# Network Security Infrastructure Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of this Standard is to define the appropriate protections for Alight’s network infrastructure.

## Standard Statements

### General

* 1. Authenticate all users and only provide access to the networks, devices, and services they are authorized to use.
  2. The technology organization must maintain current network documentation.
  3. Appropriate security design controls must be used to segment networks of different trust levels.
  4. Secure physical and logical access to ports used to diagnose and configure systems (i.e., physical serial ports) and disable such ports when not in use.
  5. Changes to the Alight network must go through the technology organization’s change management process.
  6. Validate source and destination connection requests at internal and external network control points and deny all others not specifically allowed.
  7. Prevent external systems from directly connecting to or accessing internal systems.
  8. Prevent internal systems from directly connecting to or accessing external systems.

### Network Device Connection

* 1. In addition to deploying firewalls or other security control devices on network perimeters, dedicated network switch hardware will be used to keep networks with disparate ownership profiles separate.
  2. Clear separation between Alight's private RFC 1918 IP addressing space and routable, third-party network space must be maintained. Internally addressed RFC 1918 IP addressing space must not be routed from the external network.
  3. An Alight-controlled subnet sharing the same network infrastructure as a non-Alight-controlled subnet must use VLAN technology to separate the two broadcast domains.
  4. When a switch or router is deployed into a third-party-controlled network, dedicated physical or logical interfaces, using non-routable addresses from the RFC 1918 IP address allocation, must be used to provide remote management visibility into those switches.
  5. Networks with a high-risk acceptance level (i.e., Internet-facing DMZs) require dedicated switches for each risk type as defined by the DMZ and Internet Hosting Standard.

### Critical Network Infrastructure Management

* 1. Establish, implement, and maintain processes that are designed to ensure that firewalls and other network devices are managed using encrypted communication channels. For example, a combination of SSH and/or TLS or equivalent level of encryption as defined in the Encryption Standard.
  2. Establish, implement, and maintain processes that require a two-factor authentication (which includes a non-reusable password) protocol to be employed by Alight colleagues and contractors of Alight who wish to establish remote access to Alight's firewalls.
  3. Establish, implement, and maintain processes to restrict the deployment of security updates to firewalls only after testing has been completed on development systems and pursuant to the Change Management Request process.
  4. A quarterly review of firewall rules, using a random sample of all firewalls must be performed by the network security team within the responsible IT technology organization.
  5. All systems in DMZ and network devices must be patched according to the Infrastructure Security Standard and configured according to the appropriate Minimum Baseline Security Standard (MBSS).
  6. Administrative resources must not be available from the public Internet. All administrative access must be provided to externally facing devices through the Alight network, or an acceptable out-of-band management service.

## References and Mandates

* RFC 1918
* <http://www.isc.org/software/bind>
* NIST SP800-119 Guidelines for the Secure Deployment of IPv6

## 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 | INFOSEC\_201.11 Network Security Infrastructure Standard |
| 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 | Clarified wording and 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 |
|  |  |  |  |