# Vulnerability and Compliance Management Policy

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of this Policy is to outline Alight’s efforts to achieve and maintain an acceptable level of risk to its data by actively identifying and mitigating IT vulnerabilities/system misconfigurations that threaten Alight's ability to enforce the confidentiality, integrity, and availability of its data. Minimizing risk is accomplished by identifying and mitigating IT vulnerabilities/system misconfigurations both proactively (before information is put at risk through introduction of new technologies or processes) and reactively (after deployed technologies or processes have put information at risk).

## 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 provide 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 disciplinary action, 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 for 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

### Vulnerability and Compliance Management Framework

* 1. Alight must establish and maintain a Cyber Security Vulnerability and compliance Management Program to clearly define how vulnerability and compliance information regarding important information system devices will be collected and provided to the respective responsible parties.
  2. The framework must include:
     1. Risk assessment procedures designed to define environmental risk, focusing on architecture (External, DMZ, and Internal) as well as geography.
     2. Risk assessment procedures designed to define specific risk, focusing on business units and/or specific applications.
     3. Defined roles and responsibilities.
     4. Provisions for exception to policy or acceptance of risk.
     5. Defined workflows.
  3. The service must provide:
     1. A vulnerability monitoring process, which must provide alerts or notifications of new fixes available, and the resulting SLA for remediation.
     2. Scanning Services to provide oversight and monitoring of overall risk as well as performance against established SLA.
     3. Enable self-scan capability for IT teams to self-check the vulnerability/ misconfiguration remediation status on the system.
     4. Drive vulnerability/system misconfiguration remediation across Alight and extend necessary technical consultancy as required.
     5. Reporting to provide business units CIOs with scorecards and metrics as well as templates for technicians (self-service reporting).

### Handling vulnerabilities

* 1. Alight must implement appropriate measures to remediate all vulnerabilities and system misconfigurations found on information system devices.
  2. Alight will have a function and technology support operation established to collect vulnerability and system misconfiguration data from the information technology infrastructure.
  3. When systems are known to have vulnerabilities/systems misconfigurations which cannot be remediated, compensating controls must be implemented to mitigate the risk of the vulnerability/system misconfiguration being successfully exploited.

### Remediation

* 1. Alight to establish a vulnerability / system misconfiguration remediation process but not limited to patch management, MBSS compliance management etc. and record the corrective actions in a change control process.
  2. Patches must be applied in accordance with Alight SLAs defined in the Platform Configuration Standard.
  3. End users will not be responsible for maintaining patch levels/system configurations on software provided by Alight. The Alight IT support organization or the outsourced IT service provider will perform that role.

### Security patch application record

* 1. Details of vulnerability/system misconfiguration mitigation actions taken, such as implementation of remediation solutions or modify system configuration, must be recorded and kept for a minimum of thirteen (13) months. Retention time frames should be adjusted to meet all applicable legal and regulatory requirements.

### Contractors/Third Parties Vulnerability Management

* 1. Alight must ensure that contracts with Contractors who manage Alight data systems, networks, and applications include the necessary language to require that Contractor vulnerability management practices meet or exceed the Alight Vulnerability and Compliance management and Application Security Policy and associated Standards where applicable.

## Applicable Standards

* None

## 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](mailto:global.security.services@aon.com) for further guidance.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_202.00 Vulnerability and Compliance Management Policy |
| 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 September | 2016 Annual Review | Reviewed and validated  - Updated policy name  - Added compliance management as part of the policy  - Included self-scan, vulnerability treatment and metrics & report as core service |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |