# Password and Authentication Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Standard is to provide the requirements for the proper authentication necessary to access Alight information assets. Additionally, this Standard outlines how Alight limits access to authorized users only and prevents unauthorized access to information systems via authentication and password controls.

## Standard Statements

### Password Standard

* 1. Each account which accesses an Alight resource must require a password.
     1. Passwords on new accounts:
     2. Must be unique.
     3. Must expire upon first login.
  2. Must require an immediate password change.
  3. All default system and application passwords must be changed prior to any network connection.
  4. Authentication credentials such as passwords and tokens must not be used by anyone other than the User to whom they are assigned.
  5. Passwords must conform to the following criteria, with native system enforcement when possible:
     1. Passwords for user accounts must be a minimum of eight (8) characters long. Where supported by the system, passwords for non-interactive Functional accounts (Non Human Accounts) must be a minimum of twenty (20) characters long in order to provide additional protection because passwords for these types of accounts may not be changed periodically (for example, the system creates a password only when the account is created). See Access Control & Authorization Standard, Appendix I for an example.
     2. Passwords must contain at least three (3) of the following four (4) complexity rules:
        1. Upper case alphabets
        2. Lower case alphabets
        3. Numbers
        4. Symbols
  6. Passwords must be changed no longer than every 13 weeks (91 days).
  7. Passwords for IDs of interactive accounts that have been approved for non-expiring passwords must be changed every year. They must be changed immediately when any of the following conditions occur:
     1. Where there is a belief that the password has been compromised.
     2. Upon termination of employment of an asset owner or custodian.
     3. When an asset owner or custodian is reassigned or transferred to another position within the organization and, as a result, relinquishes responsibility of the asset.
  8. Unsuccessful logon attempts must be restricted by locking out the user account after ten (10) unsuccessful logon attempts.
  9. In order to prevent a user from “cycling” through passwords:
     1. A user must not use a previously used password for a period of twelve (12) months.
  10. All passwords must be immediately changed if known or suspected of being disclosed.
  11. Password resets must only be performed by authorized individuals.
  12. User identity must be verified before performing password resets.
  13. Passwords must not be stored in clear text in an application, script, or file and must be protected using approved hashing/encryption solutions (see Encryption Standard).

### Secure Logon

* 1. Display a general notice warning that the computer must only be accessed by authorized users.
  2. Prohibit the display of passwords when being keyed.
  3. Do not provide help messages during logon procedures that would aid an unauthorized user.
  4. Validate the logon information only on completion of all input data.
  5. Do not indicate which part of the data is correct or incorrect in the event of a logon error.
  6. Depending on the sensitivity of the data within the system, minimum lockout duration must be set to between 5 and 30 minutes. Global Security Services (GSS) approval is required to disable auto-lockout after 10 failed attempts.

### Authentication

* 1. Authentication credentials, such as identifiers IDs and passwords:
     1. Must not be shared.
     2. Must not be written down or stored in readable form.
     3. Must not be used in automatic login scripts, software, source code, macros, terminal function keys, in computers without access control, shortcuts, or in other locations where unauthorized persons might discover them.
  2. Authentication data (e.g., passwords) must be stored in a cryptographically hashed format (see Encryption Standard).
  3. Authentication data transmitted to any system must be encrypted.
  4. Establishing trust through use of IP address or DNS name as an authenticating credential is unacceptable for any situations where accountability is required or where data classified as HBI or MBI based on the Data Security Classification Standard is to be protected.

### Trusted Systems

* 1. The following standards apply to unattended systems and domain controllers that require trust:
     1. Systems that are not controlled by Alight must never be granted trust relationships with systems that are controlled by Alight.
     2. The more trusted system must initiate communication with the less trusted system.
     3. Windows domain controllers at Alight must not trust non-Alight domain controllers.

### Two-Factor Authentication

* 1. Two-factor authentication solutions must be approved by Global Security Services (GSS) prior to deployment.
  2. Multiple single-factor authentications must not be used in place of two-factor authentication.
  3. Two-factor authentication solutions must be deployed for direct access to Alight systems from untrusted environments.

## References and Mandates

* None

## Legal Conflicts

Alight Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard of Alight shall take precedence over the more general provisions contained in Alight’s Security Policies and Standards.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | 201.02 Password & Authentication Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@Aon.com](mailto:global.security.services@Aon.com) |
| Version Number | 1.7 |
| Owner | Alight Global Security Services | Information Security |
| Author(s) | Alight Global Security Services | Information Security |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 2, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 March | Original | Restructured due to Aon Hewitt merger |
| 1.1 | 2012 September | Update | 13.1 Changed Nominal rating to Low and set remediation SLA no longer than 90 days |
| 1.2 | 2013 June | 2013 Annual Review | Reviewed and validated  1.5, 1.7, 1.8, 1.10, 1.11, 1.12, 2.6, 4.1.3: Changed should to must  1.7: clarified password changes for accounts with non-expiring passwords. |
| 1.3 | 2014 June | 2014 Annual Review | Reviewed and validated  1.7: Added statement to indicate that passwords must be changed immediately. |
| 1.4 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.5 | 2016 July | Update | Invalid Login Attempt value change to 10. |
| 1.6 | 2016 July | 2016 Annual Review | Clarified wording and replaced all instances of IRSS with Global Security Services (GSS) to reflect new organization name |
| 1.7 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |