Elevaite365

Password Management Policy

Version 1.0

PURPOSE

The Password Management Policy defines the rules and guidelines for password management at Elevaite365 (herein referred to as “the Organization”). This policy aims to ensure the Organization’s IT assets and sensitive information security by establishing robust password practices that protect against unauthorized access and disclosure.

SCOPE

This policy applies to the Organization’s IT assets, employees, contractors, and third parties. It applies to all individuals who create and use passwords to access the Organization’s information and IT systems.

DEFINITION

1. **ISG:** Information Security Group
2. **CISO:** Chief Information Security Officer

RESPONSIBILITIES

Information Security Group (ISG) and Chief Information Security Officer (CISO)

1. **Policy Implementation:** Responsible for implementing this policy under the guidance of top management and the DevOps Team.
2. **Administrative Procedures:** Develop and implement procedures for creating, changing, resetting, and communicating initial passwords to all users.
3. **Monitoring and Compliance:** Ensure adherence to the policy and report non-compliance to top management.
4. **Security Oversight:** Oversee the protection of superuser and administrator passwords, ensuring they are managed securely

IT and DevOps Team

1. **Technical Support:** Support password management systems and ensure all IT assets comply with this policy.
2. **Password Management:** Manage the technical aspects of password creation, modification, reset, and protection.
3. **Security Controls Implementation:** Implement and maintain security controls related to password management, including encryption and storage solutions.

POLICY

Password Management Levels

Passwords will be managed at the following levels:

1. **Employees:** This is for accessing email, endpoints, web applications, etc.
2. **System Level:** For root accounts, service accounts, application admin accounts, etc.

All employee-level and system-level passwords must conform to this policy.

Password Creation Requirements

Cloud Infrastructure

1. **Length and Complexity:** Passwords must contain at least 10 Characters , including at least one uppercase letter, one lowercase letter, one number, and one unique character.
2. **Multi-Factor Authentication (MFA):** All users accessing the production environment in the cloud must be enabled.
3. **Uniqueness:** Passwords and user IDs must not be identical.
4. **Exclusion of Personal Information:** Passwords must not contain personal information such as birthdays, names, addresses, or phone numbers.
5. **Guessability:** Passwords must not be easily guessable by third parties or automated software.
6. **Password History:** Any new password must differ from the previous 3 Previous Passwords .
7. **Expiration:** All passwords will expire after 180 Days .

Passwords for Email, End-Points, and Web Applications

1. **Length and Complexity:** Passwords must contain at least 10 Characters , including at least one uppercase letter, one lowercase letter, one number, and one unique character.
2. **Uniqueness:** Passwords and user IDs must not be identical.
3. **Exclusion of Personal Information:** Passwords must not contain personal information such as birthdays, names, addresses, or phone numbers.
4. **Guessability:** Passwords must not be easily guessable by third parties or automated software.
5. **Password History:** Any new password must differ from the previous 3 Previous Passwords .
6. **Expiration:** All passwords will expire after 180 Days.

Password Modification

1. **User-Initiated Changes:** Following this policy, users may modify or change their passwords using the password change option provided within the system.

Password Reset

1. **Forgotten Passwords:** The IT Head will initiate a password reset through email or phone verification if a user cannot remember a password.
2. **Reset Process:** The CISO or ISG will reset the password to a predefined default password and prompt the user to change the password upon first login.
3. **Record-Keeping:** Records of password resets performed by the CISO or ISG will be maintained for accountability.

Password Protection

1. **Initial Password Change:** Default passwords set during employee onboarding must be changed at first login.
2. **Single Password Usage:** Avoid using a single password to access multiple organizational information systems (e.g., Active Directory).
3. **Secure Communication:** Do not send user IDs and passwords via email or SMS in clear text.
4. **Password Confidentiality:** Do not reveal passwords to anyone verbally, in person, over the phone, or through Internet messenger services.
5. **Encryption:** Encrypt passwords when stored in files or databases or transmitted over the Internet, public networks, or wireless devices. Where encryption is impossible, restrict access to such files and databases.
6. **Password Format Confidentiality:** Do not disclose the format of a password without authorization.
7. **Non-Disclosure:** Do not reveal passwords on questionnaires or security forms.
8. **Personal Sharing:** Do not share passwords with family members or co-workers.
9. **Avoid “Remember Password”:** Do not use the “Remember Password” feature if available.
10. **Password Managers:** Use approved password managers to secure and manage passwords.
11. **Session Management:** Administrative users with extended rights must log out when leaving their system for extended periods.
12. **Immediate Change on Compromise:** If an account or password is suspected to be compromised, change the password immediately.

Protection of Superuser Password / Administrator Password

1. **Password Management:** All superuser and administrator passwords for critical servers and devices must be secured using a password manager with a personal vault.
2. **Immediate Change on Termination:** If a user with an administrator or superuser password resigns or has their contract terminated, change the password immediately and store it securely by the ISG. Revoke access as per the Access Control Policy.

Termination of Employee Relationship

1. **IT Department Users:** Change all passwords and user IDs immediately upon termination.
2. **Other Users:** Disable and remove relevant accounts.
3. **Account Maintenance:** If an account must be maintained post-termination, the department head must request keeping the ID active and changing the password. The department head will designate who manages the new password.

User Responsibilities

1. **Unique Passwords:** Do not use your user ID as your password.
2. **No Sharing:** Do not share your password with anyone, including administrative assistants or secretaries.
3. **Confidentiality:** Treat all passwords as sensitive and confidential.

4. **Secure Communication:** Do not reveal passwords over the phone, in email messages, to managers, or in any other form of communication.
5. **Discretion:** Do not discuss passwords or mention the password format in front of others.
6. **Secure Storage:** Do not write passwords or store them in unencrypted files or systems.
7. **Password Managers:** Use approved password managers and do not share them with anyone.
8. **Session Security:** Log out of systems when leaving them unattended for extended periods.
9. **Immediate Reporting:** If an account or password is compromised, report the incident to the ISG and change the password immediately.

Application Development Standards

Application developers must ensure their programs include the following security measures:

1. **Individual Authentication:** Applications must support the authentication of individual users, not groups.
2. **Secure Password Storage:** Applications must not store passwords in clear text or any easily reversible form.
3. **Role-Based Access Management:** Implement role-based access controls to ensure one user cannot assume another's functions without authorization.
4. **Integration with OAuth and SSO:** Where applicable, integrate OAuth and Single Sign-On (SSO) mechanisms to enhance authentication security.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan