# Vulnerability and Compliance Management Standard

## Related Policy

* 202.00 Vulnerability and Compliance Management Policy

## Purpose

The purpose of the Standard pertains to the patching and secure configuration of information technology assets such as laptops, desktops, servers, and network equipment within Alight's technology infrastructure.

Alight has four core processes that define the vulnerability and compliance management process. Those processes at a high level include:

* Monitor Internet sources and technology vendors for vulnerability risk related events
* Delivery of vulnerability alerts/notifications that define risk levels and SLA
* Vulnerability and Policy Compliance scanning of existing systems
* Vulnerability and Policy Compliance scanning of new systems on the network
* Driving treatment of identified vulnerabilities and system misconfigurations.
* Reporting to provide business units CIOs with scorecards and metrics as well as templates for technology teams (self-service reporting).

.

## Standard Statements

### Authorized Scanning Organization Responsibilities

* 1. The Alight Global Security Services (GSS) team is the organization authorized to manage vulnerability management and policy compliance scanning activities. GSS may grant self-scan access to the scanning infrastructure resources upon request.
  2. GSS will evaluate and test products designed to collect vulnerability information from Alight’s technology infrastructure.
  3. GSS will evaluate technology risks and communicate those risks along with the associated patch SLA to IT Support Organizations.

### IT Support Organization Responsibilities

* 1. All technology groups and support functions must provide administrative system access (as defined by the technology selected) in order to perform comprehensive scans of the environment.
  2. IT Support Organizations will remediate vulnerabilities/system misconfigurations per the SLA, or will apply for a policy exception.
  3. IT Support Organizations will leverage the self-scan capability to scanning infrastructure to self-check the vulnerability/ misconfiguration remediation status on the system.

### Availability of Services for Scanning

* 1. System owners must make systems available for scanning as needed.
  2. As defined by scope, all systems must be evaluated for vulnerabilities/system misconfigurations accordingly.

### IT Responsibilities

* 1. IT must have a process/procedure for vulnerability and policy compliance management.
  2. IT is responsible for patch management.
  3. IT is responsible for vulnerability/system misconfiguration remediation.
  4. IT must resolve vulnerabilities/system misconfigurations in accordance with defined SLAs found in [Section 13](#_Vulnerability_Ratings) of this document.
  5. IT is responsible for maintaining updated vendor supported operating systems and application software with service packs, fixes and updates.

### Internet-Facing Systems

* 1. All internet facing devices/equipment/services must be scanned for vulnerabilities and misconfiguration through the firewall.
  2. The services and applications exposed to the Internet will be evaluated for external threat vulnerabilities.

### DMZ Systems

* 1. All devices and applications in a DMZ must also be scanned for vulnerabilities and system misconfigurations.

### Systems on the Internal Network

* 1. Computer systems shall be scanned for vulnerabilities and misconfiguration from within the network environment.

### Scanning Frequency and Schedules

* 1. GSS is responsible for the establishment of the frequency by which systems must be scanned.
  2. Schedules for scanning must be made available upon request. (Schedule will be published and ad hoc scanning will be performed on needed basis)

### Pre-Production Scanning Requirements

* 1. All servers must be evaluated for vulnerabilities and system misconfigurations prior to implementation.
  2. All confirmed vulnerabilities/system misconfigurations that are severity 3 and higher (see [Remediation Schedule, by Severity](#_Remediation_Schedule,_by) for details) must be remediated before the system is approved for Internet facing zones or before processing/storing client data.

### Vulnerability Scanning and False Positives

* 1. **Definition:** False positives describe a condition where a system or application is not vulnerable to a particular vulnerability.
  2. **Administrator Responsibility:** Administrators have the responsibility to collect evidence (i.e., logs, code versions, time stamps) and present it to the scanning authority.
  3. **Scanning Authority Responsibility**: GSS will present any false positive information collected to the scanning vendor for resolution.

### Vulnerability Alerting

* 1. The Alight Global Security Services (GSS) team will provide a vulnerability alerting function for all technology vulnerabilities that applies to the Alight infrastructure.
  2. Each alert at a minimum must contain the risk rating and remediation SLA, as defined by this standard.
  3. SLAs for vulnerability alerting will be:
     1. **Scheduled Patch Releases**: Two business days from the announcement of a patch/workaround for scheduled releases.
     2. Ad Hoc / Off Cycle Patch Release: Three business days from the announcement of a patch/workaround for scheduled releases.
  4. IT support personnel are required to manage systems to vulnerability alert SLAs and, as a result, need to subscribe to the service.

### Remediation Schedule, by Severity

* 1. The following remediation schedule defines the severity ratings used in the Vulnerability Alerting process, and provides evaluation criteria used by Alight to describe and define risk. All vulnerabilities must be remediated as outlined in this Standard.

|  |  |
| --- | --- |
| **Rating**  **(Severity)** | **Remediation SLA** |
| **Critical**  **(5)** | 72 hours from vulnerability alert released |
| **Urgent**  **(4)** | 14 days from vulnerability alert released |
| **High**  **(3)** | 28 days from vulnerability alert released |
| **Medium**  **(2)** | 60 days from vulnerability alert released |
| **Low**  **(1)** | Next scheduled system upgrade (not to exceed 90 days) |

### Vulnerability Ratings

* 1. 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:*** | **Remediation SLA** |
| **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 | 72 hours from vulnerability alert released |
| **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 | 14 days from vulnerability alert released |
| **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 | 28 days from vulnerability alert released |
| **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 | 60 days from vulnerability alert released |
| **Low**  **(1)** | Potential threat to integrity or confidentiality of non-sensitive material on a small number of internal or external facing systems | Next scheduled system upgrade (not to exceed 90 days). |

## 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.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | 202.01 Vulnerability and Compliance Management Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.7 |
| 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 August | Update | Added Section 4.5 |
| 1.2 | 2012 September | Update | 13.1 Changed Nominal rating to Low and set remediation SLA no longer than 90 days |
| 1.3 | 2013 June | 2013 Annual Review | Reviewed and validated |
| 1.4 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.5 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.6 | 2016 July | 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 |
| 1.7 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |