# Application Security Standard

## Related Policy

* 203.00 Application Security Policy

## Purpose

The purpose of the Standard is to provide the requirements for deployment of applications at Alight. The application security program is designed to identify and resolve potential security risks before the solution is introduced into Alight's environment.

## Standard Statements

### Training and Awareness

* 1. It is mandatory for all colleagues involved in the development of code for Alight or Alight clients should have completed the basic level Software Secure Code training on secure code best practices and should have taken the refresher course annually.

### Assessment – Requirements

* 1. Alight must use a risk based framework when assessing applications.
  2. All applications must undergo a security assessment by a member of the Global Application Security (SSDLC) team before being deployed to production. When available, a manual security assessment performed by a recognized independent third party, may be reviewed .and utilized in lieu of an internal assessment.
  3. Application project teams must provide adequate time to the assessor in order to properly verify the application security. Costs for external assessment resources are the responsibility of the business unit and will not be absorbed by Information Risk & Security Services unless pre-approved.
  4. Application teams must provide non-production environments to the assessment team to perform their testing. The test environment must replicate as closely as possible the production implementation in functionality, versions of underlying software, and configuration. Code development must be complete before testing and the developers are expected to minimize changes and inform Information Risk & Security Services of code changes after an application has passed an assessment. When the source code is available, it must be made available to the assessor.
  5. Application teams must provide appropriate access to the environment to allow all necessary testing to occur. This includes the necessary IP addressing and URL information to identify the location of the application on the network and multiple accounts at each access level throughout the application and test environment. It is the responsibility of the project team to create the necessary accounts and provide the necessary access to the application to perform the assessment. In instances where the auditors cannot access the servers (such as third parties with no LAN credentials), the application development or operations groups must provide support to the auditors to screen share or assist in person with monitoring server processes or log information to assist in proving or disproving vulnerabilities that require such access.
  6. Application project teams must provide source code for all applications either internally developed, or contracted out where we have source code.  In instances where we only have source for parts of the application, they will provide source code for the parts that are available.  The Global Application Security Team will maintain possession of the source code and ensure that it is properly secured at an Alight controlled premise. Any source code assessed by a third party is done so under proper supervision by a member of the Global Application Security Team or application support group.

### Assessment - New Applications

* 1. New applications require assessments before being deployed to production networks or touching production data when one of the following is true:
     1. The application is accessed externally, i.e., from a location whose network security is not fully controlled by Alight.
     2. The application operates with administrative-level privileges.
     3. The application handles HBI or MBI data based on definitions within the Data Security Classification Standard.
     4. The application is hosted by a third party.

### Assessment - Deployed Applications

* 1. Already deployed applications require assessments when one of the following is true:
     1. There is a significant change in the way the application functions.
     2. The application is going to process data classified under a more restrictive protection level than previously approved.
     3. The application is moving to or from a protected environment (security zone, DMZ).
     4. The application is exposed to a different user base (i.e., application used by a single client moving to being used by multiple clients).
     5. Previous assessment of the application is older than 3 years or more.
  2. To facilitate client requests for application assessment reports, application teams must maintain, or have reasonably available, test environments with non-production data.

### Periodic Assessments

* 1. Applications handling the HBI or MBI data of more than one (1) million individuals must have a security assessment performed by an approved, independent third party annually.
  2. Applications handling HBI or MBI data should be assessed annually and must be assessed every three years regardless of change.
  3. Applications exposed to external networks should be assessed annually and must be assessed every three years regardless of change.

### Assessment Testing Scope

* 1. When determining the scope of the assessment, Alight colleagues must, at a minimum, consider the following:
     1. Application administration processes.
     2. Application security.
     3. Network and system security.
     4. Physical security.

### Client–Facing Document

* 1. If a client requires a summary of the assessment findings, a Client-Facing Document may be generated from this process. The CFD must include summary report data only and should include executive overview, severity, synopsis, and risk statements.
  2. Alight internal summary reports may be shared with clients with approval from both the Global Application Security manager and the business unit CISO or their delegates.
  3. Detailed vulnerability documentation and other Alight internal assessment documents must not be shared with clients.

### Remediation

* 1. All vulnerabilities of medium and higher severity levels are to be remediated and retested/verified as closed before being allowed into production.
  2. Any discovered vulnerabilities that apply to already deployed applications must follow the remediation schedule as published in the Infrastructure Security Standard.
  3. Vulnerabilities are designated into one of five classes each with its own predetermined service level expectation for remediation:

|  |  |
| --- | --- |
| **Rating**  **(Severity)** | **Evaluation Criteria  *Exploitation of Vulnerability Leads to:*** |
| **Critical**  **(5)** | Immediate threat of integrity or confidentiality of customer data via the public Internet  Widespread virus or worm propagation through the Alight private network |
| **Urgent**  **(4)** | Potential threat to integrity or confidentiality of customer data via the public Internet  Potential threat to availability of customer-facing systems  Immediate threat to integrity or confidentiality of internal or customer data via internal corporate network  Immediate threat to integrity or confidentiality of internal or customer data via private third party links |
| **High**  **(3)** | Potential threat to integrity or confidentiality of sensitive internal or customer data via internal corporate network  Potential threat to integrity or confidentiality of sensitive internal or customer data via third party links  Immediate threat to availability of internal systems  Potential threat to integrity or confidentiality of sensitive internal or customer data by authenticated internal user on the vulnerable device |
| **Medium**  **(2)** | Potential threat to integrity or confidentiality of non-sensitive customer or internal data  Potential threat to integrity or confidentiality of non-sensitive customer or internal data via private third party links  Potential threat to availability of internal systems |
| **Low**  **(1)** | Potential threat to integrity or confidentiality of non-sensitive material on a small number of internal or external facing systems |

## References and Mandates

* INFOSEC 202.01 Infrastructure Security Standard

## 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.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | 203.01 Application Security Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.6 |
| 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 | 2012 June | Update | Updated Section 2.5; added 2.6 |
| 1.2 | 2013 June | 2013 Annual Review | Reviewed and validated |
| 1.3 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.4 | 2015 June | 2015 Annual Review | Reviewed and validated – added Legal Conflicts section |
| 1.5 | 2016 July | 2016 Annual Review | Reviewed and validated – modified Training & Awareness section and added a condition for periodic assessment |
| 1.6 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |