# Asset and Data Protection Policy

## Purpose

The purpose of the Asset and Data Protection Policy is to ensure the integrity, confidentiality, and availability of Alight’s information systems, data, and resources. Alight recognizes the importance of information security in maintaining the trust of our stakeholders, including shareholders, clients, colleagues, suppliers, and business partners. To help achieve this goal and support the Global Information Security Policy, the Asset and Data Protection Policy sets forth Alight’s commitment to protecting Alight and client information assets.

## Scope

The scope of this Policy is global, which includes all business units, all regions, and all entities of Hewitt Associates LLC (“Alight”). Alight refers to all wholly-owned subsidiaries of Hewitt Associates LLC, all subsidiaries in which Hewitt Associates LLC has a controlling interest, and all agents or authorized representatives of Hewitt Associates LLC or its subsidiaries.

## Applicable Audience

This Policy applies to all colleagues, contractors, and vendors of Alight. The term "colleagues" refers to all full-time employees, part-time employees, temporary employees, and interns who provide services to Alight. The term “contractor” refers to any individual on another company’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.) who provides services to Alight. The term “vendor” refers to all other third parties with which Alight does business.

## Compliance & Enforcement

Compliance with this Policy is mandatory.

Potential violations of this policy are subject to review and investigation by Alight and/or its agents. Violations of this policy may result in discipline, up to and including removal of assignment, end of contract for vendors, or termination. This is subject to the procedural requirements of the countries in which Alight operates. Alight reserves the right to refer for prosecution any violations of this policy.

This Policy constitutes the current Policy with respect to its subject matter, and it supersedes and replaces all previous policies relating to its subject matter. Alight reserves the right to modify the Policy at its sole discretion at any time with the intent to update on an annual basis.

## Policy Statements

### Access Control and Authorization

* 1. All Alight Information assets must be protected against unauthorized use or disclosure.
  2. Business requirements for access control with respect to each Information System and Service must be defined and documented.
  3. Proper identification and authentication credentials are required.
  4. Authorization for access to information assets must be:
     1. Based on the Data Security Classification Standard.
     2. Defined to provide only the level of access required to meet an approved business need or perform prescribed job responsibilities.
     3. Follow the principle of least privilege.

### Password Management

* 1. Password management systems must be in place to protect information assets based on business requirements and the classification of information being accessed, processed, or stored.
  2. Users must adhere to established password standards in the selection and use of passwords in order to minimize the risks of unauthorized access to information systems.

### Encryption of data

* 1. Encryption must be used to protect Alight’s information assets based on business requirements and the Data Security Classification Standard.
  2. Only Alight approved encryption algorithms, technologies, and products will be used to protect Alight information. Please refer to the Encryption Standard for approved encryption solutions.
  3. Encryption must be used to protect Alight information that will be transmitted over non-secure or public networks.
  4. Encryption must be used to protect Alight information that will be stored, in accordance with the Data Security Classification Standard.

### Integrity Protection

* 1. Information assets must be created and maintained with appropriate controls to ensure that the information is correct, unaltered, auditable, and reproducible.

### Platform Configuration

* 1. All computing infrastructure components must be designed, configured, and maintained to comply with Alight’s Global Information Security policies and standards.
  2. All computing infrastructure components must be configured and maintained in accordance with documented and approved global or regional minimum baseline security standards.
  3. Where no minimum baseline security standard exists:
     1. Alight Global Information Security policies and standards must be followed.
     2. The Center for Internet Security (CIS) standards will provide security configuration reference.
     3. The configuration must be documented and approved by Information Global Security Services (GGSS).
  4. All applications must be designed, configured and maintained in accordance with an approved global or regional baseline security standard.
  5. All Information assets must be protected from destructive software elements such as viruses and malicious code that impair normal operations.

### Mobile Device

* 1. Only Alight approved, authorized, and supported mobile computing devices will be permitted to connect to Alight’s corporate network and / or handle, store or transmit Alight data.
  2. All mobile computing devices must be in designed, configured, and maintained to comply with Alight’s Global Information Security policies and standards.
  3. All mobile computing devices must be configured and maintained in accordance with the documented and approved global or regional minimum baseline security standards.

### Outbound Internet Access

* 1. All network infrastructure components must be designed, configured, and maintained to comply with Alight’s Global Information Security policies and standards.
  2. All network infrastructure components must be configured and maintained in accordance with documented and approved global or regional minimum baseline security standards.
  3. Where no minimum baseline security standard exists:
     1. Alight Global Information Security policies and standards must be followed.
     2. The Center for Internet Security (CIS) standards will provide security configuration reference.
     3. The configuration must be documented and approved by GSS.
  4. Security controls must be implemented to protect networks and all exchanges of data transmitted, whether within Alight operated infrastructure or connecting to or through third party infrastructure.

### Internet Hosting & DMZ

* 1. All network infrastructure components must be designed, configured, and maintained to comply with Alight’s Global Information Security policies and standards.
  2. All network infrastructure components must be configured and maintained in accordance with documented and approved global or regional minimum baseline security standards.
  3. Where no minimum baseline security standard exists:
     1. Alight Global Information Security policies and standards must be followed.
     2. The Center for Internet Security (CIS) standards will provide security configuration reference.
     3. The configuration must be documented and approved by GSS.
  4. Foundational Technology Services (FTS) and GSS will jointly implement a secured “De-Militarized Zone” (DMZ) architecture to protect all network and infrastructure components.

### Remote Access

* 1. Alight will implement remote access solutions based on the Remote Access Standard.
  2. Only approved and authorized devices will be permitted to connect to the Alight remote access solution.
  3. Authorization for remote access to information assets must only be provided to meet an approved business need or perform prescribed job responsibilities.
  4. The Alight remote access solution will require an approved two-factor authentication solution for users to gain access to the Alight corporate network.

### Logging and Monitoring

* 1. Logging must be configured to record security events as appropriate based on the function of the infrastructure system and the information stored, processed, or transmitted.
  2. Audit logs must be securely maintained in accordance with the Logging and Monitoring Standard and retained in accordance with the records retention schedule.
  3. Procedures must be established by Foundational Technology Services (FTS) for reviewing and monitoring log files in accordance with the Logging and Monitoring standard.

### Network Security Infrastructure

* 1. Alight will use the principle of defense-in-depth for the design and implementation of the Alight network infrastructure.
  2. All networks within Alight will be explicitly documented and schematics drawn to provide accurate security assessment and audit capabilities.
  3. All changes to the network security posture of Alight must be approved by the GSS group.
  4. All unknown and/or unapproved devices are prohibited from accessing network resources. Such devices will be immediately disconnected and subjected to the normal review and approval process.
  5. Capacity plan/storage space and storage retention requirements will be established by Foundational Technology Services (FTS) in conjunction with GSS.

## Applicable Standards

* 100.01 Data Security Classification Standard
* 100.02 Data Destruction Standard
* 201.01 Access Control and Authorization Standard
* 201.02 Password and Authentication Standard
* 201.03 Encryption Standard
* 201.05 Platform Configuration Standard
* 201.07 Outbound Internet Access Standard
* 201.08 Internet Hosting and DMZ Standard
* 201.09 Remote Access Standard
* 201.10 Logging and Monitoring Standard
* 201.11 Network Security Infrastructure Standard
* 201.12 Wireless Network Security Standard

## 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.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact Alight Global Security Services at [global.security.services@aon.com](mailto:global.security.services@aon.com) for further guidance.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.5 |
| 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 | 2013 June | 2013 Annual Review | Reviewed and validated |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.4 | 2016 July | 2016 Annual Review | Wording changes including organization change to Global Security Service (GSS) and Foundational Technology Services; update wording reference to Data Security Classification Standard |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |