# Access Control & Authorization Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Standard is to provide the requirements for the proper identification and authorization controls necessary to access Alight information assets. Additionally, the Standard outlines how Alight limits access to only authorized users and prevents unauthorized access to information systems. Alight has designed the Standard to control the allocation of access rights to Alight’s IT infrastructure and services.

## Standard Statements

### Access Control

* 1. User Responsibility
     1. All account passwords must follow the Alight Password and Authentication Standard.
     2. Each user is responsible for all activity and transactions done with their account and password.
     3. Users must report any misuse of accounts or any suspicious activity they become aware of.
     4. Users must choose accounts and passwords for non-Alight systems that are different from those used on Alight systems in order to protect Alight systems from unauthorized access.
     5. Inappropriate uses of access, information resources, and/or privileges are not permitted. Examples (not all inclusive) are below:
        1. Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
        2. Disclosing or removing HBI or MBI information as defined in the Data Security Classification Standard to which you have been entrusted under your account without the explicit permission of the owner, except when so authorized as a system administrator.
        3. Using computing facilities, computer accounts, or computer data for purposes other than those for which they were intended or authorized.
        4. Reading data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission, except when so authorized as a system administrator.

## Administration and Authorization

* 1. Alight colleague accounts must be uniquely identified to the user.
  2. Access requests must be processed by an operational staff following a defined process with appropriate approvals and all components of the request must be kept for at least 13 months.
  3. User access to information should be based on the confidentiality classification of the information asset.
  4. Alight must restrict all access to information, networks, services, utilities, applications, and systems based on:
     1. A business “need-to-know”.
     2. The principle of least privilege.
     3. Access required in order to perform job responsibilities.
  5. Access to information assets must be limited to only those individuals or software programs that have been granted access rights.
  6. Application-level access control tables and profiles (the lists maintained within a computer application that contain access authorizations) must be required to be protected against unauthorized access. System administrators must be the only personnel with access to these functions.
  7. System owners must ensure that standard naming conventions are used and that developers conform to these conventions.
  8. Group and World writeable privileges must be generally restricted in order to reduce data integrity exposure.
  9. An account owner is permitted to delegate their access authority to another authorized user on systems which support secure delegation.
  10. Access to HBI or MBI data as defined in the Data Security Classification Standard must be reviewed and approved by the data owner at least every quarter.
  11. System administrators must be notified when a user changes jobs or roles so that privileges and authorization to resources are appropriately re-aligned to meet the needs of the new role.
      1. Administrators must remove access to systems that are no longer required for the new position.
      2. Management must authorize and approve the new privileges.

## Account Standards

The purpose of this section is to define standards on specific types of accounts.

#### User Accounts

* 1. User Accounts provide individual accountability and are assigned to and used only by Alight Colleagues.
     1. Alight Colleague User Accounts must not be embedded in applications.
  2. Test Accounts
     1. Test accounts must be uniquely associated to authorized, known users who will be conducting the tests.
     2. The same test accounts must not be shared by multiple users.
     3. Test accounts must be configured to automatically expire at the completion of testing.
     4. Remote Access Accounts must follow the Alight approved provisioning process.
  3. Non-Alight Colleague Accounts
     1. Non-Alight colleagues working on the Alight network are required to have accounts that belong to a non-Alight colleague group.
     2. Non-Alight colleagues also must have accounts that automatically expire when the engagement is expected to finish.
  4. "Administrator", "Supervisor", "Root", "Superuser" Accounts Privileges
     1. Administrative access must be limited to only those users that explicitly require privileged access.
     2. Users with administrative responsibilities must use their privileged account only when performing actions that require an elevated privilege level.
     3. Administrative access must be configured to:
        1. Permit only the required administrative roles and responsibilities.
        2. Minimize the number of individuals with full administrative access.
     4. Administrative access must be validated every 3 months to ensure the assigned access privileges are still required and appropriate.
     5. Users granted privileged access must be assigned a different account name rather than using their standard Alight Colleague user account.
     6. Highly privileged accounts must only login to a system using a secure transport mechanism such as SSH or SSL.

#### Functional Accounts

* 1. Functional accounts are not set up for a specific person, but can be shared only among a very limited number of authorized operations staff as long as any use of the account can be tied back to the individual that used it. The owner of an account will be responsible for all activity associated with that account. See 3.5.6.
     1. Functional accounts must have no more access to Alight systems than required.
     2. Functional account access must be clearly logged in order that all functional account use can be traced back to the entity authorized to use the account.
     3. Functional account credentials may be shared only with operations teams that manage applications.
     4. Functional account credentials must not be shared with Alight colleagues in application development roles or doing application development tasks.
     5. If an Alight colleague who has a Functional account leaves the firm and/or changes roles, the Functional account password must be changed promptly.
     6. System/Functional accounts cannot be used interactively unless a mechanism such as sudo or RunAs is implemented to enable all work to be traced back to the individual Alight colleague that used the account.
     7. Non-interactive Functional accounts do not require periodic password changes because the passwords are only known to the system and/or are very long and complex.
  2. Training or Guest Accounts
     1. If a Training or Guest account is required for a legitimate business need, it is permitted only with the "least access" principle and must be disabled or removed when no longer needed.
  3. Application Accounts
     1. Application accounts must only be authorized the level of access to information assets that is required to meet an approved business need or perform prescribed application functions.
  4. Emergency Administrator Accounts
     1. The Emergency Administrator account must be developed for all applicable platforms as required.
     2. This account along with its associated password must be stored in a secure location and must be checked out as required.
     3. Privileged access may be temporarily delegated to support production issues. In such instances:
        1. Access must be revoked immediately when access is no longer required;
        2. All activity must be monitored.
  5. System Accounts are a type of functional account that are delivered with or part of the installation of the system/application and are used to run system services and processes or to run jobs on the system. These accounts can only be shared among a very limited number of authorized operations staff as long the use of the account can be tied back to the individual that used it.
     1. System Default Accounts
        1. System Default Accounts are not permitted and must be disabled or deleted, except if required for a valid system function.
        2. If the account cannot be deleted, then the default password must be changed to comply with the Alight Password and Authentication Standard.

See [Appendix I](#_Appendix_I_1) for examples of user accounts.

## Account Management

* 1. Control and maintain a record of the approval, denial, addition, modification, revocation, and deletion of all accounts, credentials, and other identifier objects.
  2. Minimize the use of interactive accounts which cannot be traced to an individual during use.
  3. Require approval from the information or system owner prior to granting access.
  4. Always adhere to the Alight Password and Authentication Standard.
  5. Communicate initial and reset passwords in a secure fashion.
  6. Verify a user’s identity prior to resetting or unlocking accounts.
  7. Require users to change passwords on first login and password reset.
  8. Employ at least one of the following access control methods to authenticate all users:
     1. Strong passwords
     2. Multi-factor authentication
  9. Disable after 90 days of inactivity on a user’s primary account.

## Termination/Transfer

* 1. When someone is no longer working for Alight (terminated, voluntary departure, contract termination, etc.), all accounts assigned to that individual must be either disabled or revoked as follows:
     1. For accounts where user access provisioning is automated (i.e., centrally-managed, directory-enabled), accounts must be disabled or revoked within 1 business day of the termination notice to the equivalent HR system.
     2. For accounts where user access provisioning is manual (not automated), accounts must be disabled or revoked per the application or infrastructure business process. The account disablement/revocation process must be executed as expeditiously as possible, ideally within 3 business days of the termination notice to PeopleSoft or the equivalent system.
     3. Disabling or revoking accounts means that the accounts must have all access removed from systems.
     4. All user accounts of terminated users must be removed from Alight system(s) within 3 months of the termination date. (This also applies to third-parties, temporary workers and contractors who no longer need access to Alight systems).
  2. Upon transfer, user system access must be modified to provide only the access needed for their job responsibilities.  All other access must be removed.
  3. Every 6 months review inactive accounts to validate, revoke, modify, or remove access as appropriate.

## Segregation of Duties

* 1. Segregation of duties must be implemented for all HBI or MBI information as defined in the Data Security Classification Standard or systems that have regulatory implications to ensure that no single person is in a position to introduce fraudulent or malicious code or data without detection.
  2. Manual or automated role based access control must be implemented to ensure segregation of duties is enforced.
  3. Appropriate implementation of segregation of duties requires:
     1. The process used to ensure a person's authorization rights in the system are appropriate with their role in the organization.
     2. Alight approved authentication mechanism.
     3. Review of audit logs to ensure no circumvention of access has occurred.
     4. An auditable change management process.
  4. Strict control of software and data changes must require that the same person or organizations performs only one of the following roles:
     1. Identification of a requirement or change management request (Business function).
     2. Authorization and approval (Governance function).
     3. Design and development (Architect or Developer function).
     4. Review, inspect, and approval (another Architect or Developer function).
     5. Implementation in production (System Administrator function).

## 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 Security Policies and Standards.

## Appendix I

Examples of user accounts are illustrated below:

|  |  |  |  |
| --- | --- | --- | --- |
| Type of Account | Account | Description | Applicable Standard |
| Functional account | Oracle | Application Account | 3.5 |
| Functional account | Administrator | System Account | 3.5 |
| User account | A24589 | Alight Colleague User Account | 3.1 |
| Functional account | TRCONT19 | Training Account | 3.5 |
| Functional account | PSoft | Application Account | 3.5 |
| Functional account | GB00001 | System Account | 3.5 |
| Functional account | IUSER\_machinename | System Account | 3.5 |
| User account | A36790Test | Test Account | 3.2 |
|  |  |  |  |

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_201.01 Access Control and Authorization Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@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 | 3.5 Clarified functional accounts  3.5.2, 3.5.3, 3.5.4 updated language to improve clarity  3.5.6 moved to Password Standard  3.5.7 Revised  3.5.8 from the original document was merged into 3.5.7  3.5.8 Added statement about non-interactive functional accounts password changes  3.5.9 Removed service account description since functional accounts now replace service accounts  3.9 Clarified system accounts  5.1 and 5.1.1 Clarified terminology  Appendix added IUSER\_machinename as an example of a system account |
| 1.2 | 2012 November | Update | 5.1 Termination/Transfer section revised |
| 1.3 | 2013 June | 2013 Annual Review | Reviewed and validated |
| 1.4 | 2014 June | 2014 Annual Review | Reviewed and validated  2.5, 3.4.1, 3.4.2, 3.4.6, 3.5.1, 3.7.1 changed should to must. |
| 1.5 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.6 | 2016 July | 2016 Annual Review | Changed 3.4.4 Administrative access must be validated every 3 months; changed 3.5 the owner of an account will be responsible for all activity associated with that account; changed 4.9 Disable after 90 days of inactivity on a user’s primary account; 5.1.1 changed PeopleSoft to HR |
| 1.7 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |