P2010 - Password Protection Policy

Contents

Purpose:

The purpose of this policy is to establish a standard for creation of strong passphrases/passwords and the protection of those authentication methods.

Scope:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password or passphrase) on any system that resides at any Integrity, LLC ("Integrity") facility, has access to the Integrity network, or stores any non-public Integrity information.

Statement:

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy. In addition, the Security Governance Committee is responsible for ensuring vulnerability management practices are in place and conducted on a regular basis in accordance with this policy.

Business Owners: Business Owners are responsible for understanding and serving as the point-of contact for, specific assets within Integrity's technological environment.

Integrity IT: The Integrity IT Team is responsible for threat intelligence gathering and dissemination efforts, including the monitoring of global services and forums that provide updates on prominent and growing security threats. The Integrity IT Team is also responsible for vulnerability management efforts, including vulnerability scanning, criticality assessment, and patch management. Integrity IT will serve in a role that ensures facilitation and collaboration amongst all Integrity Marketing Group teams.

Business Unit IT: The Business Unit IT Teams are responsible for remediation of vulnerabilities on systems for which they are responsible.

Contractors and Third Parties: All contractors and third-party vendors are responsible for notifying Integrity of any vulnerabilities in their products when they are discovered. As applicable, they are also responsible for providing patches for identified vulnerabilities in their devices/software, including support for necessary operating system upgrades.

Policy Statement

Passphrase Usage

Where technically feasible, passphrases shall be utilized in place of traditional passwords. The use of passphrases aligns with recommendations of the NIST Cybersecurity Framework 2.0, which advocates for stronger and more user-friendly authentication methods. A passphrase is defined as a sequence of words or other text used to control access to a computer system, program, or data. It is typically longer than a traditional password for added security. When utilizing

passphrases, the following requirements are to be enforced:

- Minimum Length: All passphrases must be a minimum of fourteen (14) characters in length, encouraging the use of sentences or phrases that are easy to remember but hard to guess.
- Complexity: Passphrases shall contain a mix of upper- and lower-case letters, numbers, and special characters to increase their complexity and resistance to brute-force attacks.
- Unpredictability: Common phrases, famous quotations, or sequences of words from published literature must not be used. Each passphrase shall be unique and not easily deducible.
- Memorability: Users are encouraged to create passphrases that are meaningful and memorable to them to reduce the likelihood of needing to write them down.
- Change Frequency: Passphrases shall be changed at least once every 12 months, or sooner if there is a suspicion of compromise.
- Prohibited Use: Sharing of passphrases is strictly prohibited. If a passphrase must be shared for business reasons, it shall be done through secure means and changed immediately afterward.

Password Usage

All user-level and system-level passwords must conform to the Identity and Access Management Policy. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it required for all active accounts that some form of multi-factor authentication is used for any privileged accounts.

Password Length / Composition

Passwords must be a minimum of fourteen (14) characters consisting of at least three of the following character sets:

- Upper-case letters (e.g., A, B, C, ...Z)
- Lower-case letters (e.g., a, b, c, ...z)
- Numerals (e.g., 1, 1, 2, ...9)
- Special characters (e.g.,?,!, %,$,#, etc.)

Authentication systems must also enforce:

- Minimum of four (4) changed characters when new passwords are created.
- Users must not be able to construct passwords that are identical passwords they have previously employed in the last six (6) times they have changed their password.
- Privileged User, super user, or administrator passwords must have a minimum length of fifteen (15) characters.
- Service Accounts (application or system passwords) must have a minimum length of twenty (20) characters.

Failed Login Attempts

Integrity must configure information systems to lock out user accounts automatically (where feasible) whether the login occurs via a local or network connection. After a maximum of five (5) failed log-on attempts, the system must lock out the account for a period that persists for a minimum of fifteen (15) minutes.

Automatic Logoff / Timeout

Information must be enabled to automatically timeout the session after a maximum period of time. Re-establishment of the session must take place only after the user has provided a valid password. The following guidelines must be followed:

- Server: Twenty (20) Minutes
- Workstation: Thirty (30) Minutes

Users must not leave any Company information system unattended that contains Company information or is connected to a Company network, and must logoff or activate a screen saver program if the information system in not used for a period of:

- General Users: Sixty (60) minutes
- Administrative Users: Fifteen (15) minutes

Password Change

Passwords shall be changed every 180 days or when there is reason to believe a password has been compromised.

Password cracking or guessing shall be performed on a periodic or random basis by the Cybersecurity Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Identity and Access Management Policy.

Passwords that have been identified as compromised will be subject to a password hash comparison.

Password Protection

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Integrity Marketing Group information.

Passwords must not be inserted into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.

Passwords shall be stored only in “password managers” authorized by the Integrity Cybersecurity team. Passwords must be stored using one way encryption or hashing (i.e., a password cannot be decrypted into clear text) to prevent their exposure to password cracking utilities. Passwords must never be written down or stored on information systems in an unprotected form. Users must not hard code any usernames/passwords in scripts or clear text files such as system shell scripts, batch jobs, or word processing documents.

Any user suspecting that his/her password shall have been compromised must report the incident to Integrity Cybersecurity and change all passwords.

Password Resets

It is the responsibility of the access control authority, whether it is the Product Owner, Development Owner, or Help Desk, to verify the identity and access level of the user requesting the reset, prior to the reset being performed. Passwords and User IDs must not be transmitted within the same electronic media (email) unless the message is encrypted.

Temporary passwords that are provided to users who maintain their own passwords must:

- Be unique to each individual and not be easily guessable; meet password complexity requirements.

- Expire upon initial use and require users to create a new one.
- Follow established procedures for verifying the identity of the user prior to providing them with the temporary password.
- Be distributed to the user in a secure manner and never be sent in clear text.

Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords/passphrases in clear text or in any easily reversible form.
- Applications must not transmit passwords/passphrases in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password/passphrase.

Multi-Factor Authentication

Multi-factor authentication is required for all active accounts and shall be used whenever possible.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Related Procedure References:

Related Regulatory Information:

P2010 - Password Protection Policy		
Document Author	**Name:** **Title:** **Email:**	Jeremy Hart Asureti - Manager jeremy.hart@asureti.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matthew Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 10/21/2025
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan McQueen Assistant General Counsel duncan.mcqueen@integrity.com 1/16/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 1/21/2026

Last Published Date: 1/21/2026

Document Version Number 3.0