# Global Information Security Policy

## Table of Contents

[Purpose 4](#_Toc488327664)

[Scope 4](#_Toc488327665)

[Applicable Audience 4](#_Toc488327666)

[Compliance & Enforcement 4](#_Toc488327667)

[Introduction 5](#_Toc488327668)

[Mission Statement 6](#_Toc488327669)

[Objectives 6](#_Toc488327670)

[Structure 6](#_Toc488327671)

[Roles and Responsibilities 8](#_Toc488327672)

[All colleague responsibilities 8](#_Toc488327673)

[Global Security Services responsibilities 8](#_Toc488327674)

[Corporate Risk owner responsibilities 8](#_Toc488327675)

[Data owner responsibilities 9](#_Toc488327676)

[Chief Security Officer responsibilities 9](#_Toc488327677)

[Chief Information Security Officer responsibilities 9](#_Toc488327678)

[Policy Statements 10](#_Toc488327679)

[1. General 10](#_Toc488327680)

[2. Policy Governance 10](#_Toc488327681)

[3. 100.01 Data Security Classification Standard 10](#_Toc488327682)

[4. 201.00 Asset and Data Protection Policy 11](#_Toc488327683)

[5. 202.00 Vulnerability and Compliance Management Policy 11](#_Toc488327684)

[6. 203.00 Application Security Policy 11](#_Toc488327685)

[7. 204.00 Mobile Device Policy 12](#_Toc488327686)

[8. 208.00 Incident Response Policy 12](#_Toc488327687)

[9. 209.00 Information Security Awareness Policy 12](#_Toc488327688)

[10. Change Management 13](#_Toc488327689)

[Applicable Standards 13](#_Toc488327690)

[References and Mandates 14](#_Toc488327691)

[Legal Conflicts 14](#_Toc488327692)

[Exceptions 14](#_Toc488327693)

[Document Control Information 15](#_Toc488327694)

[Revision History 16](#_Toc488327695)

## Purpose

The purpose of the Global Information Security Policy is to ensure the integrity, confidentiality, and availability of Alight’s information systems, data, and resources.

Additionally, the Information Security program helps to ensure the appropriate protection of Alight’s information assets.  This includes availability of timely, accurate information and information processing activities which deliver client services or supporting functions.  Information refers to all data (customer data or otherwise) held by, or on behalf of, Alight.

 Information Security goals include the following five key components:

* Confidentiality: protecting information and systems from unauthorized disclosure or interception
* Integrity: safeguarding the accuracy and completeness of information, systems, and computer processing
* Availability: ensuring that information and systems are available to authorized users when required
* Accountability: the requirement for actions of an entity to be traced uniquely to that entity
* Assurance: confidence that controls are operating effectively as expected

## 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 "colleague" 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.

## Introduction

In today’s information age, “information assets” such as intellectual property, business plans and personal information are among Alight’s most important assets. The confidentiality, availability, and integrity of the information assets must be scrupulously protected, which is why the broad effort known as “information security” is an essential and fundamental activity of Alight. Alight recognizes the importance of information security both in achieving success for the company and in maintaining the trust of our stakeholders, including shareholders, clients, colleagues, suppliers, and business partners. To help attain this goal, Alight has established the “Global Information Security Policy”, which sets forth Alight’s commitment to protecting Alight and client information assets.

Alight is committed to providing information and information-processing activities that are protected against loss or compromise to support Alight’s mission to deliver global services focused on our clients, act with integrity, and maximize shareholder value.

The Global Information Security Policy is a statement of the minimum requirements, responsibilities, and accepted behaviors required to establish and maintain a secure environment, and achieve Alight’s business objectives.

The Global Information Security Policy sets the direction, provides broad guidance, and defines requirements for information security related processes and actions across Alight. Alight’s senior leadership team is fully committed to information security and mandates that every person employed by or on behalf of Alight has important responsibilities to continuously maintain the security and privacy of Alight and client data.

The Information Security Policy regarding Alight's computing resources is based on the following guiding principles:

* Individual accountability: Every user of Alight's computing resources is responsible for protecting the confidentiality, integrity, and availability of information collected and processed on behalf of Alight, its colleagues, and its clients
* Role based access control: Users of Alight's computing resources are granted access only to the information they require to perform their roles
* Data ownership: A "data owner" is defined as a business person who is responsible for the business functions supported by the application. It is the responsibility of the "owner" to define and approve the role based access requirements

## Mission Statement

Global Security Services (GSS) provides a governance framework that ensures and enforces the confidentiality, integrity, and availability of Alight's data and that of Alight clients.

## Objectives

The Alight Global Information Security Policy, supporting policies, and security standards are provided to ensure that associated risks to Alight are managed to an acceptable level.

Alight is committed to:

* Ensuring that the availability, integrity, and confidentiality of Alight’s information systems and data are maintained and controlled
* Limiting Alight’s exposure in the event of loss, corruption or misuse of its data, information assets or systems
* Ensuring the application of information security standards is commensurate with the level of risk it faces
* Meeting legal, regulatory, and contractual requirements

## Structure

The Global Security Services (GSS) is led by the company's Global Chief Security Officer and provides the following services:

* Business Resilience
* Corporate Protection Services
* Planning & Business Management
  + Risk Governance Policy definition and governance
  + Security Architecture Information Security Strategy and Analysis
  + Security Development Security Application Testing and Verification
  + Security Champions program leadership
* Security Engineering
* Security Operations
  + Vulnerability Management
  + Incident Response support
* Service Operations
  + Identity & Access Management
* Third Party Management
  + Client security relationship management
  + Sales and renewal support

The Global Information Security policy and standards supports the services provided by Information Security group. The core policies and standards include:

* 100.01 Data Security Classification Standard
* 100.02 Data Destruction Standard
* 201.00 Asset and Data Protection Policy
* 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
* 202.00 Vulnerability and Compliance Management Policy
* 202.01 Vulnerability and Compliance Management Standard
* 203.00 Application Security Policy
* 203.01 Application Security Standard
* 204.00 Mobile Device Security Policy
* 208.00 Incident Response Policy
* 208.01 Incident Response Standard
* 209.00 Information Security Awareness Policy
* 209.01 Information Security Awareness Standard

## Roles and Responsibilities

### All colleague responsibilities

* To understand and adhere to Alight's Code of Conduct, Data Privacy Policy, and Global Information Security policies and supporting standards
* To actively participate in information security awareness programs and in the protection of Alight business operations and client data

### Global Security Services responsibilities

* To document, maintain, and enforce Alight Security policies and standards, adjusting for an appropriate balance of regional and global needs
* To support risk owners by providing decision-enabling, audience-focused reporting on gross and net risk load to risk and product owners
* To support risk owners by providing timely and source-agnostic consulting on threat disclosures
* To define the language that is used to discuss risk in a constructive business context
* To identify risk using internal vulnerability assessments, client reviews, open source intelligence, etc., as inputs
* To document, evaluate and track risk using Alight data classification and protection guidelines, internal and industry data on business cost of data breach, etc., as inputs

### Corporate Risk owner responsibilities

* To understand Alight's business
* To understand Alight's contractual and ethical obligations
* To evaluate needs of Alight and clients
* To make risk management decisions
* Accept risk (take no corrective action)
* Mitigate risk (support remediation actions)
* Eliminate risk (disable functionality)
* To accept responsibility for risks in their domain

### Data owner responsibilities

* To classify data in compliance with the Information Classification Standard and provide accurate inventories of protected and restricted data
* To define, enforce, and support a least-privilege role-based access control model for all protected and restricted data
* To regularly review all data entitlements for compliance with Alight's Information Security policy and supporting standards
* Product owner responsibilities
* To understand product or supplier capabilities
* To interface with developers or suppliers in support of the Information Security policy
* To provide accurate evaluation of risk management options

### Chief Security Officer responsibilities

* Provide vision and leadership as needed for developing and implementing technology initiatives that align with Alight’s global business goals
* Participate in strategic and operational governance processes as a member of the management team and responsible for delivering industry-leading technology globally across Alight’s business
* Develop, track, and control the technology annual operating and capital budgets

### Chief Information Security Officer responsibilities

* Provide strategic leadership of the Information Security Program and to prioritize security initiatives to maintain acceptable amount of risk for each business initiative
* Provide guidance and counsel to the Chief Security Officer and leadership team in defining objectives for information security
* Provide leadership, direction and guidance to maintain the confidentiality, integrity, and availability of data

## Policy Statements

### General

* 1. Alight has established a method by which all Alight colleagues and contractors can report information security concerns or request guidance regarding information security practices. Report questions or concerns to [Global.EOC.Mailbox@aon.com](mailto:Global.EOC.Mailbox@aon.com) and/or [Global.Security.Services@aon.com](mailto:SRM.Mailbox@aon.com?subject=SRM%20Policy%20Exception%20Inquiry).

### Policy Governance

* 1. Alight has documented its policy governance framework in place to ensure all Information Security policies and standards are managed, controlled, and support Alight’s business objectives.
  2. The Alight Information Security policies must be reviewed annually. Supporting standards must be periodically reviewed and updated to ensure that they are applicable to the current Alight security posture and risk tolerance (at least every second year).
  3. The annual review and updates for Alight Security policies and standards is led by the Global Security Services group.
  4. The Global Information Security Policy is approved by the Global Chief Security Officer.

### 100.01 Data Security Classification Standard

* 1. The Data Classification Standard sets the tone at Alight for how data is classified, protected, handled, and securely destroyed. The policy and corresponding standard provides all Alight colleagues with the necessary guidance to be sure all data assets receive the appropriate level of protection in relation to the value of the data asset.
  2. All Alight colleagues must classify the data using one of four data classification levels defined by Alight.
  3. All data must be handled in accordance with the appropriate data classification level and information protection standard.
  4. Pertinent Standard
     + 100.02 Data Destruction Standard

### 201.00 Asset and Data Protection Policy

* 1. Alight must configure its information systems to support the mission of ensuring and enforcing confidentiality, integrity, and availability of Alight's data and that of its clients. Alight must ensure that its information systems support authorized access to information, enable consistent enforcement of its Information Classification Standard, and prevent unauthorized access or inappropriate use of information.
  2. Pertinent Standards
     + 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

### 202.00 Vulnerability and Compliance Management Policy

* 1. Alight must provide an approach to the overall direction to protect information resources by establishing a secured perimeter and network to protect the confidentiality, integrity, and availability of information assets by applying appropriate physical, content, system, and technical controls.
  2. Based on the role of the individual or the type of information being handled, more specialized training will be provided as needed.
  3. Pertinent Standards
     + 202.01 Vulnerability Management Standard

### 203.00 Application Security Policy

* 1. During the course of conducting business, Alight uses software that is either developed internally, developed by third parties on behalf of Alight, or commercial software. It is imperative that, regardless of where the software originates, it must not create a security exposure for Alight.
  2. Alight will take a risk based approach with both the development and purchase of software.
  3. Alight will take a proactive stance with regards to software. This includes:
     + Building software that is secure by design
     + Including security requirements at the beginning of any development project or acquisition of software
  4. Provide ongoing monitoring of software that includes code review, penetration testing, and risk assessments to ensure the secure state of the software is maintained.
  5. Pertinent Standards
     + 203.01 Application Security Standard

### 204.00 Mobile Device Policy

* 1. Alight will provide an approach in the overall direction to protect the confidentiality, integrity, and availability of information that resides on Alight’s approved mobile computing platform. This policy intends to prevent business classified data from being deliberately or inadvertently stored in an unsecured manner on a mobile computing device as well as sensitive data being transmitted over an unsecured network.
  2. The Global Mobile Device Security Policy will define the minimum Information Security requirements that must be met by all mobile devices and colleagues in direct support of Alight’s approved mobile computing platform.

### 208.00 Incident Response Policy

* 1. Alight has an established incident response policy and standard to address suspected or real attempts to compromise Alight information resources and assets. It is every Alight colleague’s responsibility to report suspected or known issues that could compromise Alight’s information security posture or events that violate Alight’s policies, standards, or procedures.
  2. Pertinent Standards
     + 208.01 Incident Response Standard

### 209.00 Information Security Awareness Policy

* 1. Information security and awareness training is required by all Alight colleagues. All Alight colleagues will receive awareness training that will provide an overview of the importance of information security and each individual’s roles and responsibilities for protecting Alight information resources and assets.
  2. Pertinent Standards
     + 209.01 Information Security Awareness Standard

### Change Management

* 1. Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized, tested and implemented in a controlled manner; and that the status of each proposed change is monitored.
  2. All configuration changes that have a direct or indirect impact on the security posture of Alight must be logged per the change control process, and be easily accessible to appropriate personnel and management.

## Applicable Standards

* 100.01 Data Security Classification Standard
* 100.02 Data Destruction Standard
* 201.01 Access Control and Authorization Standard
* 201.02 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
* 202.01 Vulnerability and Compliance Management Standard
* 203.01 Application Security Standard
* 208.01 Incident Response Standard
* 209.01 Information Security Awareness Standard

## References and Mandates

* None

## Legal Conflicts

Alight’s 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’s 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:SRM.Mailbox@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 | 1.6 |
| 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 | Document published |
| 1.1 | 2013 June | 2013 Annual Review | Reviewed and validated |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated  Scope – Changed to Aon plc  Compliance & Enforcement – updated wording from Legal  Structure – update policy & standard list  Add Section 7 for 204.00 Mobile Policy  Updated Applicable Standard list |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.4 | 2015 November | 2015 OCIE Audit Improvement recommendation | Add CIO and CISO Responsibilities |
| 1.5 | 2016 July | 2016 Annual Review | Wording changes including Global Security Services (GSS) name change |
| 1.6 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |