# Remote Access Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Remote Access Standard is to build on the principles established in the Asset and Data Protection Policy and provide requirements for the proper [identification](https://eroom7.hewitt.com/eRoomReq/Files/AppData/Local/Fishnet/2010/AON/Deliverables/Policy_Standard%20content/InformationSecurityTerms&Definitions.htm#Identification), [authentication](https://eroom7.hewitt.com/eRoomReq/Files/AppData/Local/Fishnet/2010/AON/Deliverables/Policy_Standard%20content/InformationSecurityTerms&Definitions.htm#Authentication), and [authorization](https://eroom7.hewitt.com/eRoomReq/Files/AppData/Local/Fishnet/2010/AON/Deliverables/Policy_Standard%20content/InformationSecurityTerms&Definitions.htm#Authorization) controls necessary to remotely access Alight information assets.

## Standard Statements

### General

* 1. Users must submit requests for remote access through an Alight approved remote access request process.
  2. Alight-owned equipment must be used to directly access Alight systems and networks.  The equipment must be configured according to Corporate Standards, including current service packs, patches, Anti-Virus software, and personal firewalls, as appropriate.
     1. All approved users who are using Alight-owned workstations to remotely connect to the Alight network must pass endpoint inspection rules including verification of latest OS patches and verification of the latest anti-virus signatures.  Any Alight-owned workstation that passes endpoint inspection can obtain a full network connection.
     2. All approved users who are NOT using Alight-owned workstations to remotely connect to the Alight Network must pass endpoint inspection rules including verification of latest OS patches and verification of the latest anti-virus signatures.   Any approved user using a non-Alight-owned workstation will be placed in a Citrix session that will prevent any data from Alight's internal network from being copied to the workstation.
  3. Simultaneous Connectivity to Non-Alight Networks: Remote systems must not be configured to connect to a non-Alight network while simultaneously connected to the Alight network (also known as split-tunneling).
  4. Remote access to Alight systems and networks must be done using a Global Security Services (GSS)-approved solution. The following solutions are permissible for remote access into the Alight network:
     1. SSL VPN
     2. Citrix Secure Gateway

### Identification

* 1. Each Remote User is required to have unique Remote Access Credentials.

### Authorization

* 1. Alight colleagues must receive written approval for remote access privileges and follow the Alight-approved remote access request process.
  2. Non-colleagues with a legitimate business need must receive written approval for remote access privileges, have a company sponsor, and follow the Alight-approved remote access request process.

### Authentication

* 1. Remote users must use two-factor authentication on any connections to internal systems.
  2. Use of Password AutoSave mode with the remote access system client software is prohibited.

### Architecture, Configuration, Monitoring, and Control

* 1. Remote access gateways must be located at perimeter entry points into the Alight network.
  2. Remote Activity logging must follow the Logging and Monitoring Standard, based on Tier 1 requirements.
  3. If Alight remote access systems are not functioning properly, they must default to denial of all privileges to users.  Malfunctioning remote access systems must remain unavailable until the issue has been resolved.
  4. Remote access systems must enforce encryption during the connection authentication process and during the session between the user and remote access systems.
  5. All Alight remote access systems accepting remote connections from public networks (such as the Internet) must include an idle time-out system. This time-out system must terminate all connections that have had no activity for a period of 24 hours.
  6. Where systems software permits, login banners must be used on all Alight information systems and networks that are directly accessible through remote access and on all remote access systems.
  7. All endpoint systems accessing the Alight network must comply with all applicable Alight Policies and Standards.

### Modems and Dial-up Access

* 1. Any use of a modem and/or dial-up access must be approved through the Information Security Policy Exception process.

## 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\_201.09 Remote Access 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 June | 2016 Annual Review | Reviewed and validated |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |