# Information Security Incident Response Policy

## Purpose

This policy covers incidents that may affect the confidentiality, integrity, and availability of Alight's information assets and documents the key requirements for effectively addressing the information security incident.

This policy is not intended to provide a substitute for legal advice but approaches the topic from an information security perspective.

## 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 Statements

### Managing Information Security Incidents

* 1. Alight will comprehensively address information security incidents in a timely manner to ensure the restoration of the confidentiality, integrity, and availability of Alight's information assets.
  2. Alight will assemble a computer security incident response team to analyze and effectively address the incident.
  3. Alight will maintain documentation of incident response roles, responsibilities, and incident response timeline.
  4. Alight must document an incident response standard that addresses the following, at a minimum:
     1. Identification of potential information security incidents.
     2. Process to report observed or suspected information security incidents.
     3. List of stakeholders.
     4. Communication and contact strategies.
     5. Notification requirements and communication plans.
     6. Analysis.
     7. Containment.
     8. Business recovery and continuity plans.
     9. Data backup processes, roles, and responsibilities.
     10. Alerts from intrusion detection, intrusion prevention, and file integrity monitoring.
     11. Feedback and lessons learned.
  5. Alight must test the incident response plan at least annually. Testing must occur on a yearly basis per region, and at the discretion of that region’s CISO.
  6. Alight will update the incident response plan based on lessons learned and industry developments.
  7. Alight must designate personnel to be available on a 24/7 basis to respond to alerts. The initial point of contact and control for information security incidents is the Global Emergency Operations Center.
  8. Alight must train Alight colleagues responsible for responding to information security incidents.
     1. As part of the annual test, expected responding groups must be given training on how to respond to information security incidents. Those who received the training are then responsible for disseminating that information to their respective teams.
  9. All information related to an information security incident must be treated as highly sensitive information and only shared with those individuals who are involved in the response to the incident. This will serve both to protect Alight colleagues' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.
  10. Any suppliers that handle Alight’s information assets and could potentially impact the confidentiality, integrity, and availability of those assets as part of providing services must be in adhere to all aspects of the Information Incident Response Policy and Standard.

### Applicable Standards

* 208.01 Incident Response 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 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 for further guidance.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_208.00 Incident Response Policy |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:global.security.services@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 | 2013 September | Original | Document published |
| 1.1 | 2013 June | 2013 Annual Review | No Changes |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.4 | August 2016 | 2016 Annual Review | Updated name change from IRSS with Global Security Services (GSS) to reflect new organization name |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |