



**YOUR LOGO**

# Privileged Password Security Policy Template

**Policy #**

#####

**Effective Date**

DD/MM/YYYY

**Email**

policycontact@company.com

**Version**

1.0

**Contact**

Policy Contact

**Phone**

888.641.5000

## About this Template

This sample security policy can be used as a starting point template for a privileged account management policy for your organization. Privileged accounts present a much greater risk than typical user accounts and thus require a higher level of control. The policy is divided into several sections according to the common governance areas regarding privileged accounts. It contains over 40 pre-written information security statements. Organizations can remove policy statements that do not apply or fit the organization's governance requirements.



**Information  
Shield**

This template is structured using the "Best Practices Security Policy Template" from Information Shield. The template has been used by well over 1000 organizations.

Template Co-Created by



InformationShield

and

**thycotic**

**Table of Contents**

Policy Information and About this Template

- Customizing the Template ..... 2
- Disclaimer ..... 2
- Support..... 2
- 1.0 Purpose ..... 3
- 2.0 Scope ..... 3
- 3.0 Policy ..... 3
  - 3.1 SYSTEM APPROVAL AND AUTHORIZATION ..... 3
  - 3.2 Password Categorization ..... 3
  - 3.3 Password Composition ..... 4
  - 3.4 Password History and Change Interval ..... 5
  - 3.5 Account Lockout and Compromised Passwords ..... 6
  - 3.6 Acceptable Use Privileged Accounts ..... 6
  - 3.7 Privileged Account Approval ..... 7
  - 3.8 Privileged Account Construction ..... 7
  - 3.9 Privileged Account Management ..... 8
  - 3.10 Third Party Privileged Accounts ..... 9
  - 3.11 Application Development ..... 9
  - 3.12 Privileged Account Logging ..... 9
- 4.0 Violations ..... 10
- 5.0 Definitions ..... 10
- 6.0 References ..... 11
- 7.0 Approval and Ownership..... 12
- 8.0 Revision History ..... 12
- 9.0 Appendix – Secret Server Policy Enforcement..... 13

## Customizing the Template

To customize this template perform the following steps:

1. Download the template
2. Open the template as a Microsoft Word document
3. Remove the “About this Template” and “Customizing the Template” instructions and other author comments
4. Replace the term “Company X” with the name of your organization
5. Replace the current logo or add your company logo in the upper left corner
6. Update all of the company-specific contact information (highlighted in yellow)
7. Update the effective date
8. Revise any policy guideline to meet your organization’s policies
9. Revise the Violations section to meet your organization’s policies
10. Save your changes
11. Obtain your management and auditors’ approval of the completed Policy
12. Distribute Policy according to your management guidance

## Disclaimer

This document is a template only and should be revised to meet the information security guidelines of your organization. Organizations should not adopt any security policy without proper review and approval by senior management, information security, and legal.

## Support

Support for the Privileged Password Security Policy Template is available in our Free Tools forum at <http://my.thycotic.com/forums/topics.aspx?ForumID=4>

## 1.0 Purpose

---

This policy defines the requirements for establishing and maintaining account settings for all privileged user accounts on any **Company X** computer and communications system.

## 2.0 Scope


---

This policy applies to all information security analysts and system administrators responsible for the maintenance of accounts and password management systems on **Company X** electronic information resources.

## 3.0 Policy

---

### 3.1 SYSTEM APPROVAL AND AUTHORIZATION


 *(Default accounts and passwords present one of the greatest risks to production systems. This section defines specific controls for controlling and managing privileged accounts when systems are placed into production. These controls may also be part of a policy regarding System Configuration Management.)*

**3.1.1 Default Password Changes** - All vendor-supplied default passwords must be changed before any computer or communications system is used for **Company X** business.

**3.1.2 Privileged User ID Review** - Before any production multi-user computer operating system is installed at **Company X**, all privileged user IDs that are not assigned to a specific employee or job role must have their passwords changed to large random values and these should be recorded in the privileged account management system with appropriate permissions for the administrators responsible for managing these accounts.

**3.1.3 Unnecessary Software** - Software features that could be used to compromise security, and that are clearly unnecessary in the **Company X** computing environment, must be disabled at the time when software is installed on multi-user systems.

### 3.2 Password Categorization

 *(This section defines specific terminology for understanding different categories of passwords which is then helpful for prescribing controls on those passwords. Treating all passwords the same is not effective.)*

**Passwords fall into two categories:**


**User Account Passwords** – First, a password is a secret that allows the use of an account. An account may represent a human being and therefore that password determines a human identity, for example, an Active Directory user account. The Active Directory user account

password is the secret known by the human that identifies that human to the system. These types of passwords are known as user account passwords and they need to be memorized by the human whose identity they represent. A goal is to strive for as few user account passwords per human user as possible, ideally a single user account password per human user. .

**Privileged Account Passwords** – Privileged account passwords are passwords where the account does not represent a human being – this could be a system account like UNIX root or a service account. The passwords on these accounts do not typically provide for any identity of a human and therefore do not need to be memorized. These passwords can be set to very large values and stored in the privileged account management system.

The focus of this Privileged Password Security Policy document is on the second type of password, Privileged Account Passwords. However, because User Account passwords often have elevated or administrative privileges attached to them, both types of passwords are described in many of the guidelines in this policy.

### 3.3 Password Composition

 *(This section defines specific controls for creating secure passwords for privileged accounts. Passwords for privileged accounts must generally be more secure than for regular user accounts.)*

**3.3.1 Role-Based Password Length** - The minimum length for fixed passwords, or passwords created by users, must be set to six for handheld computers, eight for all network-connected computers, and ten for administrator and other privileged user IDs.

**3.3.2 User Account Password Complexity** - All user-chosen passwords for user accounts must meet the following complexity requirements:

- Must contain at least one alphabetic, one numeric and one symbol character.
- Must be at least 8 characters in length.
- Ideally passphrases should be used to increase length. Increased length provides more security than complexity and is easier for a human to memorize.

For example:

1) If@j7asFd! versus 2) Blue5Chandelier2@

The seven extra characters in (2) make it 64 trillion times stronger than (1).

**3.3.3 Privileged Account Password Complexity** – These passwords should be optimized for security since no human needs to memorize these passwords. They can be optimized for the maximum lengths of the platform. For example: Recent versions of Windows allow for up to 127 characters for the password – therefore random passwords should be generated between 80 and 127 characters in length to provide the maximum security. The following requirements should be followed for Privileged passwords:

- Should maximize the possible length of password for each platform.
- Should not be memorized.
- Passphrases should not be used since memorization is not desirable.


- Should have a complete mix of upper case, lower case, numbers, and symbols.

**3.3.4 Seed for Generated Passwords for Privileged Accounts** - If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other very-frequently-changing and unpredictable source.

**3.3.5 Null Passwords Always Prohibited** - At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

**3.3.6 Enforce Password Complexity** - All passwords must meet the above complexity requirements and this complexity must always be checked automatically at the time that the password is created or changed.

### 3.4 Password History and Change Interval

 *(This section defines specific controls for changing passwords for privileged accounts. Passwords for privileged accounts must generally be more secure than passwords for regular user accounts.)*

**3.4.1 User Account Password Changes** – Users must be required to change their password at least once every 90 days. It is better to have good passwords that can be memorized than frequent changes of these passwords. More frequent changes will lead to more forgotten passwords or weaker passwords being chosen with little security benefit.

**3.4.2 User Account Maximum Password Changes** – Users must not be permitted to change their password within 7 days of their previous change. This requirement is only helpful for passwords that users are memorizing (user accounts) and is used to prevent users from changing the password multiple times back to a previously used password (therefore defeating the requirement to change the password).

**3.4.3 Privileged Account Password Changes** – All privileged accounts must be automatically required to change their passwords at least once every 90 days. This time interval should be set based on an internal risk assessment for any potential disruption to the business. For example: A service account password change can be highly disruptive if it is part of a mission critical system and therefore this password change could be once every 90 days. However a Domain Admin account password change would have zero disruption to the business and is very high risk – these accounts should have their passwords changed as often as possible – ideally after every use to reduce exposure to abuse, misuse or exploits such as Pass the Hash attacks.

**3.4.4 Password History** - On all multi-user **Company X** computers, system software or security software must be used to maintain an encrypted history of previously chosen fixed passwords. This history must contain at least the previous thirteen passwords for each user ID.

### 3.5 Account Lockout and Compromised Passwords

**i** *(Privileged accounts must be protected against brute-force password guessing techniques just as user accounts are protected. The specific parameters of password attempts and lockout duration should be customized based on the organization's specific requirements.)*

**3.5.1 Maximum Login Attempts** - All **Company X** computer systems that employ fixed passwords at log on must be configured to permit only five attempts to enter a correct password, after which the user ID is deactivated.

**3.5.2 Lockout Duration** – All accounts that have been disabled for incorrect logon attempts must remain inactive for at least 15 minutes.

**3.5.3 Lockout Notification** – All disabling of accounts for incorrect logon attempts must be notified to the security team so that investigation can occur if necessary and anomalies can be detected.

**3.5.4 Password Changes After Privileged User Credential Compromise** - If a privileged user credential has been compromised by an intruder or another type of unauthorized user, all passwords on that system and any related systems must be immediately changed.

**3.5.5 Fixed Password Change Confirmation** – System administrators must be immediately notified when fixed passwords are changed or updated outside of the central privileged account management system.

### 3.6 Acceptable Use Privileged Accounts

**i** *(Sharing passwords between systems creates great risk. A single compromised system can allow an attacker to quickly move laterally across the network. This section contains controls to limit password sharing across systems.)*

**3.6.1 User Account Password Sharing** – User Account Passwords must never be shared or revealed to anyone other than the authorized user. If they are shared then they are no longer a User Account since the identity of the user is not known.

**3.6.2 Privileged Account Password Sharing** - Passwords for privileged accounts can be shared among administrators as long as controls are in place to know which administrator is using the account at any one time. This must include full auditing and non-repudiation mechanisms. Each system must have a unique password.

**3.6.3 Password Display And Printing** - The display and printing of account passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. Any display of a privileged account password to a user must be audited and the password should be changed after it has been used.

### 3.7 Privileged Account Approval

**i** *(Because of the added risk of compromise, privileged accounts must be strictly controlled. The following sections contain controls for the approval, creation and maintenance of accounts.)*

**3.7.1 Privileged Account Requirements** – All privileged accounts on **Company X** systems must employ greater security than non-privileged accounts. This includes longer, more secure passwords and greater audit accountability.

**3.7.2 Privileged User Account Approval** – The creation or modification of privileged user accounts must be approved by at least two individuals: The System Owner and an authorized member of the Information Technology department. System administrators must not be allowed to create other privileged accounts without authorization.

**3.7.3 Number of Privileged User IDs** - The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

**3.7.4 Role Based Account Privileges** – To facilitate secure management of systems, wherever possible, privileged accounts must be defined based on the specific role of the system administrator.

### 3.8 Privileged Account Construction

**i** *(One way to reduce confusion and gain oversight is to adopt standards for privileged accounts that are created by the organization. For proper separation of duties, administrators must use separate accounts for their day-to-day user activities.)*

**3.8.1 Privileged User ID Construction**- All privileged user IDs on **Company X** computers and networks must be constructed according to the **Company X** user ID construction standard, and must conform to one of the following:

- Must clearly indicate the responsible individual's name.
- Must clearly define the purpose of the account (i.e. purpose of the account, type of account, etc.
- Must be managed in a system which can clearly associate a single User Account to each use of the Privileged Account in order to document accountability for the use of the Privileged ID


**3.8.2 Generic User IDs** - User IDs must uniquely identify specific individuals and generic user IDs based on job function, organizational title or role, descriptive of a project, or anonymous, must be avoided wherever possible. User IDs for service accounts and other application accounts should also follow the **Company X** naming convention and requirements outlined in section 3.8.1 above.



**3.8.3 Re-Use Of User IDs** - Each **Company X** computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with **Company X**.

**3.8.4 Separate Systems Administrator User IDs** - System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day-to-day work.

### 3.9 Privileged Account Management

 *(The variety of privileged account types across various systems presents unique management challenges. Modern software applications provide ways to automate account discovery, management and removal. These systems should be used whenever possible to reduce risk and increase visibility.)*

**3.9.1 Central Automated Management** – All privileged accounts on **Company X** systems must be managed by a central system. This system must provide an audit trail that tracks specific additions, changes, and deletions.

**3.9.2 Integration with Native Directories** – Any privileged account management system must integrate with native operating system account management systems or directory services (such as Active Directory)

**3.9.3 Integration with Strong Authentication Methods** – Any privileged account management system must integrate with strong authentication methods (such as multi-factor authentication) to ensure the identity of the user in addition to their directory authentication.

**3.9.4 Password Vault** – **Company X** system administrators must have access to a vault system that enables the temporary provisioning of access to privileged accounts and passwords (aka FireID) for emergency maintenance.

**3.9.5 Password Vault Encryption** – **Company X** must maintain any credentials stored in a central management system within an encrypted password vault, using strong encryption algorithms that meet compliance and/or regulatory requirements.

**3.9.6 Privileged Account Inventory** – **Company X** must maintain an inventory of all accounts with privileged access on production information systems. These include, at a minimum, local administrator accounts and service accounts.

**3.9.7 Account Inventory Update** – The privileged account inventory must be updated at least quarterly to identify new or changed accounts.


**3.9.8 Inactive Account Maintenance** - All inactive accounts over 90 days old must be either removed or disabled.

**3.9.9 Disaster Recovery** – Any privileged account management system must be configured to utilize robust backup, recovery and availability methodologies in order to ensure resiliency and availability of the credentials stored within the system as well as the timely recovery of the system in the event of a system failure.

### 3.10 Third Party Privileged Accounts

**Third Party User ID Expiration** - Every privileged user ID established for a non-employee or third party application must have a specified expiration date, with a default expiration of 30 days when the actual expiration date is unknown.

### 3.11 Application Development

 *(Most applications that require privileged accounts to operate present unique challenges. In many cases these accounts are not disclosed, or use default accounts with fixed passwords. Privileged account security can be greatly enhanced using secure application design and coding principles.)*

**3.11.1 Special Application Accounts** – All production applications that require privileged access must use special application accounts that are created specifically for the given application. Applications must never use default administrator accounts.

**3.11.2 Secret IDs or Passwords** - Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.

**3.11.3 Hard-Coded Passwords In Software** - Passwords must never be hard-coded in software developed by or modified by **Company X** workers.

**3.11.4 Test Account Removal** - Test data and accounts used during development and testing must be removed before a production system becomes active.

### 3.12 Privileged Account Logging

 *(To provide audit visibility into privileged accounts, systems must be designed and configured to log events linked to privileged accounts.)*

**3.12.1 Privileged System Commands Traceability** - All privileged commands issued on computer and communication systems must be traceable to specific individuals through the use of comprehensive logs.

**3.12.2 Privileged User ID Activity Logging** - All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs must be securely logged.

**3.12.3 Privileged User ID Activity Log Review** - All logs recording privileged ID activity must be reviewed at least quarterly via periodic management reports.

**3.12.4 Privileged User ID Activity Log Correlation** – All logs recording privileged ID activity must be aggregated into a central log management or Security Information and Event Management (SIEM) tool in order to correlate privileged ID activity to other security events, log entries and related non-privileged ID activity.

**3.12.5 Privileged User ID Session Logging** – In addition to event logging, all activity on privileged accounts must be logged via session or keystroke recording.

## 4.0 Violations

---

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Company X does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or in the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

## 5.0 Definitions

---

**Account (User ID or Username)** - A unique string of characters assigned to a user by which a person is identified to a computer system or network. A user commonly must enter both a user ID and a password as an authentication mechanism during the logon process.

**Fixed Password** – A password created by a user for an account or credential.

**Least Privilege** - Least privilege means that for each task or process, the administrator is granted the minimum rights required to perform the task.

**Password** – An arbitrary string of characters that is used to authenticate an account when attempting to log on, in order to prevent unauthorized access to the account.

**Privileged Account** – An account that can either be a user account on any system that has system privileges beyond those of a normal user or an account that does not represent a human use. Privileged accounts are typically not assigned to a user, but can, in some cases, be dedicated user accounts which are given more permissions than a typical user account. Root, local administrator, domain admin and enable passwords are all examples of privileged accounts that have elevated access beyond that of a normal user. Passwords for privileged accounts should be randomized, not memorized by anyone, and changed frequently.


**System Administrator** – An employee or partner who is responsible for managing a Company X multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

**Third Party** – Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**User** - Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

**User Account** – An account that represents a single human user. They are the only person to ever use the account and it is their way of authenticating into Company X systems. The password for this account is something they would memorize and would not be shared with any other user.

## 6.0 References

 (This section contains references to the information security laws and governance frameworks applicable to this Privileged Password Security Policy.)

### Policy and Regulation Section Mapping (for reference only)

Section	Thycotic Policy Description	PCI DSS v3 Section	NIST 800-66 HIPAA Security Rule	HIPAA Section	ISO 17799/27001
3.3.2	User Account Password Complexity	8.2.3		164.308(a)(5)(ii)(D)	11.2.2, 11.3.1, 12.1.1
3.3.3	Privileged Account Password Complexity	8.2			11.3.1
3.4.1	User Account Password Changes	8.2.4		164.308(a)(5)(ii)(D)	11.2.2, 11.3.1, 12.1.1
3.4.3	Privileged Account Password Changes	8.2.4		164.308(a)(5)(ii)(D)	11.2.2, 11.3.1, 12.1.1
3.4.4	Password History	8.2.5		164.308(a)(5)(ii)(D)	11.2.2, 11.3.1, 12.1.1
3.5.1	Maximum Login Attempts	8.1.6		164.308(a)(5)(ii)(D)	11.2.2, 11.3.1, 12.1.1
3.5.2	Lockout Duration	8.1.7		164.312(a)(1)	11.2.2, 11.3.1, 12.1.1
3.7.2	Privileged Account Approval		4.14.6	164.312(a)(4)	11.2.4, 12.5.1
3.7.4	Role-Based Account Privileges	7.1.2, 7.1.3			11.2.2
3.8	Privileged Account Construction		4.14.3	164.312(a)(4)	11.5.2
3.9.1	Central Automated Management	8.5	4.14.5	164.312(a)(4)	11.5.3
3.9.3	Integration with Strong Authentication Methods	8.3 & 8.2.2			11.5.1
3.9.5	Password Vault Encryption	8.2.1			11.5.3
3.9.6	Privileged Account Inventory		4.16.1	164.312(c)(1)	8.3.3, 11.2.4
3.9.8	Inactive Account Maintenance	8.1.4			8.3.3
3.12.2	Privileged User ID Activity Logging	8.1.2	4.15.1, 4.14.2, 4.14.4	164.312(b)	11.5.2

## 7.0 Approval and Ownership

Owner	Title	Date	Signature
Policy Contact	Title	MM/DD/YYYY	
Approved By	Title	Date	Signature
Executive Sponsor	Title	MM/DD/YYYY	

## 8.0 Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	10/25/15		

## 9.0 Appendix – Secret Server Policy Enforcement

This Appendix is optional and should be deleted before you distribute this security policy to your organization. This Appendix is a table listing the Policy statements in this document that are enforceable using Thycotic’s Secret Server solution. Having a written Privileged Password Policy using this template is a great first step, but now you need to enforce this policy—making sure passwords are vaulted, encrypted, changed, and monitored, all according to this policy. Thycotic Secret Server automatically discovers, vaults, and manages privileged passwords, ensuring your compliance with your written policy guidelines. Details on this enforcement are in the table below.

Guideline #	Policy Guideline	Secret Server Enforcement of this Guideline
3.1.1	All vendor-supplied default passwords must be changed before any computer or communications system is used.	Secret Server can be configured through its Discovery capabilities to find new systems on the network and automatically secure their passwords and store them in the vault with access for the appropriate admins.
3.1.2	Before any production multi-user computer operating system is installed, all privileged user IDs that are not assigned to a specific employee or job role must have their passwords changed to large random values and these should be recorded in the privileged account management system with appropriate permissions for the administrators responsible for managing these accounts.	Secret Server offers Discovery capabilities with configurable rules for how to find systems, accounts, how to securely randomize their passwords and also who to grant access to the secure credentials in the Secret Server vault. The entire process is customizable and automated.
3.2	Passwords fall into two categories: <ul style="list-style-type: none"> <li>• User Account Passwords</li> <li>• Privileged Account Passwords</li> </ul>	Secret Server provides the secure vault to store all privileged account passwords as well as user accounts with elevated or administrative privileges. They need to be large, random and frequently changed – Secret Server automates this process.
3.3.1	The minimum length for fixed passwords must be set to six for voice mail boxes and handheld computers, twelve for all network-connected computers, and longer for administrator and other privileged user IDs	Secret Server uses templates and Password Requirements to set the rules for length and complexity on passwords. This makes it easy to ensure that all passwords have sufficient complexity and this is automated.
3.3.3	The following requirements should be followed for privileged account passwords: <ul style="list-style-type: none"> <li>• Should maximize the possible length of password for each platform.</li> </ul>	Secret Server has policies, templates and password requirements which allows you to easily maximize the length and complexity of privileged account passwords. Secret Server can easily generate, enforce and rotate passwords that are 100 random characters or more for these accounts. This makes it

	<ul style="list-style-type: none"> <li>• Should not be memorized.</li> <li>• Passphrases should not be used since memorization is not desirable.</li> </ul> <p>Should have a complete mix of upper case, lower case, numbers and symbols</p>	impractical to memorize or write down. The use of these passwords is still simple for administrators using the Secret Server tool.
3.3.4	If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other very-frequently-changing and unpredictable source.	Secret Server uses secure random numbers to generate large random passwords. The libraries used are approved by Microsoft to produce cryptographically secure random numbers.
3.3.5	Null Passwords Always Prohibited.	Secret Server can find weak passwords using the Discovery capability. These passwords can then be automatically changed by Secret Server to ensure policy requirements are met.
3.3.6	All passwords must meet the above complexity requirements and this complexity must always be checked automatically at the time that the password is created or changed	Secret Server will enforce policy and password requirements on new passwords as they are created and on existing accounts. Customizable alerts and reporting ensure that all passwords meet your requirements and can be proven to an auditor.
3.4.3	All privileged accounts must be automatically required to change their passwords at least once every 90 days.	Secret Server offers an expiration policy capability that can be enforced as part of your policy. This ensures that all privileged account passwords are changed on a configurable schedule. Calendar specifics can also be set – for example: Only change this password on Sundays at 2am once the 90 day threshold has been met.
3.4.4	On all multi-user computers, system software or security software must be used to maintain an encrypted history of previously chosen fixed passwords. This history must contain at least the previous ten passwords for each user ID.	Secret Server automatically tracks history on all passwords keeping a full log of previous passwords. This is helpful when restoring a system from backup and an earlier password is needed.
3.5.4	If a privileged user ID has been compromised by an intruder or another type of unauthorized user, all passwords on that system and any related systems must be immediately changed.	Secret Server provides mechanisms to easily identify vulnerable passwords and automatically change thousands of passwords in minutes.
3.5.5	System administrators must be immediately notified when fixed passwords are changed or updated outside of the central privileged account management system.	Secret Server provides the Heartbeat capability to constantly test and validate passwords kept in the vault. If an administrator or an intruder changes a password outside of the vault or creates a

		backdoor account on a system, then alerts can be generated to the administrator team or Security Office.
3.6.2	Passwords for privileged accounts can be shared among administrators as long as controls are in place to know which administrator is using the account at any one time. This must include full auditing and non-repudiation mechanisms	Secret Server provides full auditing on all use of passwords from the vault. If a password is given to an administrator then the CheckOut capability should be used to ensure that the password is changed when the admins are finished using it. This ensures there is full accountability on the usage of all accounts.
3.6.3	The display and printing of account passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. Any display of a privileged account password to a user must be audited and the password should be changed after it has been used.	Secret Server provides controls to allow the authorized use of a password without revealing the password itself. This protects the password from disclosure while still auditing its use. If the password has to be provided to the administrator (for example, for legacy systems) then Secret Server provides the CheckOut capability to ensure that the password is changed after it is used.
3.7.1	All privileged accounts on Company systems must employ greater security than non-privileged accounts. This includes longer, more secure passwords and greater audit accountability.	Secret Server takes security on privileged account passwords to the maximum while preserving convenience for the administrators – ensuring long random passwords, auditing their usage and controlling access.
3.7.2	The creation or modification of privileged user accounts must be approved by at least two individuals: The System Owner and a member of the Information Technology department. System administrators must not be allowed to create other privileged accounts without authorization.	Secret Server provides workflow capabilities with dual approval for sensitive accounts. Backdoor accounts can also be detected, secured and the Security Office can be notified to ensure that administrators never create unauthorized accounts.
3.7.3	The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.	Granular permissions within Secret Server allow access to be limited to specific individuals and groups allowing teams to follow the security best practice of “least privilege” with ease.
3.7.4	To facilitate secure management of systems, wherever possible, privileged accounts must be defined based on the specific role of the system administrator.	Secret Server allows specific access to privileged accounts, and access can be easily provisioned to administrators based on their membership in Active Directory groups. This allows privileged access to be granted only for certain functions based on role.
3.8.2	User IDs must uniquely identify specific individuals, and generic user IDs based on job function, organizational title or role, descriptive of a project, or anonymous, must be avoided wherever possible. User IDs for service accounts and other	In the cases where generic user IDs can't be avoided then Secret Server can be used to manage access using these accounts to ensure they are both secure and users remain accountable.



	application accounts should also follow the Company naming convention.	
3.8.4	System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day-to-day work.	Secret Server can be used to effectively manage named privileged accounts (a common example are Active Directory Domain Admin accounts – these can be vaulted ensuring passwords are very strong, changed frequently and Pass the Hash attacks are mitigated). While these accounts are assigned to a user, the high levels of access and privileges they are given require that they are governed as privileged accounts for purpose of this policy.
3.9.1	All privileged accounts on Company systems must be managed by a central system. This system must provide an audit trail that tracks specific additions, changes and deletions.	Secret Server tracks all usage of privileged accounts being managed. There is extensive auditing of all changes and usage which can be configured to provide alerts, daily reports or ad-hoc reporting for auditors.
3.9.2	Any privileged account management system must integrate with native operating system account management systems (such as Active Directory)	Secret Server integrates with Active Directory for authentication, granular permissions (role based access control) and automation for password changing.
3.9.3	Any privileged account management system must integrate with strong authentication (such as multi-factor authentication) to ensure the identity of the user in addition to their directory authentication.	Various multi-factor technologies can be used with Secret Server including RSA SecurID, Duo Security, Google Authenticator (TOTP) and any technology that is RADIUS compatible (this covers most vendors).
3.9.4	Company system administrators must have access to a vault system which enables the generation of temporary privileged accounts and passwords (aka FireID) for emergency maintenance.	Secret Server provides Unlimited Administrator Mode which can be used in emergency situations to gain access to restricted credentials. All actions are notified to appropriate groups and everything is fully audited. This ensures that an organization is prepared for any catastrophe from a password perspective and includes the ability for dual control to activate the firecall mode.
3.9.6	Company must maintain an inventory of all accounts with privileged access on production information systems. These include, at a minimum, local administrator accounts and service accounts.	Secret Server provides Discovery capabilities to find new accounts on the network and automatically track those accounts against those in the vault. Accounts can also be automatically imported into the vault using configurable discovery rules. This ensures that the vault automates the process of inventory and reconciliation of accounts.
3.9.7	The privileged account inventory must be updated at least quarterly to identify new or changed accounts.	Secret Server provides an updated inventory of accounts on an ongoing basis through its automated discovery which is continually

		reviewing the environment for changes. There is no need for human intervention or manual work.
3.9.8	All inactive accounts over 90 days old must be either removed or disabled.	Secret Server provides extensive APIs to allow configuration of rules such as this. However the risk is much lower with managed privileged accounts since Secret Server is setting strong passwords, controlling access and rotating passwords on a regular basis.
3.9.9	Any privileged account management system must be configured to utilize robust backup, recovery and availability methodologies in order to ensure resiliency and availability of the credentials stored within the system as well as the timely recovery of the system in the event of a system failure.	Secret Server supports load-balanced front end application server configurations and back-end database clustering to ensure the highest levels of resiliency and system uptime. Secret Server also supports all standard backup and recovery methods for database backups and application recovery on standard platforms.
3.10	Every privileged user ID established for a non-employee or third party application must have a specified expiration date, with a default expiration of 30 days when the actual expiration date is unknown.	Secret Server provides workflow approval for temporary access. The access is approved by an appropriate manager and the non-employee / third party application can then use the credentials for the approved period of time such as 30 days.
3.11.1	All production applications that require privileged access must use special application accounts that are created specifically for the given application. Applications must never use default administrator accounts.	Application account credentials can be stored in Secret Server and then retrieved through either a push or pull mechanism with various API options. This allows these credentials to be controlled, access to be audited, and also allows these credentials to be rotated on a regular basis. Allowing Secret Server to manage these credentials ensures that they are strong and meet policy requirements.
3.11.2	Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.	Secret Server provides easy APIs that developers can use to remove credentials from their applications and pull them from the vault programmatically at runtime. This allows the credentials to be secured, audited and rotated frequently by Secret Server.
3.11.3	Passwords must never be hard-coded in software developed by or modified by Company workers.	Secret Server provides easy APIs that developers can use to remove credentials from their applications and pull them from the vault programmatically at runtime. This allows the credentials to be secured, audited and rotated frequently by Secret Server.
3.11.4	Test data and accounts used during development and testing must be removed before a production system becomes active.	Secret Server can find test accounts using the Discovery capability and these accounts will then be secured.

<p><b>3.12.1</b></p>	<p>All privileged commands issued on computer and communication systems must be traceable to specific individuals through the use of comprehensive logs.</p>	<p>Using the SSH proxy/jump host, Secret Server intercepts all commands to the target system and records them in the audit trail for the session for that user. These sessions can then be searched by users of Secret Server with the correct role permissions. This ensures that users are accountable for their activity.</p>
<p><b>3.12.2</b></p>	<p>All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs must be securely logged.</p>	<p>Secret Server can control access to all privileged accounts and can monitor activity through alerts, SIEM integration and even video recording of sensitive account usage.</p>
<p><b>3.12.3</b></p>	<p>All logs recording privileged ID activity must be reviewed at least quarterly via periodic management reports.</p>	<p>This can be done in Secret Server through scheduled reports to be sent each quarter and reviewed by the appropriate people.</p>
<p><b>3.12.4</b></p>	<p>All logs recording privileged ID activity must be aggregated into a central log management or Security Information and Event Management (SIEM) tool in order to correlate privileged ID activity to other security events, log entries and related non-privileged ID activity.</p>	<p>Secret Server supports native integration with several SIEM tools and can also output log files in standard CEF or Syslog formats for easy integration into most any log management or SIEM tool.</p>
<p><b>3.12.5</b></p>	<p>In addition to event logging, all activity on privileged accounts must be logged via session and keystroke recording.</p>	<p>Secret Server provides event logging (to a SIEM tool) and can also capture session activity through recording and keystroke logging.</p>

### About Thycotic

Thycotic, a global leader in next-generation IT security solutions, delivers an indispensable, comprehensive Privileged Account Management (PAM) solution to protect your "keys to the kingdom" from cyber-attacks and insider threats. Unlike any other security offering, Thycotic Secret Server assures the protection of privileged accounts while being the fastest to deploy, easiest to use, scalable enterprise-class solution offered at a competitive price. Already securing privileged account access for more than 3,000 organizations worldwide, including Fortune 500 enterprises, Thycotic Secret Server is simply your best value for PAM protection. For more information, please visit [www.thycotic.com](http://www.thycotic.com).

### About Information Shield

Information Shield provides time-saving products and services to help build, update and maintain [information security policies](#). Information Shield's Common Policy Library (CPL) contains over 1600 pre-written information security policy templates covering all aspects of information security. Based in Houston, Texas, Information Shield has over 10,000 satisfied customers in 60 countries. For more policy templates, visit <http://www.informationshield.com>, email [sales\(at\)informationshield\(dot\)com](mailto:sales@informationshield.com) or call 1.888.641.0500.