# Platform Configuration Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Standard is to define the appropriate protection and configuration for Alight’s system devices.

## Standard Statements

### General

* 1. Configuration standards must be established and documented for common technologies and infrastructure services used in the production environment.
  2. Configuration standards should be reviewed and approved by the Global Security Services business unit.

### IT System Device Configuration

* 1. All system devices (including servers, voice and data networking equipment, or other devices enabling Alight colleague’s access to data) must be configured to minimize potential security threats, as documented in the Alight hardening standards (Minimum Baseline Security Standards), while facilitating the conduct of Alight's business.
  2. Alight owned and managed (inclusive of Alight managed service providers) computing platforms are the only systems allowed to connect to the Alight corporate network.
  3. As defined Global Security Services standards, business or client requirements, systems in scope of Logging and Monitoring requirements will deploy technologies/forward logs to Alight managed or provisioned security event incident management systems.
  4. All system configuration changes must be approved and follow Alight change control processes.
  5. Installed applications should run with functional ID (or service account) privileges, as opposed to administrator-equivalent privileges.
  6. Systemic controls must be implemented which prevent installation of unauthorized hardware on the Alight network.
  7. Systemic controls must be implemented which prevent installation of unauthorized software on system devices.
  8. All systems must be security hardened which remove or disable all unnecessary software-based utilities and system software.
  9. All systems must be security hardened which require the session time-out mechanism to lock the screen.
  10. Require a session time-out after a maximum of fifteen minutes of inactivity.
  11. Configure IT system devices so that all remote administrative access is through secure channels (‘secure’ methods include, but are not limited to, using encrypted protocols, passwords not in the clear using acceptable Alight-defined methods, i.e., scp, ssh, secure rdp as opposed to telnet and ftp).
  12. Review all vendor-supplied defaults (accounts and security roles) on all IT system devices connected to the Alight network (production or otherwise) are required to be changed during building the system for use.
  13. Review all vendor-supplied default password on all IT system devices connected to the Alight network (production or otherwise) are required to be changed during building the system for use.
  14. Disable unnecessary services and devices on deployed servers by changing default access to devices and services using the “deny all”, except required for business purposes” model.
  15. Systems must utilize Network Time Protocol (NTP), obtaining time information from an approved time source.

### Workstation and Laptop Configuration

* 1. General
     1. By default, Alight colleagues use non-privileged ("Power User") accounts to access workstations or laptops.
     2. Alight colleagues must not install other unapproved software packages on workstations or laptop computers without obtaining advance permission from Alight’s Workplace Technology Services.
     3. Laptop computers must securely log all significant security relevant events.
     4. Laptop computers must utilize full-disk encryption with no less than 128-bit key strength using approved cipher suite algorithms defined in Global Security Services Encryption standard.
     5. Anti-virus software must be running at all times and updated with reasonable regularity on workstations or laptops.
     6. Alight colleagues must not permit automatic software installation routines to be run on Alight workstations or laptop computers unless these routines have been approved by the Alight Workplace Technology Services.
  2. Physical Protections for Laptops
     1. Alight colleagues must never leave the laptop unattended in an unsecured area.
     2. Alight colleagues must lock the workstation or laptop in their office or work area during off-hours.
     3. Alight colleagues must never check their laptop as part of their luggage when traveling.
     4. Alight colleagues must not leave an unsecured meeting or conference room without their laptop.
     5. Alight colleagues must back up all important information periodically to ensure data availability in the event of theft.
     6. In the event of a stolen laptop, contact the Global.EOC.Mailbox@aon.com immediately.
  3. Use of Shared Accounts
     1. The use of shared accounts must be kept to a minimum and only on systems that are part of a pooled resource and may never be used in production environments. All users should be uniquely identified wherever possible. A shared account with privileged access is required to have call alter / privilege elevation procedures that provide audit capability.
     2. Shared accounts must have a documented and identified owner.
     3. Upon return of a shared resource (such as a shared laptop), the system must be wiped and reinstalled.
     4. Upon return of a shared resource (such as a shared laptop) using a common User ID, the password to the system must be changed.
     5. Logging and monitoring of shared resources must be configured and reviewed in accordance with the Logging and Monitoring Standard.

### Mobile Storage Device

* 1. Alight requires the use of an approved industry standard encryption methods to protect corporate data. Please refer to the Encryption Standard for more information.
  2. Alight may access or confiscate privately owned equipment, used for conducting Alight business, during investigations of data use, security configuration and review, or incident forensics.
     1. Anyone using a mobile device for Alight business must agree to this requirement.

### Password Configuration

* 1. Require passwords to meet or exceed Alight’s password rules defined in the Password and Authentication Standard.

### Antivirus

* 1. All Alight systems must deploy systems capable of detecting malicious code (including spyware and adware) on workstations, servers, and other related network devices where a commercially viable option is readily available.
  2. Ensure detection systems are kept current using automated update processes.
  3. Configure detection systems to actively scan appropriate targets and generate logs.
  4. Employ integrity checking software on sensitive business systems to detect unauthorized changes.
  5. Workstations must be protected with real-time, on-access scanning features.
  6. Servers are protected with scheduled scans during low-traffic timeframes.

### Network Device Configuration

* 1. Configure stored start-up files for routers and firewalls to be the identical secure configuration as the running configuration.
  2. Configure modems to auto-disconnect based on Alight’s accepted hardening documents. The default standard is to not allow dial in modems. For modems requiring dial-in, the source must be screened.
     1. Modem use should restricted to only critical infrastructure
  3. Disable vendor access modems as a default and require activation when needed.

### Database Configuration

* 1. Databases and applications that interface with databases must be configured in accordance with the following practices:
     1. All databases must authenticate users. Every user must be individually identifiable and must not use shared/functional accounts to log into database resources.
     2. Database access controls must be applied per schema or tables as required by the application.
        1. Access to HBI or MBI data as defined in Data Security Classification Standard within the database must be limited to only those Alight colleagues/systems that require access to that information.
        2. Access must be limited to only those functions (e.g., read, write, modify, etc.) required using a role based access paradigm.
     3. The Data Security Classification Standard defines data types that must be encrypted within database
     4. The Data Security Classification Standard defines data types that must be encrypted in transit when accessed from the database.
     5. Restricted data integrity verification and monitoring techniques must be used to detect data tampering and unauthorized modification.
     6. Database servers with HBI or MBI data as defined in the Data Security Classification Standard must be secured using internal firewalls to only allow connections from authorized and database-system-authenticated sources.
     7. HBI or MBI data as defined in the Data Security Classification Standard access event records must be created and written to a centralized log server in accordance with the Logging and Monitoring Standard.
     8. All Restricted Access databases must log connections and Data Control Language (DCL) changes.
     9. If users are allowed to make updates to a database via a web page, these updates must be validated to ensure that they are warranted and safe.

### DNS

Domain Name Service (DNS) is a hierarchical, distributed database that provides IP address to name (and name to IP address) translation for applications that need to access specific hosts. The standard implementation of DNS is with software named BIND (Berkeley Internet Name Domain), which runs on UNIX platforms.

* 1. DNS settings for Alight systems will only be sourced from Alight managed or provisioned DNS server resources.
  2. Externally accessible (from the Internet or from a trusted, third-party network) DNS servers must be deployed and configured in a secure manner in order to protect Alight systems from unauthorized access.
  3. The DNS architecture must be implemented in a secure way to minimize threats and outages.
     1. The externally accessible DNS server must be located behind a firewall DMZ to minimize potential for attack. Placing the externally accessible DNS server behind the firewall DMZ protects the DNS server from attacks by limiting external replies to one packet. This prevents a spoofed query by accepting only one reply that contains a query ID that matches the query ID sent in the query message.
     2. The firewall should also provide state-based TCP-filtering and UDP traffic inspection to restrict from unauthorized queries.
     3. Split-DNS must be used to provide separate name resolution for external lookups.
     4. External DNS resolution must be provided so that users on the Internet can find Alight public servers.
        1. This DNS server must not have information about the internal DNS, which means that internal network structure will be unavailable to outsiders.
        2. The internal DNS (located on the inside of the firewall) handles name resolution for the Alight WAN.
     5. The internal DNS servers are the only hosts permitted to make outbound DNS queries to the external DNS servers.
     6. Use at least 2 DNS servers to avoid a single point of failure.
     7. Two (2) geographically separate DNS servers must be used to provide external name resolution. DNS servers will be provisioned with a different ISP, so that in the event of a failure, DNS resolution is still available with the other DNS server.
  4. Use the most recent version of the DNS server software to minimize the security vulnerabilities and minimize the possibility of attack. Old versions of BIND have widely known vulnerabilities.
  5. Restrict zone transfers from slave DNS servers and the primary DNS master.
     1. DNS Zone transfers are only allowed to and from authorized internal DNS servers.
     2. Zone transfers are not permitted from internal DNS servers to external untrusted networks (the Internet or the DMZ). Any exceptions to this rule require approval from the Chief Information Security Officer.
  6. If dynamic update must be used, it must be restricted as much as possible to individual addresses.
  7. Strong anti-spoofing mechanisms must be used on the perimeter router and bastion host since addresses are used for authentication.
  8. Protect against spoofing by turning off recursion.
  9. Dynamic DNS
     1. Dynamic DNS is allowed to provide DNS resolution for workstations and systems in user LANs and build networks.
     2. Dynamic DNS is not allowed in datacenter or server LANs.
     3. Dynamic DNS entries will expire within the same period that DHCP leases have been defined, or if the host is granted a new IP within the same time period.

## 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\_201.05 Platform Configuration 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. Added section on unauthorized hardware installation. |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.4 | 2016 August | 2016 Annual Review | Clarified wording, name change from IRSS to GSS; changed Standard Statements 1.1, 1.2, 2.1, 2.2, 2.3, 2.6, 2.7, 2.8, 2.9, 2.11, 3.1.2, 3.1.3, 3.1.4, 3.1.6, 3.3.1, 4.1, 4.2, 4.2.1, 6.1, 7.2, 7.3, 9.3, 9.3.1 |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |