Standard Account Minimum Contractual Setting	Standard Account Preferred Setting	Service Account Preferred Setting
Enforce password history	IRRELEVANT		
Maximum password age [1]			
Minimum password age [2]			
Minimum password length			
Password must meet complexity requirements			
Store passwords using reversible encryption			

Table 3 – MSAD Account Password Policy

[1] Maximum password age and expiration notification: Maximum password age must be always higher than minimum password age unless it is set to 0 (password never expires).

[2] Minimum password age: To avoid potential password sync conflicts and prevent users from bypassing the password history policy.

Password expiration: Due to Service continuity reasons Service Accounts passwords are set to never expire.

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	IRRELEVANT
Account lockout threshold	
Reset account lockout counter after	

Table 4 – Account Policies/Account Lockout Policy

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	IRRELEVANT
Maximum lifetime for service ticket	
Maximum lifetime for user ticket	
Maximum lifetime for user ticket renewal	
Maximum tolerance for computer clock synchronization	

Table 5 – Account Policies/Kerberos Policy

Interactive Logon

Policy	Setting
Interactive logon: Prompt user to change password before expiration	IRRELEVANT

Table 6 – Interactive Logon

4.3 Account Ownership

Where possible, privileged accounts must be centrally managed by POA SecOps. Centralising management of such credentials is a step forward to limit the potential for misuse of privileged accounts. This should include accounts that do not comply with Sub-Master Policy rule 9 (SMP09). Access to these centrally managed accounts will then follow the POA Privileged Account Release Procedure (SVM/SDM/PRO/4537).

4.4 Account Lifecycle

Privileged accounts must be created and disabled through the Joiners, Movers and Leavers (JML) process for POA. All account requests must follow the POA JML process.

4.5 Guidance on Selecting Strong Passwords

4.5.1 Risks with weak Passwords

If someone else obtains your passwords, they may use your account to perform actions or to commit crimes and all transactions they perform will be performed in your name. If it cannot be proven that anyone else was using your account, or it is proven that you failed to adequately protect your password, you may be held accountable for all actions performed using your account and for any damage caused by that use.

The longer and more complex a password, the safer it is against hacking attacks. However, it is also more difficult to remember, especially when it must be changed frequently. Choosing a secure password which can be remembered easily is therefore challenging.

4.5.2 Selecting a Secure Password

Selecting a secure password is important. The password is used by the computer to verify the user, so pick a password that cannot be guessed by others.

Cyber criminals use sophisticated tools and common password databases that can rapidly decipher passwords. The top reasons people gain unauthorised access to a password protected system are:

- They guessed someone's password (often because they found it on a piece of paper next to the victim's computer).
- They saw the person type the password in.
- They use software programs that are very good at guessing common passwords.
- The password was intercepted between the user and the application due to lack of encryption at the network layer.

The following guidelines should guard against someone finding out your password and using your account without your permission:

- Make your password as long as possible. The longer it is, the more difficult it will be to attack the password with a brute-force search. Fujitsu application and system support for minimum and maximum password lengths varies and may constrain the password that may be set. For privileged account passwords POA mandates a 16 character minimum length.

- Use as many different characters as possible when forming your password. Use numbers, punctuation characters and mixed upper and lower-case letters. Choosing characters from the largest possible alphabet will make your password more secure by requiring more effort by someone to guess it correctly.
- Do not use personal information in your password that someone else is likely to be able to figure out. Things like your name, phone number, and address are to be avoided. Even names of acquaintances, pets, sports teams, hobbies and family names should not be used.
- Do not use words, geographical names, or biographical names that are listed in standard dictionaries.
- Never use a password that is the same as your account number.
- Do not use passwords that are easy to spot while you're typing them in. Passwords like 12345, qwerty (i.e., all keys right next to each other), or nnnnnn should be avoided.

4.5.3 Difficulties selecting a Secure Password

If you are having difficulty picking a good password, some good methods include:

- Use a long phrase you can easily remember and apply different capitalisation and special characters. Some examples:
  - "Paris is my kind of place to eat cheese" could be "Paris-is.my-kind.of-place.to-eat.cheese"
  - "My computer is 5 years old and slow" could be "MY ComputeR IS FivE YearS OlD AnD SloW"
- Use the first letter of each word in a phrase you can easily remember. Some examples:
  - "Paris is my kind of place to eat cheese" would be "Pimkop2ec"
  - "My computer is 5 years old and slow" would be "Mci5yo&s"
  - "I am 28 and Madonna is a star" would be "Ia28&Mia*"
- Use a phrase instead of a word:
  - Todayis32degrees!
  - Coffee&twobiscuits4me
- Join two (or more) completely unrelated words with symbols:
  - Yellow%thoughtful
  - teabags$$Advocate
  - airline*(punctual)

4.5.4 Things to Avoid as Passwords

Here are some guidelines of what <u>not</u> to include in your password:

- Names, including any part of your name, your spouse's name, your parent's or children's name, your pet's name
- Names of your boss, close friends or co-workers, or favourite fantasy characters
- The name of the operating system you're using, or the hostname of your computer
- Other information that is easily obtained about you, including phone numbers, birth dates, car licence plates etc
- Words such as wizard, guru, Gandalf etc – although this is ok if combined with many other words to create a longer phrase

- Any username on the computer in any form (as is, capitalised, etc.)
- A dictionary word, in any language– although this is ok if combined with many other words to create a longer phrase
- A place name– although this is ok if combined with many other words to create a longer phrase
- Passwords of all the same letter (typically prevented by system policy)
- Simple patterns on the keyboard, like qwerty (typically prevented by system policy)
- Any of the above spelled backwards (typically prevented by system policy)
- Any of the above followed or pre-pended by a single digit
- Avoid simple things like words spelled backwards, or common substitutions like '3' for 'e' etc.

5 Password Handling and Protection

5.1 MSAD Accounts

5.1.1 Initial Password Allocation

The following requirements are to be met when creating or supplying a password to a user for the first time or after a password has been reset:

- Users must be provided initially with a secure temporary password which they are required to change at first login.
- Temporary passwords provided to a user must be unique (i.e. not the same password supplied to every user).
- Temporary passwords must meet password complexity requirements in the previous section.
- Temporary passwords must be provided to users in a secure manner. The use of third parties or unprotected (clear text) messages are to be avoided.

5.1.2 Password Resets

When a user requests their password to be reset:

- Support staff are required to validate the identity of the user.
- Users should be provided initially with a secure temporary password, which they are required to change at first login.
- Where phone calls to help desk agents are involved, identification of the user is mandatory, for example, use of the users' UK personnel number.
- Where the user account is a privileged account, a TfSNow ticket must be raised to record the request and action taken.

5.2 Storage of Privileged Passwords

Passwords for any privileged account must be stored in a Fujitsu approved secure storage system or not stored at all (MP15 / SMP16).

Access controls within the password storage system are to be implemented in a manner which ensures access to passwords is only possible to defined personnel for legitimate business reasons.

5.3 Network Transmission

The passwords for data that has been shared should not be transmitted via the same medium. It is much more difficult for an adversary to combine data from two sources (e.g. Teams and Email) to decrypt the data.

Using public key cryptography (i.e. gpg, pgp) removes the secure key exchange problem for symmetric keys. The first recommendation should be to use asymmetric keys if possible, followed by the secure exchange of symmetric keys if asymmetric is not possible.

5.4 Built-in Administrator Accounts

Built-in Administrator accounts should be disabled and POA defined accounts should be setup instead wherever possible.

Default vendor passwords for Built-in Administrator accounts must be changed during the installation of applications, systems and network devices wherever possible.

Built-in Administrator accounts must be handed over to POA SecOps for central ownership and management under the Privileged Account Release Procedure wherever possible.

5.5 Oracle Privileged Access Management

To enhance auditability, POA Oracle users are required to work as described in Appendix B.

Auditing relies on the UNIX /var/log/secure syslog file and the Oracle audit. Sudo commands are logged to /var/log/secure and Oracle commands are logged to the audit destination as defined by the Oracle database audit parameter audit_file_dest.

Users accessing Oracle from their own user account without escalating to SYSDBA are logged in the SYS.AUD$ table as their user id. Users accessing Oracle via sudo using another account (oracle or grid for example) have their session logged as the target account. In this instance a combined review of the /var/log/audit and Oracle audit is required to correlate user activity.

Refer to Appendix B for further policy information.

5.6 Changing Passwords for Centrally Managed Accounts

For privileged accounts managed by SecOps, PP08 (30-day password rotation) does not apply as the passwords are rotated on each use as per the POA Privileged Account Release Procedure [SVM/SEC/PRO/4537]

Rotation of the password is dependent on access levels. POA SecOps will use one of the following methods to securely rotate passwords.

- Where POA SecOps can access the infrastructure/applications/devices, they will rotate the password themselves in a controlled manner that is tracked with date/time stamp.
- Where POA SecOps do not have access, they will initiate password rotation by means of an incident ticket reference, screen share with an Individual Privileged user and a "baton pass" approach will be used where the user gives POA SecOps control of the session so they can input the new password known only to them.
- Where none of the above apply, then POA SecOps will initiate password rotation by means of an incident ticket reference, screen share with an Individual Privileged user, and then a verbal communication of the new password which will be witnessed as being typed in. There will be no written password confirmation making it extremely unlikely that the Individual Privileged user will remember the complex password used. Any verbal communication should also ensure it has not been recorded.

Once the password is successfully rotated, this is then under the control and management of POA SecOps.

5.7 SecOps Managed Privileged Account Release Policy

Requesting and releasing of POA SecOps centrally controlled privileged account details must follow the POA Privileged Account Release Procedure (SVM/SDM/PRO/4537). This will ensure adherence to the following release process rules:

Release Process Ref	Release Process Rule	Mandatory
RP01	Requests for privileged accounts are made via the agreed request process (e.g. TfSNow)	Yes
RP02	Requests for multiple privileged accounts are made separately and following the agreed request process (e.g. TfSNow)	Yes
RP03	Requests for privileged accounts are made with documented justifications which must include timescales over which the credentials will be needed (e.g. within the TfSNow ticket)	Yes
RP04	Requests for privileged accounts are approved by the designated authorising party(ies) as recorded in the Register. A requestor cannot self-authorise	Yes
RP05	Approvals for release of privileged accounts are documented (e.g. within the TfSNow ticket)	Yes
RP06	Privileged accounts are only made available for the approved time period	Yes
RP07	The password is changed (as per the password policy rules) when the privileged account is returned, or the end time period is reached	Yes
RP08	The details of the request, approval, time period, and password change actions are recorded in a central log for at least 12 months	Yes

Table 7 – SecOps Managed Privileged Account Release Policy

5.8 Password Management Requirements

Credentials assigned to an individual must be treated as confidential information. No employee is allowed to handover their own account credentials or any credentials released to them under the process described in Section 5.7 to another person, including IT staff, administrators, superiors, other colleagues, friends, or family members. Shared Privileged accounts managed by local POA teams must comply with the Sub-Master and Password Policies and must be administered as stated in the section above "Storage of Privileged Passwords".

If someone demands your password or you suspect someone knows your password or is using your account, immediately change the compromised credential and contact POA SecOps to raise a Security Incident.

5.9 Protecting Passwords

At a minimum the following steps are to be taken to protect passwords:

- Users must be able to change non-centrally managed passwords themselves.
- Avoid typing your password in the presence of others.
- Passwords must be kept securely and must not be accessible for anyone else (e.g. programmable keys on the keyboard or written on paper and placed under the keyboard).
    - *If you have difficulty in remembering your password, store it in a password safe or encrypted file.*

- Passwords must not be stored in any applications, system folders or Cookies
    - *If you have difficulty in remembering your password, store it in a password safe or encrypted file.*
- "Remember password" or "Save automatically" features of applications should be avoided
    - *Web browser password managers can be used provided the "synchronise passwords" feature is avoided so the passwords are only stored locally*
- If possible, don't use the same password to access multiple company systems unless this is controlled by a Fujitsu approved Single Sign On (SSO) solution.

5.10 TESQA Accounts

The creation of TESQA accounts, and the re-enablement of existing TESQA accounts, must be done following the POA JML process and must not be performed without prior approval from POA SecOps.

5.11 iKey Exemptions

Users are required to use an MFA token (iKey) to access the support terminal servers (SSNs) unless they have been granted membership of the IRRELEVANT

It is recognised that iKeys can exhibit faults thereby rendering authentication impossible. The IRRELEVANT IRRELEVANT group on IRRELEVANT and IRRELEVANT allows users to access POA systems without using MFA. Only users in this group will be able to logon without using iKey MFA.

All other Live system SSNs always enforce the use of MFA using an iKey.

A user account IRRELEVANT exists as a permanent member of the IRRELEVANT group. This is a break glass account and must be requested under the process described in Section 5.7.

Use of the IRRELEVANT will only be released to a member of the POA NT support team.

5.11.1 Emergency iKey Exemption Process

In the event of an issue with a support user's MFA token or the MFA solution, action will be required to add the support user's account to the MSAD\ikey-exemptou-users group so that they can logon to the Live systems via the iKey exempt SSNs. This emergency iKey exemption will then allow them to login with their own credentials without MFA. This MUST only be done after a TfSNow Incident has been raised AND pre-approved by SecOps following the process below Once the MFA issue is resolved, the user will be removed from the group to restore mandatory MFA authentication.

This process describes the following roles and how they must work together:

- Support User – is the POA support specialist that needs to logon to perform a task
- NT Support User – is a POA Windows skilled support specialist
- SecOps – the POA Security team that approve any exemptions to the mandatory use of iKey MFA authentication

The process below starts when a Support User experiences MFA issues and cannot proceed to logon to the POA environment with their iKey.

1. The Support User raises a TfSNow Incident to record that they have an MFA issue and routes it to SecOps
    a. Note: If the Support User does not have access to create the TfSNow Incident themselves then they should contact the POA Major Account Controller (MAC) team at mac.uk GRO
2. SecOps review the Incident to decide if the Support User's account should be added to the IRRELEVANT group

   a. If SecOps do not provide approval, then the process ends, or reverts to the start for re-consideration
   b. If SecOps provide approval, then they will update the TfSNow Incident accordingly and route the TfSNow Incident to the NT Support User

3. The NT Support User adds the Support User account approved by SecOps (that has the MFA issues) to the IRRELEVANT group
   a. If a NT Support User is also unable to use iKey MFA then they can follow the POA SVM/SEC/PRO/4537 - POA Privileged Account Release Procedure to request the IRRELEVANT IRRELEVANT" account credentials
   b. Once approved, SecOps release the credentials to the NT Support User
   c. The "NT Support Access" logs on to a SSN in the iKey exempt OU
   d. The NT Support User then adds their own NT Support User account and the Support User account (when prompted via User Access Control (UAC) to IRRELEVANT IRRELEVANT group
      i. **NOTE – the "IRRELEVANT" user account is only to be used for this task. All other actions are to be taken using the Support User's own credentials**
   e. The NT Support User signs out as "IRRELEVANT
   f. The Support User and the NT Support User are then able to log on to a SSN in the iKey exempt OU with their own – now MFA exempt - credentials
   g. The NT Support User checks the IRRELEVANT break glass account back in with SecOps as described in Section 4 "Check-In Procedure" - of SVM/SEC/PRO/4537 - POA Privileged Account Release Procedure
   h. SecOps confirm the IRRELEVANT group has the correct entries, that the TfSNow ticket is correctly updated, and completes the password reset for IRRELEVANT IRRELEVANT

4. The NT Support User updates the TfSNow Incident to note the action taken
5. Support User logs on via an SSN in the iKey exempt OU and continues their required tasks
6. SecOps will monitor the MFA issue until resolved
   a. If the underlying MFA issue has been resolved
      i. SecOps will ensure the Support User and NT Support User accounts are removed from the IRRELEVANT group
   b. If the underlying MFA issue has not been resolved
      i. SecOps will consider an extended time-bound continuation of the MFA exemption for the Support User account to remain in the IRRELEVANT IRRELEVANT group. The TfSNow Incident will be updated accordingly by SecOps
      ii. If SecOps approve the continuation, no further action is required, and the Support User account remains in the IRRELEVANT group
      iii. If SecOps reject the continuation, then SecOps will notify the NT Support User to remove the Support User account from the IRRELEVANT group
7. SecOps confirm the IRRELEVANT group has the correct entries and that the TfSNow ticket has appropriate updates

6 Service Accounts

6.1 Service Account creation

Service Accounts must be requested via the POA JML process so that they are correctly approved and recorded on the Privileged Account Register maintained by POA SecOps. Where they are generated automatically by systems, POA SecOps must be notified of the Service Accounts created so they can be recorded.

The platform and/or service owner should complete the relevant JML form that is available from POA SecOps or from the POA intranet page. There are several fields that must be completed. These will be checked before approval is granted for the new service account to be created at which point POA SecOps will raise tickets in either TfSNow or Peak for the relevant system owner to create the approved service account.

POA Integration may also be requested to create an updated baseline containing the service account details (account name and password) which would then go to POA Release Management for the planning and deployment of the new service account to be scheduled into a release specific for each environment.

All service account requests must be based on the principle of least privilege ensuring the accounts created have only the privileges required. Using unique service accounts for each task is a stronger security practice and adheres to service account isolation. By doing this, it prevents increased privileges on any one account which can happen when a service account is used for multiple services, resulting in merged privileges which then violates the principle of least privilege. By adhering to the principle of least privilege and service account isolation, this helps to reduce the attack surface and lateral movement between services should an account be compromised.

6.2 Service Account password expiry

Service Account passwords are set not to expire by design. This is typically because if a service account password expires, the service the account supports may cease to work.

If a Service Account password is compromised in any way, it should be changed.

6.3 Requesting a Service Account password change

If there is a need to change a service account password, the platform/service owner who requires the Service Account password to be changed should contact POA SecOps (email: cspoa.security GRO) with details of the service account. Details to include:

- What service(s) the account supports
- The Service Account name
- What platforms and/or domain account the service account is to be deployed to
- Why the service account needs to be changed

6.4 Deleting/Disabling a Service Account

If a Service Account is no longer in use, it should be disabled. The POA JML process should be followed using a “Leaver” notification.

POA SecOps will then manage the process of the controlled removal of the service account.

Appendix A – Master Policy Rules (information only)

The Master Policy rules set a vision for POA. If POA deployed Privileged Access Management (PAM) toolsets, then these rules would be integral to that solution. POA does not have such a toolset, so some of the Master Policy rules are challenging, or impractical to achieve. Every effort must be made when changes are implemented in any parts of the solutions on POA to move towards compliance with the Master Policy. The Master Policy is shown in Appendix A for reference only.

Compliance with the Master Policy is considered highly desirable for all privileged accounts in use on POA.

A.1 Master Policy Rules

The table below details the Master Policy references and associated policy rules. Items marked with an asterisk in the Highly Desirable column are not applicable to Service Accounts.

All privileged accounts that are held on the POA SecOps Register record the compliance to these policy references. Any non-compliant responses show the reason for the non-compliance and once approved by POA SecOps, be deemed to be approved exceptions to the policy.

Master Policy Ref	Master Policy Rule	Highly Desirable
MP01	The privileged account has a clearly stated named owner	Yes
MP02	The privileged account is held in a central tool and is only available on receipt of an authorised request	Yes*
MP03	The privileged account password is not known to potential users until it is needed and provided by the central tool on receipt of an authorised request	Yes*
MP04	The privileged account, if a Service Account, must not permit human interactive logon	Yes
MP05	The privileged account password complies with the Password Policy rules	Yes
MP06	Superseded by MP08. Ignore	
MP07	Superseded by MP08. Ignore	
MP08	The timestamp for the periods of time over which a privileged account is used are recorded and stored for at least 12 months	Yes
MP09	The actions taken by the privileged account are recorded and stored on the local systems for at least 1 months	Yes
MP10	The actions taken by the privileged account are recorded and stored centrally for at least 12 months	Yes
MP11	Whenever practical, the actions taken by the privileged account are witnessed by another entity (e.g. user) the details of the entity that witnessed the actions are stored where they can be queried for up to 12 months	Yes*
MP12	The privileged account can only be used by one person at a time	Yes*
MP13	The privileged account password must be changed after each use	Yes*
MP14	There must be a documented list of all parties/systems that have authorised access to use the privileged account	Yes
MP15	Privileged account credentials must be securely stored (e.g. in a Password Manager/encrypted file) or not stored at all	Yes*
MP16	Privileged accounts must require the use of Multi-Factor Authentication	Yes*

Table 8 – Master Policy Rules

Appendix B – Oracle Privileged Access Management Ways of working

B.1 Standard Operating Procedure (SOP)

POA Oracle database access must comply with the following directives:

- Users use their own user account to access the databases via sqlplus
- All sudo access must be initiated from the users own MSAD account on the server hosting the database to be accessed
- Users may sudo to the grid user but may only access the ASM SID database instance as SYSASM
- sudo must not be used to open an interactive shell to either the oracle or grid users (opening a unix shell via sudo as the oracle or grid users means subsequent commands (sqlplus for example) are attributed to the sudo user rather than the original user. Running a command as oracle or grid users via sudo is logged to /var/log/secure and is attributable to the original user.)

B.2 Exceptional access to Oracle user account

Access other than that defined in the SOP above may be granted according to the following directives:

- Access outside of the SOP requires authorisation from POA SecOps
- A TfSNow incident must be raised to record the reason for the access and the duration
- The TfSNow incident should be raised in advance of the access but may be raised retrospectively where a live incident takes precedence
- Access must be for the minimum time required to resolve the issue
- The PuTTY session must be recorded (via the PuTTY logging mechanism) and a copy of the PuTTY session log must be attached to the TfSNow incident
- POA SecOps must be informed when the exceptional access is terminated.

B.3 Access examples

B.3.1 SOP access examples:

- Generic form to run any command as the logged in user or as the grid or oracle users:

```
<command1>[;<command N>]
```

- Access an interactive sqlplus prompt as the logged in user who is a member of the unix dba group:

```
sqlplus / as SYSDBA
```

- Run a database query as the logged in user:

```
export ORACLE_SID=BRDB1; echo 'show parameter audit' | sqlplus / as SYSDBA |
grep audit_file_dest
```

- Generic form to run any command as the grid or oracle users:

```
sudo -u <oracle|grid> -i /bin/bash -c "<command1>[;<command N>]"
```

- Examine an audit file for the oracle or grid users

```
export ORACLE_SID=BRDB1; echo 'show parameter audit' | sqlplus / as SYSDBA |
grep audit_file_dest
```

```
sudo su - oracle -c 'ls -lrt /u01/admin/BRDB/adump | tail -1'
sudo su - oracle -c 'less /u01/admin/BRDB/adump/
BRDB1_ora_22391_20221125115501575867143795.aud'

export ORACLE_SID=+ASM1; echo 'show parameter audit' | sqlplus / as SYSASM |
grep audit_file_dest
sudo su - grid -c 'less
/u01/app/11.2.0/grid/rdbms/audit/+ASM1_ora_7152_20221124104051138619143795.a
ud'
sudo su - grid -c 'ls -lrt /u01/app/11.2.0/grid/rdbms/aud | tail -1'
```

B.3.2 Exceptional access examples:

- Access a unix shell as the oracle or grid user:

```
sudo -u oracle -i

sudo -u grid -i
```

- Access an interactive sqlplus prompt as the oracle or grid users:

```
sudo -u oracle -i /bin/bash -c "export ORACLE_SID=BRDB1; sqlplus / as
SYSDBA"
sudo -u grid -i /bin/bash -c "export ORACLE_SID=+ASM1; sqlplus / as SYSASM"
sudo -u grid -i /bin/bash -c "export ORACLE_SID=+ASM1; asmcmd"
```

- Display the audit files location:

```
sudo -u oracle -i /bin/bash -c "export ORACLE_SID=BRDB1; echo 'show
parameter audit' | sqlplus / as SYSDBA | grep audit_file_dest"
sudo -u grid -i /bin/bash -c "export ORACLE_SID=+ASM1; echo 'show parameter
audit' | sqlplus / as SYSASM | grep audit_file_dest"
```

B.3.3 Not permitted examples

- Open an interactive shell as root to subsequently su to oracle or grid users:

```
sudo su -
su - <oracle|grid>
```

B.4 sudoers modifications

DES/SEC/ION/2591 describes the sudoers integration with AD via sssd. Changes are required to the sudoers AD delivery to facilitate limited user access to the grid and oracle accounts without requiring root access.

The following configuration snippet permits members of the *dba* unix group access to the *oracle* and *grid* accounts on the Oracle database servers defined in the ORACLEDBSERVERS Host_Alias to execute any command.

```
Host_Alias ORACLEBRDB =
IRRELEVANT
Host_Alias ORACLENPS =        IRRELEVANT
Host_Alias ORACLEDAT =
Host_Alias ORACLEBRSS =
%dba ORACLEBRDB,ORACLENPS,ORACLEDAT,ORACLEBRSS=(oracle,grid) NOPASSWD: ALL
```