# Information Security Awareness Standard

Related Policy

* 209.00 Information Security Awareness Policy

## Purpose

The purpose of the Information Security Awareness Standard (“Standard”) 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 systems and information, and is critical for providing the knowledge Alight colleagues need to comply with our security protocols while performing their jobs.

Technical security controls can be rendered ineffective by users 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.

## Standard Statements

### General

* 1. At hire and annually, the training program will provide guidelines on the use and protection of Alight information and assets.
     1. Alight colleagues will be reminded that they play an important role in safeguarding and protecting Alight information and assets.
     2. All Alight colleagues and contractors that access Alight information assets must attend a security awareness class or take online awareness training within three (3) months of their start date.
  2. The effectiveness of the Global Security Services (GSS) Information Security Awareness Program must be monitored by testing course participants on information security content knowledge.
  3. All Alight colleagues must be made aware of certain security-related issues as they occur, including but not limited to:
     1. Virus alerts, hoaxes, and approved Company responses.
     2. SPAM alerts and phishing attempts.
     3. Social engineering techniques.
     4. Security topics of interests.
  4. The following topics must be included in the on-going GSS Information Security Awareness Program for Alight colleagues and contractors:
     1. Information Security and Privacy Policies.
     2. Data Security Classification, Labeling, and Handling Guidelines.
     3. Password Selection and Usage Guidelines.
     4. Laptop and Mobile Device Guidelines.
     5. Secure Workplace Guidelines.
     6. Acceptable Usage Guidelines (e.g., for email or Internet access).
     7. Social Engineering attacks and appropriately handling requests for information.
     8. Physical security related guidelines.
     9. Crisis Management guidelines.
  5. Alight Security policies and standards are available for review by all Alight colleagues.

## 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.

# 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 | 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 |
|  |  |  |  |