# Outbound Internet Access Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Standard is to define the appropriate protections for Aon’s network borders.

## Standard Statements

### General

* 1. Communication between the internal networks and the external networks including the Internet must be limited to only those services as required for business use and approved by Global Security Services. Exceptions to the ‘required by business use’ are defined in the Aon Acceptable Use Policy.
  2. Global Security Services must evaluate services for outbound access prior to deployment in the Aon network.
  3. Outbound communication is prohibited to connect to the Internet from an internal network directly.
     1. Outbound communication from the internal network to the Internet must be made through a DMZ and use a device defined in 1.4 of this document.
     2. Refer to the Internet Hosting and DMZ Standard for additional information regarding DMZ implementation.
  4. Access to the Internet from systems on the Aon network must be routed through a proxy firewall that logs and negotiates the connection on behalf of the Aon colleague or system.
  5. Any device accessing the Internet bypassing the standard proxy/firewall configuration must have no connectivity to the Aon network.
  6. All Aon colleagues must be authenticated prior to accessing the Internet.
  7. All web activity must be logged by source, destination, service port, userID, and URL.
  8. All web browsing activity will use a reputation-based filtering system to define categories of web usage.
  9. All e-mail transmitted outside the Aon network must use an Aon approved mail gateway.
  10. Traffic between the Aon network and the Internet or perimeter gateways must be scanned for malicious software.

## References and Mandates

* Aon Acceptable Use Policy

## 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\_201.07 Outbound Internet 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 | Updated IRSS with Global Security Services (GSS) to reflect new organization name |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |