YOUR LOGO

Privileged Account Management Policy Template

Policy #	Effective Date	Email
##########	DD/MM/YYYY	policycontact@company.com
Version	**Contact**	**Phone**
1.0	Policy Contact	888.555.1212

What is the Privileged Account Management Policy Template?

Delinea designed this template to help you develop security policies for privileged accounts and credentials. You can decide which policies are appropriate for your business and customize them to your needs.

Use this sample policy as a starting point to build a working credential governance policy for your organization. We have divided the template into sections based on common governance areas regarding privileged accounts. You can select from over seventy information security policy statements to match your organization's governance requirements.

About the Policy Template

Privileged accounts present a much greater risk than typical user accounts and thus require a higher level of security controls. To lower risk of privileged account misuse, security policies define how credentials (passwords, keys and secrets) connected to these accounts should be managed.

You can use this sample policy as a starting point to build a privileged access management (PAM) policy for your organization. The template is divided into several sections according to common governance areas regarding privileged accounts. It contains over 40 pre-written information security policy statements you can select from to match your organization's governance requirements.

What are (Privileged) Accounts and Credentials?

For this template, we define the following in general terms:

- **Account**: Used to log in to applications, websites, and computers. It is a collection of personal information such as name, email address, and password.
- **Non-Privileged Account**: An account for non-administrative use by regular users. Grants basic access and privileges to a personal workstation and business productivity applications such as Microsoft Office, Salesforce.com, and Zoom.
- **Privileged Account**: An account granting access and privileges beyond non-privileged accounts. IT admins, contractors, auditors, applications, services, and computers typically use privileged accounts.
- **Credential**: The set of unique identifiers used to verify the user's identity when logging in to the account.

Note that credentials associated with non-privileged accounts are typically passwords only (although MFA is desirable in conjunction to assure the identity of the user), whereas credentials related to privileged accounts may include stronger types such as SSH keys, SSH certificates, API keys, and tokens such as OAuth, JWT, and OpenID Connect. Using stronger credentials for privileged accounts is necessary to ensure the security of sensitive data and systems, as privileged accounts pose more significant risks than non-privileged accounts.

Privileged Account Security

Cybersecurity frameworks and regulations address account and credential security by providing guidelines and best practices to help you protect your systems and data from unauthorized access.

Security is a large domain. This template addresses one security facet – Privileged Access Management (PAM.) Further, it focuses on the subset of PAM that protects access to privileged account passwords and their use to access critical computer systems. The industry often categorizes this as Privileged Account and Session Management (PASM, coined by the analyst firm Gartner.)

Privileged accounts can give an administrator (or threat actor) complete control over computers, applications, and data, while regular user accounts have limited privileges. Thus, privileged accounts are a prime target for cyberattackers and represent a much greater risk requiring specialized security treatment.

PAM security policies govern access to these privileged account credentials. *PAM controls* enforce these policies, lowering the risk of privileged account misuse.

This policy template is valuable because it can help you to:

- **Save time and resources**: Developing security policies from scratch can be time-consuming and resource intensive. Using this template can help you get started quickly and easily.
- **Ensure compliance**: We based this policy template on industry best practices and regulatory requirements. This can help ensure your security policies comply with applicable laws and regulations.
- **Improve security posture**: This template can help you identify and address security risks. You can improve your overall security posture by implementing the policies in this template.

One of the most widely recognized guidelines is the National Institute of Standards and Technology (NIST) password guidelines, considered the gold standard for password security by many experts. For this template, we aggregated policies from the NIST guidelines, plus other international best practices, frameworks, and regulations, such as:

- CIS Critical Security Controls
- European Union (EU) Digital Operational Resilience Act (DORA)
- Australian Prudential Regulation Authority (APRA) Standard CPS 234: Information Security
- Hong Kong Monetary Authority (HKMA) Cyber Security Risk Management Guidelines
- SOC 2
- Federal Information Security Management Act (FISMA)
- New Zealand Information Security Manual (NZISM)
- COBIT 5
- NIST Cybersecurity Framework (CSF)
- Australian Cyber Security Centre (ACSC) Essential Eight
- Singapore Personal Data Protection Act (PDPA)
- General Data Protection Regulation (GDPR)
- Saudi Arabian Monetary Authority (SAMA) Cybersecurity Controls
- EU NIS2 Directive (2022/255)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO/IEC 27001

References

This section references the information security laws and governance frameworks applicable to this PAM Policy. As noted above, Delinea researched privileged account and credential requirements from several common frameworks and regulations.

If you must satisfy a specific one, please visit our Audit & Compliance web page to find whitepapers that map Delinea solutions to the requirements in these frameworks and regulations. Thus, for example, if you must comply with PCI DSS, the mapping whitepaper will explain how Delinea PAM solutions satisfy those requirements.

While this template focuses on a subset of PAM – privileged account and credential management – the other referenced mapping white papers incorporate capabilities from all Delinea products, including DevOps Secrets management, Privilege Control for Servers, and Privilege Control for Workstations.

Customizing the Template

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

To customize this template, perform the following steps:

1. Remove the “About the Policy Template” and “Customizing the Template” instructions, and “Appendix” and other author comments.
2. Replace the term “Company X” with the name of your organization.
3. Add your company logo in the upper left corner and the document header.
4. Update all the company-specific contact information (highlighted in yellow).
5. Update the effective date.
6. Revise policy guidelines to meet your organization’s policies.
7. Revise the Violations section to meet your organization’s policies.
8. Save your changes.
9. Obtain your management and auditors’ approval of the completed policy.
10. Distribute the policy according to your management guidance.

About Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization’s most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. delinea.com

[Company Name] Privileged Account Management Policy

Customizing the Template **3**

References **4**

About Delinea **4**

1.0 Purpose **6**

2.0 Scope **6**

3.0 Policy **6**

3.1 System Approval and Authorization 6

3.2 Password Categorization 6

3.3 Password Composition 7

3.4 Password History and Change Interval 9

3.5 Account Lockout and Compromised Passwords 9

3.6 Acceptable Use of Privileged Accounts 10

3.7 Privileged Account Approval 11

3.8 Privileged Account Construction 11

3.9 Privileged Access Management 12

3.10 Third-Party Privileged Accounts 14

3.11 DevSecOps 15

3.12 Privileged Account Logging 15

3.13 Privileged Account Logging 15

4.0 Violations **16**

5.0 Definitions **17**

7.0 Approval and Ownership **18**

8.0 Revision History **18**

[Company Name] Privileged Account Management Policy

1. Purpose

This policy outlines how Company X manages and secures privileged account passwords for its employees, contractors, and other third parties. It is a vital part of a more extensive set of Company X policies and guidelines to manage and secure its information environment. This policy ensures that privileged account passwords are created, stored, and used securely according to Company X's security requirements.

2. Scope

This policy applies to all staff and contractors responsible for setting up and maintaining privileged accounts related to Company X's electronic information resources. Resources include user workstations, servers, databases, applications, and systems managed on-premise and in the cloud. Several regulations and frameworks, such as NIST CSF, NIST 800-161, GDPR, and PCI DSS, require organizations to ensure their supply chain partners have specific security controls.

3. Policy

3.1. System Approval and Authorization

Default accounts and passwords present one of the most significant risks to IT systems. This section defines specific controls for controlling and managing privileged accounts when you place systems 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 passwords with privileged user IDs not assigned to a specific employee or job role must be changed to large random values. These should be recorded in the PAM solution with appropriate permissions for the administrators responsible for managing these accounts. The PAM solution should support password quality of service policies that allow you to control password effectiveness against guessing and brute-force attacks, measured as a function of length, complexity, and unpredictability.

3.2. Password Categorization

This section defines specific terminology for understanding different categories of passwords, which is helpful for prescribing controls on those passwords. Treating all passwords the same is impractical.

Passwords fall into two categories:

3.2.1. User Account Passwords

A password is typically a word, phrase, or string of characters used to verify the identity of a user during the authentication process. "Secret" data differentiates an authorized user from an unauthorized user. It is usually paired with a username and typically tied to a unique individual, for example, an Active Directory user account.

3.2.2. Privileged Account Passwords

Privileged account passwords provide administrative or specialized access to enterprise systems and sensitive data based on higher permissions. A privileged account can be associated with a human being or non-human entity, such as:

- **Service accounts**, which run application services such as Windows Services, scheduled tasks, batch jobs, and Application Pools within Microsoft Internet Information Services (IIS.)
- **A**pplication accounts used by applications to access databases, run batch jobs, digitally sign software, and used during software development embedded in code, build scripts, and configuration files.
- **System administrator accounts** used to manage and administer computer systems. They are typically for local administration of a single system.
- **Domain administrator accounts used to** manage and administer a domain or network of servers and control Active Directory users and local domain accounts at the workstation level.
- **Root accounts, w**hich are special user accounts in Unix and Linux with unrestricted read and write privileges to all file system areas.

3.3. Password Composition

This section defines specific controls for creating secure passwords for privileged accounts. Passwords for privileged accounts must be more secure than 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:

- It must contain at least one alphabetic, numeric, and symbol character.
- It must be at least eight characters in length.

- Ideally, passphrases should be used to increase length. Increased length provides more security than complexity and is easier for humans to memorize.

For example, if you were told to use six lowercase letters — such as, afzjxd, auntie, secret, wwwwww — the space would contain 266, or 308,915,776, possibilities.

If you were told to select a twelve-character password that can include uppercase and lowercase letters and ten digits and symbols (say, !, @, #, $, %, ^, &, ?, / and +), the size of the possibility space would then be 7212 or 19,408,409,961,765,342,806,016 possibilities. That's more than 62 trillion times the size of the first space.

A computer running through all the possibilities for your 12-character password one by one would take 62 trillion times longer. If your computer spent a second visiting the six-character space, it would have to devote two million years to examining each of the passwords in the 12-character space. The multitude of possibilities makes it impractical for a hacker to carry out a plan of attack that might have been feasible for the six-character space.

3.3.3. Privileged Account Password Complexity

These passwords should be optimized for the maximum lengths of the platform. Random passwords between 80 and 127 characters should be generated for the best security.

The following requirements should be followed for privileged account passwords:

- They must be unique and not reused across multiple accounts.
- The user must be prevented from using passwords that threat actors can easily compromise, such as common words, phrases, and personal information
- Maximize the possible length of password for each platform.
- Passphrases ***should not be used*** to avoid memorization.
- They should have a 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, which must always be checked automatically when 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 and Expiry

User passwords must be changed at least once every 90 days. Users may be required to change passwords, or this may be done automatically. Passwords must be changed if there is any suspicion a threat actor may have compromised them.

3.4.2. User Account Maximum Password Changes

Users must not be permitted to change their password within seven 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 and Expiry

All privileged account passwords must be automatically changed at least once every 90 days, or if there is any suspicion a threat actor may have compromised them. This time interval should be set based on an internal risk assessment for any potential disruption to the business. A domain administrator account, for example, carries very high risk. If compromised, it could result in significant disruption to the business. Such accounts should have their passwords changed often – ideally after every use to reduce exposure to abuse, misuse, or exploits such as Pass-the-Hash attacks. Access to privileged account password reset and change functionality must be restricted to authorized personnel. Administrators can use self-service workflows to request access just-in-time pending approval.

3.4.4. Password History

On all multi-user Company X computers, system 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. This can be valuable, for example, when restoring from a backup after a ransomware attack. If the restore point is before a more recent password change, the history provides access to a valid credential to ensure access.

3.5. Account Lockout and Compromised Passwords

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 directions should be customized based on the organization's requirements.

3.5.1. Maximum Login Attempts

All Company X computer systems that employ fixed passwords at log in must be configured to permit only five attempts to enter a correct password, after which the authenticator is locked or the user ID is deactivated.

3.5.2. Lockout Duration

All accounts disabled for incorrect login attempts must remain inactive for at least 15 minutes.

3.5.3. Lockout Notification

The security team must be notified of all accounts disabled for incorrect login attempts so that anomalies can be investigated.

3.5.4. Password Changes After Privileged User Credential Compromise

If an intruder or another unauthorized user has compromised a privileged user credential, 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 the central PAM system.

3.6. Acceptable Use of Privileged Accounts

Sharing passwords between systems introduces significant risk. A single compromised account password can permit an attacker to move laterally across the network quickly. 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 shared, they are no longer considered a user account since the user's identity is unknown.

3.6.2. Privileged Account Password Sharing

Privileged account passwords should not be shared; each privileged account must have a unique password. Passwords for privileged accounts can be shared among administrators only if controls are in place to know which administrator is using the account at any time. This must include full auditing and non-repudiation mechanisms.

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. PAM solutions that can establish login sessions to servers must be able to use a vaulted credential to authenticate without revealing the password to the administrator.

3.7. Privileged Account Approval

Privileged accounts must be strictly controlled because of the added risk of compromise. The following sections contain controls for account approval, creation, and maintenance.

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. Such passwords should be vaulted and automatically rotated on a frequent schedule or after use. Ideally, administrators should only log in to servers using their enterprise ID and password, with the least privilege and privilege elevation enforced on the server to avoid sharing privileged accounts.

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

One way to reduce confusion and gain oversight is to adopt standards for privileged accounts created by the organization. For the 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 indicate the responsible individual's name.
- Must clearly define the account (i.e., purpose of the account, type of account, etc.)

- Must be managed in a system that can associate a single user account to each use of the privileged account to document accountability for using the privileged ID.

3.8.2. Service Account Governance

User IDs for service and application accounts should also follow the Company X naming convention and requirements outlined in the previous section.

An inventory of service accounts must be established and maintained.

3.8.3. Generic User IDs

User IDs must uniquely identify specific individuals. Generic user IDs based on job function, organizational title or role, descriptive of a project, or anonymous must be avoided wherever possible.

3.8.4. Reuse of User IDs

Each Company X computer user ID must be unique and connected solely with the user to whom it was assigned. It must not be reassigned after a worker, contractor, or customer terminates their relationship with Company X.

3.8.5. Separate System Administrator User IDs

System administrators managing computer systems with multiple users must have two user IDs. One provides the privileges of a regular user for day-to-day work and may be public (e.g., on a business card or email signature.) The other, often known as an "alternate admin" or "dash-a" account, is not public and is exclusively used for privileged server access. Further, this account ID should be cryptic so a threat actor can't derive it from the user's public ID.

3.9. Privileged Access Management

The variety of privileged account types across various systems presents unique management challenges. Modern PAM vaults provide ways to automate privileged account discovery, creation, management, and removal. These systems should be used whenever possible for centralized management to reduce risk and increase visibility.

3.9.1. PAM Password Vault

A centralized PAM vault must manage all privileged accounts on Company X systems. This system must provide an audit trail that tracks additions, changes, and deletions. The system must be the source of truth for all managed credentials, alerting if unsanctioned changes are made outside the system. If the PAM vault has that capability, unsanctioned changes must be manually or automatically corrected.

3.9.2. Privileged Account Discovery and Inventory

Company X must maintain an inventory of all accounts (including alternate admin accounts) with privileged access to production computer systems. The inventory must be

centrally managed via a PAM vault with a continuous privileged account discovery capability.

3.9.3. Account Inventory Update

The privileged account inventory must be updated at least quarterly to identify new or changed accounts.

3.9.4. Emergency Break Glass

Company X system administrators must have access to a PAM vault that temporarily provides access to privileged accounts and passwords (aka break glass or firecall) for emergency access to secure computer systems. The vault must automatically change the password after use or a defined period to prevent reuse, sharing, and standing privileges.

3.9.5. Brokered Server Login

Company X system administrations must have access to a PAM vault to identify a vaulted account and password to log in to a server. The vault must establish the login session on behalf of the user without revealing the account password.

3.9.6. Vaulted Password Encryption

Company X must store vaulted credentials securely to protect their confidentiality and integrity. For example, using hashing and salting or encryption via strong encryption algorithms that meet compliance and/or regulatory requirements.

3.9.7. Integration with Native Directories and Directory Services

Company X's PAM vault must integrate with native operating system account management systems to manage local account passwords (for example, scheduled remote password changing.)

The PAM vault must also integrate with enterprise directory services, such as Active Directory or Azure Active Directory, to permit users to log in to the vault and access vaulted accounts using their enterprise credentials.

3.9.8. Strong Authentication for Identity Assurance

Company X's PAM vault must integrate with strong authentication methods.

Company X must use two-factor authentication to provide an additional layer of security for administrator access to the PAM vault and sensitive vaulted accounts. Users must be challenged to prove their identity (ownership of the account used to log into the vault and access Secrets) via additional factors appropriate for the sensitivity of the Secret. Company X should follow guidelines such as NIST's Authentication Assurance Levels (SP 800-63.)

Challenging for additional factors can be based on contextual factors if the PAM solution enforcing MFA policies supports this. For example, the day of the week, the time of day, location, or risk score derived from a PAM behavioral analytics capability can be used.

3.9.9. Inactive Account Maintenance

All accounts must be created with an expiration date. All inactive accounts over 90 days old must be either removed or disabled.

3.9.10. Disaster Recovery

Any PAM system must be configured to utilize robust backup, recovery, and availability methodologies to ensure resiliency and availability of the credentials stored within the system and the timely recovery of the system in the event of a system failure.

3.9.11. Dedicated Admin Accounts

Per Privileged Account Construction above, the PAM vault should support a secondary (alternate admin) account for administrators managing computer systems.

3.10. Third-Party Privileged Accounts

Company X must manage all privileged accounts since they can give a threat actor elevated rights to access sensitive assets. However, third parties represent potentially greater risk since you do not have as much control over the users or the systems they use. If their identity security is weak, the privileged accounts you give them can be compromised, increasing the risk for you.

3.10.1. Third-Party Federated Login

Company X recommends federated identity protocols such as Security Assertion Markup Language (SAML) for third-party access to Company X's PAM vault. The PAM vault is a critical security platform. SAML improves security by only transferring identity information (no passwords) from the identity provider (IDP), and Company X can revoke third-party user access at any time.

3.10.2. Third-Party User ID Expiration

If federated login is not supported by the third-party, necessitating the creation of a dedicated Company X privileged account, the privileged user ID must have a specified expiration date with a default expiration of 30 days when the actual expiration date is unknown.

3.10.3. Secure Remote Access

If federated login is not supported by the third-party, remote access must use a secure mechanism that does not require VPN access to the network.

3.11. DevSecOps

Privileged accounts pose unique challenges for applications that must authenticate to other applications or operating system services. These accounts are often non-compliant, created ad-hoc, using default passwords, and embedded in code as plaintext where threat actors can discover them. Privileged identity security can be significantly enhanced using a PAM vault for password management or provisioning temporary tokens.

3.11.1. Application Accounts

All development applications and systems requiring privileged access, including DevOps tools, containers, and microservices, must use secure privileged accounts.

3.11.2. Hard-Coded Passwords in Software

Passwords must never be hard-coded in software developed by or modified by Company X workers or contractors. They must be obtained programmatically at run-time from a PAM vault that enforces Company X password policies such as password complexity and rotation.

3.11.3. Ephemeral Tokens

Company X applications and services must use ephemeral tokens such as OAuth instead of static passwords to authenticate other applications and services, wherever practical. Company X should set token expiration to ten seconds or as short as possible. Tokens must be obtained programmatically and in real-time from a secure token service such as a PAM vault.

3.11.4. Third-Party Repositories

Static credentials, such as passwords, used in the application development process must never be stored in remote repositories, such as GitHub. Company X must protect them in a PAM vault that enforces Company X's password policies.

3.11.5. Test Account Removal

Test accounts and permissions used during development and testing must be removed before a production system becomes active.

3.12. Privileged Account Logging

Systems must be designed and configured to log events linked to privileged accounts to provide audit visibility into privileged account use.

3.12.1. Continuous Monitoring and Analysis

Continuously log, monitor, assess, and track privileged activity within Company X's PAM vault, including activity in all server login sessions brokered through the vault. The goal is to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

3.12.2. Privileged Session Monitoring

All privileged activity performed on Company X servers via sessions brokered by a PAM vault must support session monitoring for real-time viewing of session activity.

3.12.3. Privileged Activity Traceability

All privileged activity within Company X's PAM vault and any subsequent vault-brokered login sessions must be traceable to specific individuals using comprehensive logs.

This includes account creation, password checkout, session initiation, and permissions modification. Logging provides traceability and ensures that no user (Company X or third-party) can perform any subversive activity in the guise of a privileged account. The use of shared privileged accounts must be by exception only (and similarly logged) to ensure activity is attributed to a single user.

3.12.4. Privileged User ID Activity Logging

All activity performed by Systems Administrators and others with privileged user IDs, including third-party vendors, must be securely logged, such as rotation, deletion, modification, and vault access permissions.

3.12.5. Privileged User ID Activity Log Review

All logs recording privileged ID activity must be reviewed at least quarterly via periodic management reports.

3.12.6. Privileged User ID Activity Log Correlation

All logs recording privileged ID activity must be aggregated into a central management tool for privileged accounts or a Security Information and Event Management (SIEM) tool to correlate privileged ID activity to other security events, log entries, and related non-privileged ID activity.

3.12.7. Privileged User ID Session Recording

Company X must record all privileged activity for server sessions brokered by a PAM vault. The PAM vault must support session replay and the ability to search for applications run or commands executed by the user.

4. Violations

Any violation of this policy may result in disciplinary action, 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 violating 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. 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 must commonly enter a user ID and a password as an authentication mechanism during the login process.

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

Least privilege – Least privilege prevents "over-privileged access" by users, applications, or services. It helps reduce the risk of exploitation should user credentials be compromised by an outside attacker or malicious insider. Thus, users are granted only enough authority to complete a specific task or job.

Password – An arbitrary string of characters used to authenticate an account when attempting to log on to prevent unauthorized access to the account.

Privileged account – An account that can be a user account on any system with system privileges beyond those of a regular user or an account that does not represent human use. Privileged accounts are typically not assigned to a user but can sometimes be dedicated user accounts with more permissions than a typical user account. Root, local administrator, and domain admin are all examples of privileged accounts with elevated access beyond a regular user's.

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

Third-party – Any non-employee of Company X contractually bound to provide some service to Company X.

User – Any Company X employee or partner authorized to access Company X electronic information resources.

User account – An account that represents a single human user who is the only person ever to use the account and 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. Approval and Ownership

Owner	Title	Date	Signature
<Name>	<Title>	<Date>	<Signature>

Approved By	Title	Date	Signature
<Name>	<Title>	<Date>	<Signature>

7. Revision History

Version	Description	Revision Date	Review Date	Reviewer/ Approver Name
1.0	Initial Version	<Date>	<Date>	<Name>