# Application Security Policy

## Purpose

The purpose of the Policy is to outline Alight’s efforts to achieve and maintain an acceptable level of risk to its data by actively identifying and mitigating application vulnerabilities that threaten Alight's ability to enforce confidentiality, integrity, and availability of its data. Minimizing risk is accomplished by identifying and mitigating application vulnerabilities both proactively (before information is put at risk through the 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 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.

## Compliance Measurement

The Global Security Services (GSS) will verify compliance to this policy through various methods, including but not limited to, periodic walk-through reports, internal audits, and feedback to the policy owner.

## Non-Compliance

Application security assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All applications releases must pass through the change control process. Any applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Security Officer.

Violation of policy may be subject to disciplinary action, up to and including termination of employment. Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process.

## Policy Statements

All applications custom, off the shelf or third party applications developed, maintained or implemented on behalf of Alight which involves coding are free from medium or greater application security vulnerabilities before going live in production environment.

### Application Vulnerability Management Framework

* 1. Alight must establish and maintain an Information Security Application Vulnerability Management Program that clearly defines how application vulnerability information related to applications will be collected and provided to the respective responsible parties.
  2. The framework must include risk assessment procedures designed to define environmental risk, focusing on architecture (External, DMZ, or Internal facing) as well as geography. The framework must also have provisions for business unit focus which must identify specific risks in the environment.
  3. The framework must include:
     1. A method to monitor for new vulnerabilities, which must provide alerts or notifications of new fixes available, and the resulting SLA for remediation.
     2. Scanning where funded to provide oversight and monitoring of overall risk as well as performance against established SLA.
     3. Reporting to provide business unit CIOs with scorecards and metrics as well as templates for technicians (self-service reporting).
  4. Free or Open Source Software (FOSS)
     1. Before using free or Open Source Software (FOSS) in any product implementation or otherwise, Application Security team ensure it complies with the Application Security Standard and to check for existing vulnerabilities.
     2. Engage Alight Legal to review the terms of any applicable FOSS license agreement prior to use.
     3. Use licensed software only in accordance with the terms of its license agreement.

For details on FOSS please review the Application Security Standard.

* 1. Intellectual Property (IP) owned by others
     1. Do not use copyrighted work of others without the permission of the Copyright owner, including but not limited to, software code, images, photos, music, video, and literary works.
     2. Do not use the code or project development related activities that are IP of others
     3. For additional information about protecting IP please visit:

<https://sp.aonavenue.aon.net/myaon/aonasc/en-us/law/Documents/Global%20IP%20Policy%20v1%20082015.pdf>

### Handling Application Vulnerabilities

* 1. Alight colleagues must implement appropriate measures to remediate any confirmed vulnerabilities on applications in accordance with defined SLAs within the Application Security Standard.
  2. When applications have known vulnerabilities and the applications cannot be patched, compensating controls must be implemented to mitigate the risk of the vulnerability being successfully exploited.
  3. Alight will have a function and technology support operation process established to collect vulnerability and system configuration information from the information technology infrastructure.

### Remediation

* 1. Alight colleagues are to implement automated application patch management systems where applicable and appropriate and record corrective actions in a change control process.
  2. Patches must be applied in accordance with defined SLAs within the Application Infrastructure Security Standard.
  3. The methodologies to accomplish patch delivery must adhere to one of the following techniques:
     1. Centralized agent-based automated patch management w/reporting.
     2. Centralized host-based automated patch management.
     3. Centralized manual delivery of patches by authorized personnel.
  4. Alight colleagues will not be responsible for maintaining patch levels on software provided by Alight.

### Security Patch Application Record

* 1. Details of vulnerability mitigation actions taken, such as implementation of latest security patches, 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 Infrastructure and Application Security Policy and associated Standards where applicable.

## Applicable Standards

* 203.01 Application Security Standard

## References and Mandates

* OWASP Top 10 Project
* SANS

## 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.

## Communications

Questions regarding this Policy should be directed to Global Security Services at global.security.services@aon.com.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_203.00 Application Security 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 July | 2016 Annual Review | Reviewed and validated – modified Compliance & Enforcement, Policy Statements, References & Mandate section, and added 1.4 Free or Open Source Software & 1.5 Intellectual Property statements owned by others section.  Application security assessments are required; added OWASP Top 10 Project Reference and SANS Reference; updated name change from SRM with Global Security Services (GSS) to reflect new organization name |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |