# SOP: Temporary Secret Sharing via BT Secret Safe

Owner: IAM / Security Engineering

Last Updated: [Insert Date]

Version: 1.0

Status: Draft for Team Review

## Purpose

This procedure defines a standardized approach for temporarily sharing secrets with other teams or developers. It replaces previous ad hoc methods (e.g., Vault) with a consistent, time-bound, and auditable process using BT's Secret Safe.

## Scope

Applies to any internal team needing to share credentials or sensitive secrets temporarily with other teams or project collaborators — including cross-functional groups such as Helios, TTWN Ad+, etc.

## Procedure Overview

### 1. Secret Creation

• Create the secret in BT Secret Safe using the naming convention: KV-[ProjectName] (e.g., KV-Helios).

• Avoid using Vault for one-off secrets going forward unless exception approved.

### 2. Access Group Management

• Confirm with the project owner (e.g., Steve for Helios) who needs access.

• Create or update a BT group (e.g., Helios\_BT) with those members.

• Avoid including overly broad groups with 20+ users unless explicitly necessary.

### 3. Assign Permissions

• Grant View and Retrieve permissions to the group on the specific safe.

• Optionally grant Delete permission if the receiving team is responsible for cleanup.

• Set permissions to expire in 7 days (default) unless otherwise specified.

### 4. Notification

• Notify the receiving team via email or chat:

- The secret is available in BT Secret Safe

- Access will expire in 7 days

- They are responsible for copying the secret into their own managed system (e.g., AWS Secrets Manager)

### 5. Post-Access Cleanup

• After the expiration period:

- Remove group access if not already expired

- Delete the secret from BT if it is no longer needed

- Confirm the secret was successfully migrated by the receiving team

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Requesting Team | Confirm who needs access, retrieve secret, migrate to own system |
| IAM/SecOps Team | Create the secret, manage access group, set expiration, notify users |
| Project Owner | Approve access list (e.g., confirm team members) |

## Audit and Logging

• All access is logged automatically in BT for audit purposes.

• Periodic reviews should be conducted to ensure no long-term secrets are left in temporary safes.

## Exceptions

• Long-term access or production credentials must follow formal provisioning processes.

• Requests to use Vault must be approved by IAM management.

## Next Steps

• This draft is open for team input and feedback.

• Once finalized, this SOP will replace any informal processes currently in place for temporary secret sharing.