

MSP Password Rotation SOP

Document no.	SOP-MSP-010
Revision	1.0
Owner	Security Lead
Effective date	October 15, 2026
Review cycle	Every 6 months

1. Purpose

To keep the privileged and shared credentials an MSP holds for its clients from being misused, by rotating them on a schedule, rotating them immediately when someone leaves or a compromise is suspected, and proving it in the vault.

2. Scope

Applies to privileged and shared credentials the MSP manages for clients: domain and cloud admin accounts, service accounts, local administrator accounts, network device logins, break-glass accounts and shared Wi-Fi keys. Personal user passwords follow the client's own password policy.

Definitions

Privileged account	An account with administrative rights over systems, tenants or network devices.
Service account	A non-person account that applications, scheduled tasks or services use to run.
Break-glass account	An emergency admin account kept for when normal admin access fails, used rarely and monitored closely.
Trigger event	An event that requires immediate rotation, such as a technician leaving or a suspected compromise.

3. Responsibilities

Security Engineer	Maintains the credential inventory and rotation schedule, handles trigger-based rotations and audits the vault.
Systems Engineer	Rotates credentials, updates the systems that depend on them and confirms nothing broke.
Service Manager	Makes sure rotations happen on schedule across clients and reports compliance.
Client Point of Contact	Is told about rotations that affect client staff, such as shared Wi-Fi keys, and reports client-side trigger events.

RACI matrix

Activity	Security Engineer	Systems Engineer	Service Manager	Client Point of Contact
Maintain the credential inventory	R/A	C	I	-
Rotate credentials on schedule	A	R	I	I
Rotate after a trigger event	R/A	R	I	C

Activity	Security Engineer	Systems Engineer	Service Manager	Client Point of Contact
Audit and report rotation compliance	R	-	R/A	I

R = Responsible, A = Accountable, C = Consulted, I = Informed

4. Materials and PPE

Materials, tools and systems

- Password manager with a vault per client
- Credential inventory with rotation intervals
- Local administrator password management tool
- PSA recurring tickets for manual rotations
- Vault audit log
- Service account dependency list

5. Procedure

Step	Task	Owner	Done
5.1	Inventory the credentials in scope The Security Engineer lists every privileged, service, network device, break-glass and shared credential per client in the vault, each with an owner and account type.	Security Engineer	☐
5.2	Set rotation intervals by account type The Security Engineer sets a rotation interval for each account type, for example quarterly for admin and network device accounts and yearly for service accounts, and records it on each entry.	Security Engineer	☐
5.3	Turn on automatic rotation where possible The Systems Engineer enables automatic rotation for local administrator accounts and any vault-managed accounts that support it, and confirms the new passwords sync to the vault.	Systems Engineer	☐
5.4	Schedule manual rotations The Security Engineer creates recurring PSA tickets for every credential that must be rotated by hand, due before its interval ends.	Security Engineer	☐
5.5	Check service account dependencies Before rotating a service account, the Systems Engineer lists every service, scheduled task and application that uses it from the dependency list and the system itself. Warning: Rotating a service account without updating everything that uses it can take a client's application down. Check dependencies first.	Systems Engineer	☐
5.6	Generate and store the new password The Systems Engineer generates a long random password in the password manager and saves it to the vault entry at the moment it is changed on the system.	Systems Engineer	☐
5.7	Update dependent systems and test The Systems Engineer updates every dependent service and task with the new password, restarts what is needed and confirms everything runs. Checkpoint: The account works on the system, every dependency runs and the vault holds the current password.	Systems Engineer	☐

Step	Task	Owner	Done
5.8	Rotate immediately after a trigger event When a technician leaves the MSP, a client admin leaves, a credential is shared insecurely or a compromise is suspected, the Security Engineer rotates every affected credential at once. Checkpoint: All credentials affected by a trigger event are rotated within 24 hours.	Security Engineer	☐
5.9	Rotate break-glass accounts after use After a break-glass account is used, the Systems Engineer rotates its password, records why it was used and confirms its alerts are still active.	Systems Engineer	☐
5.10	Tell the client about shared credential changes The Client Point of Contact receives notice of rotations that affect client staff, such as shared Wi-Fi keys or shared mailbox logins, and passes the change on internally.	Client Point of Contact	☐
5.11	Audit the vault every month The Security Engineer reviews the vault audit log and inventory for overdue rotations, credentials viewed by people who left and entries without an owner.	Security Engineer	☐
5.12	Report rotation compliance The Service Manager reports rotation compliance per client every month and follows up on overdue rotations with the responsible engineers.	Service Manager	☐

6. Quality checks

- Every privileged and shared credential is in the vault with an owner and rotation interval.
- No credential is past its rotation date.
- All credentials a departing technician could access were rotated within 24 hours.
- Service account rotations caused no unplanned outages.
- Every break-glass use is followed by a rotation and a recorded reason.

7. Records

- Credential inventory with rotation intervals
- Rotation tickets and vault change history
- Trigger event log with rotations performed
- Monthly vault audit and compliance report

8. KPIs

- Percentage of credentials rotated within their interval
- Hours from trigger event to completed rotation
- Number of outages caused by credential rotation
- Number of vault entries without an owner

9. Common mistakes

- Not rotating client credentials when a technician leaves the MSP.
- Rotating a service account without updating the services that use it.
- Changing a password on the system but not saving it to the vault.
- Forgetting break-glass and network device accounts entirely.

10. Revision history

Revision	Date	Description	Reviewed by
1.0	October 15, 2026	Initial release	Ilia Pirozhenko

Approval

Prepared by	Approved by	Date

This is a template. Adapt it to your organization, equipment and local regulations before use.



Scan for the latest version

Opens this template online, where you can download it again in Word, PDF, Excel or CSV — free, no sign-up.

Or [add it to Perfect Wiki](#) so your team can find it and ask questions about it in Microsoft Teams, Slack, kChat or Mattermost.