# Information Security Awareness Policy

## Purpose

The purpose of the Information Security Awareness Policy is to establish the minimum requirements and desired processes needed for an information security awareness program for all users of Alight informational assets.

An effective information security awareness program explains proper rules of behavior for the use of Alight IT systems and information, and is critical for providing the knowledge Alight colleagues need to comply with Alight security protocols while performing their jobs.

Technical security controls can be rendered ineffective by colleagues who do not use them correctly. The goal of an information security awareness program is to educate all users so they can supplement technical security controls, as opposed to detracting from them.

## 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.

## Policy Statement

### General

* 1. Alight must establish a formal Information Security Awareness Program.
  2. The Global Security Services (GSS) team must designate ownership of and responsibility for the Information Security Awareness Program at Alight.
  3. The program must communicate relevant information security policies, standards, and procedures that users need to adhere to during the course of their duties.
  4. All Alight colleagues and contractors with access to Alight facilities and information assets will actively participate in the Information Security Awareness Program and in the protection of all business operations and client data.
     1. All Alight colleagues and contractors with access to Alight facilities and information assets must complete appropriate security awareness training to include Data Privacy and Code of Business Conduct upon hire and on an annual basis thereafter.
     2. The Information Security Awareness Program will be set up as a continuous program with a variety of targeted alerts and brief topical reminders distributed to Alight colleagues and contractors.
  5. GSS is responsible for ensuring the content of GSS information security awareness materials remain compatible with current technologies and relevant to Alight.
  6. Alight will develop enhanced security awareness training necessary for colleagues in specific roles.
  + System Administrators
  + Application Developers
  + Database Administrators
  + Others as deemed appropriate
  1. Alight must establish a method by which all Alight colleagues and contractors can report security concerns or request guidance regarding information security practices. Report questions or concerns to GEOC Mailbox at [global.eoc.mailbox@aon.com](mailto:global.eoc.mailbox@aon.com) and/or the Global Security Services Mailbox at [global.security.services@aon.com](mailto:global.security.services@aon.com).

## Applicable Standards

* 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: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 | Risk Controls and Assessments |
| Author(s) | Alight Global Security Services | Risk Controls and Assessments |
| 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 policy due to Aon Hewitt acquisition |
| 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 June | 2016 Annual Review | Policy Practice change from InfoSec to PBM – Plan & Business Management  Clarified wording and replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organization name |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |