FUJ00235007

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
External Distribution:	None
Information Classification:	See section 0.9

Approval Authorities:

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

FUJ00235007

0 Document Control

0.1 Table of Contents

FUJ00235007

FUJ00235007

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	

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

Optional Review	
Role	**Name**
IDAM Consultant	Rob Fellows
IDAM Consultant	Charlotte Hollands

(*) = 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

FUJ00235007

Reference	Version	Date	Title	Source
Ask Security	Latest		Europe Security Policy Manual	Ask Security
Ask Security	Latest		Security Toolkit Password Policy	Ask Security
SVM/SEC/PRO/4537	Latest		POA Privileged Account Release Procedure	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).

FUJ00235007

1 Introduction

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

The privileged account types in the POA include:

- **Personal Privileged** – Individual privileged accounts
- **Shared Privileged** – Shared privileged accounts
- **Local Administrator** – Local host admin access
- **Domain Administrator** – Windows domain accounts
- **Break Glass / Last Resort** – Emergency use only accounts
- **Service Accounts** – Local or domain non-interactive system accounts
- **Application Accounts** – Used by Application to access DBs
- **MSAD Service Accounts** – Domain non-interactive system accounts with local and network permissions

The Personal Privileged and Shared Privileged accounts can be further divided into two types:

- Internal Accounts for Fujitsu employees; and
- External Accounts for partners, suppliers, and external companies.

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. It is expected that every effort will 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 can be operated and complied with. Complying with the Sub-Master Policy is mandatory on POA and will see a significant alignment to the Master Policy too.

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

POA SecOps will maintain a Privileged Account Register of all privileged accounts which will include their compliance to the Master Policy, Sub-Master Policy and Password Policy. Exceptions will be recorded on the Privileged Account Register along with the reason for non-compliance. This will allow 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 to any specific rules.

2 Master Policy

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. It is expected that every effort will 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

2.1 Master Policy Rules

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

FUJ00235007

All privileged accounts that are held on the POA SecOps Register will record the compliance to these policy references. Any non-compliant responses will show the reason for the non-compliance and will, 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 centrally by POA SecOps and is only available on receipt of an authorised request – excludes User Service Accounts	Yes
MP03	The privileged account password is not known to potential users until it is needed and provided by POA SecOps on receipt of an authorised request – excludes User Service Accounts	Yes
MP04	The privileged account, if a User Service Account, must not permit human interactive logon	Yes
MP05	The privileged account password meets the Password Policy rules	Yes
MP06	The logon activity when the privileged account is used is logged on the local systems and stored for at least 1 month	Yes
MP07	The logon activity when the privileged account is used is stored centrally for at least 12 months	Yes
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	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 can only be used by another person after its password has been changed	Yes
MP14	There must be a documented list of all parties that COULD use/have access to 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

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 can be operated and complied with. Complying with the Sub-Master Policy is mandatory on POA and will see a significant alignment to the Master Policy too.

3.1 Sub-Master Policy Rules

The table below details the Sub-Master Policy references and associated policy rules.

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

FUJ00235007

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 meets 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 User Service Account, must not permit human interactive logon	Yes
SMP08	Privileged account owners will be required to respond to verification process checks every 90 days - and failure to respond 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	Privileged accounts must only make changes to the Live system under Change Control or formally operated processes such as APPSUP	Yes
SMP11	Changes made to the Live system using a privileged account under Change Control or formally operated processes such as APPSUP must be documented in the Fujitsu service management toolset (TfSNow)	Yes
SMP12	Changes made to the Live system using a privileged account under Change Control or formally operated processes such as APPSUP should be witnessed/checked by another Fujitsu user be documented in the Fujitsu service management toolset (TfSNow)	Yes
SMP13	When using a privileged account to make changes to the Live system every effort must be made to ensure the actions being performed are logged to a local system log that is also stored centrally and into the Audit Archive	Yes
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

4 Password Policy

The Password Policy is referred to in both the Master and Sub-Master Policies and compliance is considered mandatory for all privileged accounts in use on POA. The Password Policy is incremental to any password rules stated in the Europe Business Management System (EBMS) and applies more stringent local rules for POA.

FUJ00235007

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 will record the compliance to these policy references.

Password Policy Ref	Password Policy Rule	Mandatory
PP01	Is 16 characters exactly	Yes
PP02	Contains at least 2 upper case characters	Yes
PP03	Contains at least 2 lower case characters	Yes
PP04	Contains at least 1 special character (Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)	Yes
PP05	Contains at least 3 numeric characters	Yes
PP06	Does not contain back-to-back characters in sequence (e.g. abc)	Yes
PP07	Has not used a recycled modified password and is unique in format	Yes
PP08	The password is rotated every 90 days	Yes
PP09	The date of last password rotation is recorded	Yes

4.2 MSAD Account Password Policy

POA Password Policy is managed by POA SecOps and the following minimum criteria, further detailed in DEV/APP/LLD/0028, should be followed where the system allows:

Policy	Standard Account Minimum Contractual Setting	Standard Account Preferred Setting	Service Account Preferred Setting
Enforce password history	24 passwords remembered	24	0
Maximum password age [1]	30 days	30	0
Minimum password age [2]	1 days	1	0
Minimum password length	14 characters	16	25
Password must meet complexity requirements	Enabled	Enabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled	Disabled

[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	30 minutes

FUJ00235007

Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	3 minutes

Interactive Logon

Policy	Setting
Interactive logon: Prompt user to change password before expiration	14 days

4.3 Account and Password Principles

The following Account and Password Principles are essential for secure account and password management. All accounts created must follow least privileged access.

- **Account Privilege –** Minimum privilege access is granted according to the assigned role. Domain Admins have admin access to all computers in the domain but are issued to limited users and have tighter controls.
- **Account Review –** Account privileges and settings are reviewed monthly and compared to the assigned roles and tasks. This ensures that changes in roles and tasks are reflected in the account settings and privileges.
- **Password Handling –** All passwords are changed on a 90-day basis and never stored or transferred in an unsecure way. This reduces the risk of accounts being hacked or compromised. The only exceptions are those which are recorded in the Privileged Account Register as not meeting the Password Policy rules for an agreed reason.
- **Password Complexity –** All passwords will have the minimum complexity level according to the account class and risk level. This optimises the balance between password handling and the risk of accounts being hacked or compromised.
- **Reporting –** The implementation of the account and password policy with its underlying management processes is analysed, reported, and reviewed monthly. This supports the account and password security management and enables continuous improvement.
- **Documentation –** Principles, policies and guidelines are documented, published and communicated to the affected users. This ensures consistency and no interruption to service, or data loss through password compromise.

4.4 Account Separation

Strict separation must be maintained between account types for assigned tasks. This adheres to least privilege access principles.

4.5 Account Ownership

FUJ00235007

Where possible, privileged accounts should 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).

4.6 Account Lifecycle

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

4.7 Guidance on Selecting Strong Passwords

4.7.1 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.

4.7.2 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 applications and systems have been configured to require you to use a minimum of 14 characters in your password, but you can use longer passwords.
- 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.

FUJ00235007

- 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.

4.7.3 Difficulties selecting a Secure Password

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

- 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)

4.7.4 Things to Avoid as Passwords

Here are some guidelines of what not 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
- Any username on the computer in any form (as is, capitalised, etc.)
- A dictionary word, in any language
- A place name
- Passwords of all the same letter
- Simple patterns on the keyboard, like qwerty
- Any of the above spelled backwards
- 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

4.8 Account Lockout Policy

Note that account lockout policies must be set very carefully as they can be used for denial-of-service-attacks. Please see DEV/APP/LLD/0028 for more detail.

FUJ00235007

4.9 Personal Identification Numbers (PIN)

A PIN code is an ID number which is known only by a specific person or group of persons. It enables the PIN owner to identify themself to an IT system.

A PIN maybe used for:

- In combination with a hardware device (security token, smart card, employee badge). On POA, the iKey Smartcard uses a password and not a PIN.
- Personal security environment in the PKI.

Requirements:

- In general, a PIN must have a minimum of 4 numbers
- It is recommended to change an initial send PIN into a personal PIN, whenever possible.
- No employee is allowed to hand over the PIN to another person, including IT staff, administrators, superiors, other colleagues, friends, or family members.
- The loss of a PIN must be immediately reported to POA SecOps.

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 forced to change immediately.
- 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) electronic mail 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 forced to change immediately.
- Where phone calls to help desk agents are involved, identification of the user is mandatory, for example, use of the users' UK personnel number.

5.2 Default Passwords

Default vendor passwords must be changed during the installation of applications, systems and network devices.

5.3 Storage of Privileged Passwords

FUJ00235007

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.

Audit logging controls are to be implemented within the password storage system, to ensure that all access to passwords stored within password storage system is recorded.

5.4 Network Transmission

Clear text passwords must not be transmitted over the unprotected Internet or internal networks.

Specific passwords may be transmitted over the internet to gain remote access to company resources, via the company's IPSEC-secured Virtual Private Network or SSL-protected website but they must also be secured.

5.5 Built-in/root Administrator Accounts

Built-in/root administrator passwords must be individual per system. The passwords are to be changed on a regular basis as per the Password Policy.

The built-in Administrator password must not be transmitted over unprotected internet connections and never in clear text.

The password used for external services must be different from the password used for the internal account, especially when the company e-mail address is related to this account.

5.6 Changing Passwords for Centrally Managed Accounts

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.

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

5.7 Password Release Process 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

FUJ00235007

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

5.8 Password Management Requirements

Passwords should be treated as confidential information. No employee is allowed to handover their own account password to another person, including IT staff, administrators, superiors, other colleagues, friends, or family members. Any 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 contact POA SecOps as this is a Security Incident that must be recorded and investigated.

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.
- If possible, don’t use the same password to access multiple company systems.

6 Service Accounts

6.1 Service Account creation

FUJ00235007

Service Accounts should be requested via the POA JML process so that they are correctly approved and recorded on the Privileged Account Register maintained by POA SecOps.

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 to conduct each task they have been created for. Using distinctive 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 storage

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@uk.fujitsu.com) 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 Changing a Service Account password

The process is described in “Changing Passwords for Centrally Managed Accounts” above.

6.5 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.