# Wireless Network Security Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Wireless Network Security Standard is to build on the principles established in the Asset and Data Protection Policy to provide the requirements for Alight's standards for use of wireless network technology so that sensitive data is appropriately protected and wireless network technologies are used and managed appropriately.

## Standard Statements

### Internal Corporate Wireless Networks

Corporate wireless networks are deployed for the sole use of internal Alight colleagues and contractors and their approved systems. The wireless network is an extension of the corporate LAN, and as such, all devices must follow the same policies and standards as wired devices. To ensure these standards are enforced, the following controls must exist within the wireless technology:

* 1. Non-exportable machine certificates must be deployed via Alight Technology delivery mechanisms to only approved endpoints connecting to the corporate wireless network.
  2. Standards must be implemented that utilize both 802.1x extensible authentication protocol – transport layer security (EAP-TLS), and the advanced encryption standard (AES) with a bit strength of 256 as specified within IEEE 801.11i.
  3. Wi-Fi Protected Access 2 (WPA2) must be enabled, while the use of WPA2 with a pre-shared key (PSK) is prohibited.
  4. WPA2 encryption keys must be changed every 60 days.
  5. All wireless access points will be managed by AITS personnel and/or an Alight approved managed provider.
  6. All wireless access points must have their default administrator username and password changed.
  7. The Service Set Identifier (SSID) may be broadcasted; however it must be changed from default.
  8. Bridging of wireless and other networks, both wired and wireless, including the corporate network, is strictly prohibited and must be disabled.
  9. Rogue wireless access points must be detected and disassociated with the corporate wireless network.
  10. All security events are logged and monitored via the Global Security Event and Incident Management system.

### Internal Guest Wireless Networks

Internal guest wireless networks are implemented for the use of Alight guests and contractors, and colleague’s personal devices that have a need to connect to the Internet from an Alight office. To ensure internal guest wireless networks are wholly separated from the Alight corporate network, the following controls must exist within the wireless technology:

* 1. Systems connected to the internal guest wireless network must not connect to the Alight corporate network and are trunked so that they may only connect to the Internet.
  2. Users of the internal guest wireless network will receive a code of conduct message that they must accept prior to utilizing the service.
  3. Authentication to the guest wireless network will consist of certificates or passwords, and will be assigned on an as-needed basis. These will expire in 24 hours.
  4. The use of WPA2 with a pre-shared key (PSK) is prohibited.
  5. Web usage must go through a proxy that will categorize traffic, replicating the existing corporate LAN standards on web filtering.
  6. Connection inactivity time-outs will be enabled for eight (8) hours.
  7. All wireless access points will be managed by Alight Technology personnel and/or a managed provider.
  8. All wireless access points must have their default administrator username and password changed.
  9. The Service Set Identifier (SSID) may be broadcasted; however it must be changed from default, and must be different from the internal corporate wireless SSID.
  10. Bridging of the guest wireless and other networks, both wired and wireless, including the corporate network, is strictly prohibited and disabled.
  11. Rogue wireless access points must be detected and disassociated with the internal guest wireless network.
  12. All security events are logged and monitored via the Global Security Event and Incident Management system.

### Externally Sourced Wireless Networks

Externally sourced wireless networks refers to instances where Alight has procured a DSL connection, with the intent to attach access points to it in order to provide guests / vendors / consultants / contractors the ability to connect to external sources. To ensure these types of wireless networks are wholly separated from the Alight corporate network or any extension of it, the following controls must exist within the externally sourced wireless technology:

* 1. Systems connected to the externally sourced wireless network must not connect to the Alight corporate network.
  2. Employees, contractors, consultants, vendors, etc. cannot use Alight equipment. Exceptions may exist such as remote connectivity testing, however any exceptions require Alight Technology authorization and approval.
  3. Wi-Fi Protected Access 2 (WPA2) must be enabled, as well as the advanced encryption standard (AES) with a bit strength of 256, as specified within IEEE 801.11i.
  4. WPA2 encryption keys or passwords must be changed every 60 days.
  5. All wireless access points will be managed by Alight Technology personnel.
  6. All wireless access points must have their default administrator username and password changed.
  7. The Service Set Identifier (SSID) must not broadcast, and it must be changed from default. It must be different from the internal corporate and guest wireless SSID.
  8. Bridging of the externally sourced wireless and other networks, both wired and wireless, including the corporate network, is strictly prohibited and disabled.
  9. During extended periods of non-usage, the wireless access points supporting the externally sourced wireless network must be powered down.

## 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 | INFOSEC\_201.12 Wireless Network Security 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 | Changed AITS to Aon Technology; updated wording in 2.4; 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 |
|  |  |  |  |