# Supplier Security Governance Standard

## Standard Related Policy

* 600.00 Supplier Security Governance Policy

## Purpose

The purpose of this standard is to outline the requirements that suppliers must meet to ensure they are taking reasonable and appropriate actions to protect Alight information.

## Standard Statements

Supplier is required to comply, at a minimum, with the following standards set forth below, as applicable to the service delivered to Alight and/or Alight clients. In addition, Supplier must comply with Alight’s applicable policies.

| Supplier Standards | Description |
| --- | --- |
| Supporting Evidence | Supplier’s applicable supporting documents, as identified in the survey, will be attached to the survey in a readable format or provided separately |
| Privacy and Security Policies | Supplier provides copies of formal privacy and security policies. |
| **Service Delivery Information** | Supplier evidences a role(s) based access control policy that restricts access to all computerized data. |
| Supplier encrypts the hard drive of every company laptop or other portable device used in the delivery of services to Alight and/or Alight’s clients, in accordance with Alight’s Encryption Standard. |
| Supplier prohibits the use of mobile media for PII/PHI storage. |
| Supplier implements a Clear Desk/Clear Screen Policy that protects PII/PHI from risk of exposure. |
| Supplier provides annual security training of employees and contingent workers. |
| Supplier has established and implemented investigative and response protocols that are initiated upon the suspicion of a security/privacy breach. |
| Supplier discourages the use of SSNs/NINs in Processing activities, except where specifically directed by a Client or required by law. |
| Supplier advises Alight of any legal actions to which they have been party for the past three years |
| **Operations Management** | Supplier will indicate whether or not their company or dependent third parties have Systems which access, receive, transmit or store Personally Identifiable Information and Protected Health Information. If so, supplier has oversight measures in place substantially similar to those in this document to control risks of third party access. |
| Supplier describes Service Level Agreements and Metrics associated with services provided to Alight and its clients |
| Supplier evidences how Personally Identifiable Information and Protected Health Information is protected in relation to inbound and outbound mail or fulfillment processing |
| Supplier identifies if their service includes mailroom or fulfillment center activities |
| **Business Continuity/ Disaster Recovery** | Supplier describes electronic file transfers occurring in the course of service delivery, transfer method, and frequency of such transfers |
| Supplier describes any encryption methods utilized in the file transfers, logging methods and error reports, and how errors are resolved |
| Supplier indicates whether service includes payment processing and if so, provides a description of policies, processes and controls to ensure accurate payment processing |
| Supplier identifies whether credit card information is stored and provides evidence of acceptable security methods for storage of the information |
| If service delivery requires multiple internal systems, Supplier will provide details of data synchronization processes |
| Supplier describes policies and controls to ensure Alight documents are securely stored and segregated from other records |
| Supplier describes Change Management process, including back out plans and notification process |
| Call Center Management procedures are defined and documented |
| Supplier describes dependencies required for resumption of service in the event of an interruption of service |
| Supplier has a formal and documented BC/DR plan and provides a copy as evidence |
| Supplier has a Pandemic Preparedness Plan and provides a copy as evidence |
| Supplier has a Crisis Management Team and Process in place. |
| Supplier identifies current Recovery Time Objective their plan is capable of meeting |
| Supplier identifies current Recovery Point Objective their plan is capable of meeting |
| Supplier describes data backup strategy including storage and transportation of data while recovery site is in use |
| Supplier describes Recovery site power sources and telecom connectivity |
| Supplier indicates which services cannot be provided to Alight or its clients while the Recovery Site is in use |
| Supplier stipulates annual testing of BC/DR Plans is done and provides evidence of testing |
| Supplier trains employees, as appropriate, on the DRP/BCP and communicates any changes to the BC/DR as changes occur |
| Supplier maintains current Emergency Contact List |
| Supplier describes the method and frequency in which management communicates the security and privacy policies and standards |
| Supplier indicates whether a third party supplier is utilized and whether they have access to PII/PHI |
| If third party supplier has access to PII or PHI, evidence of a supplier governance program is provided |
| Organizational Security | Supplier describes service agreements, SLAs, Quality Assurance, security and privacy controls in place with third party providers |
| Third Party Security | Supplier describes controls to protect PII/PHI in various information processing activities |
| Information Asset Classification and Control | Information assets critical to the delivery of service to Alight and Alight’s clients have been identified. |
| Supplier describes the methodology for classifying identified information assets critical to the delivery of services |
| Supplier identifies software products used to protect the transmission of PII/PHI over public networks |
| Personnel Security | Supplier describes process used to manage transmission of PII/PHI between Suppliers/Partners/Clients |
| Supplier must encrypt backup tapes |
| Supplier shall cooperate with Alight in administering its retention requirements concerning Alight Information in accordance with Alight Record Management Policies. Supplier must manage return, transfer, or if authorized by Alight, dispose of Alight Information in a secure manner in accordance with Alight’s Information Governance Policy. |
| Supplier indicates pre-employment screening is performed on hiring candidates for specific employee classification, including the type of screen |
| Supplier identifies whether or not foreign nationals are employed and describes international background checks performed |
| Supplier indicates non-disclosure and/or confidentiality agreements are signed as a condition of employment |
| Supplier describes process for employee terminations, including time frame for revocation of physical and logical access |
| Physical and Environmental Security | Security and privacy training include an awareness of the risk associated with misappropriation of user identification and password (i.e. social engineering tactics) |
| Supplier maintains records indicating that employees have been adequately trained on security and privacy policies and procedure |
| Supplier describes their company’s policies and procedures to report, analyze and resolve security violations both during and outside of normal business hours. |
| Supplier uses separation of duties to ensure no critical task is wholly dependent upon a single person or resource |
| Supplier describes process for revocation of system access for both forced terminations and planned employee separations |
| Supplier outlines acceptable physical security measures to safeguard and adequately protect their business locations |
| Supplier describes what environmental security controls are in place to protect the location from hazards such as heat/fire, water, humidity, etc… |
| Supplier maintains a current access list of all authorized persons who can enter server rooms or other restricted areas and provides same to appropriate security personnel and other individuals with a need-to-know in order to control access to this restricted space at all times. |
| Supplier understands and uses separation of duties |
| Information Security Operations Management | Supplier takes reasonable measures to stop viruses and protect data and networks from malware including reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis. |
| Policies and controls protecting e-commerce are used |
| Web servers and software are hardened to protect against attacks |
| Access Controls | Non-essential services and daemons are disabled |
| Supplier periodically reviews network security and application logs |
| Supplier has a process for securely disposing of media containing PII/PHI |
| Supplier employs dedicated staff to install, configure, test, and monitor network and computing environment security |
| Firewalls are used on all connections to internet |
| Supplier indicates use of a DMZ |
| Suppliers will define roles and responsibilities for application access |
| Supplier describes formal procedures in place to control the allocation of access rights to information systems and services. |
| Supplier environment uses unique IDs for users and utilizes them for access to applications and data |
| Supplier utilizes a formal and documented SDLC. |
| Suppliers will comply with applicable laws and regulations |
| Supplier has identified a person responsible for compliance with applicable laws and regulations |
| System Development and Maintenance | Supplier maintains list of risks as identified through audits and corresponding mitigation strategies and actions or statements acknowledging and accepting risk |
| Items rated as High Risk or Medium Risk in Survey requires a risk mitigation plan. |
| Supplier must comply with Alight’s Infrastructure and Application Security Standards. |

## 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 local laws or regulations. In the event of any conflict with relevant local 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’s Security Policies and Standards.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact Alight Global Security Services at [global.security.services@aon.com](mailto:global.security.services@aon.com) for further guidance.

## Related Documents

* Supplier Security Governance Policy

## References & Mandates

* None

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| 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 | Risk Controls and Assessments |
| Author(s) | Alight Global Security Services | Risk Controls and Assessments |
| 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 policy due to Aon Hewitt acquisition |
| 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, replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organization name and replaced all instances of Security Assessment Services (SAS) with Global Risk Assessments (GRA) |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |