**Supplier Security Governance Policy**

## Purpose

Alight relies on a global supply base to extend Alight’s service delivery and enable business growth. To protect data entrusted to its care, Alight must govern the supply base to ensure suppliers have adequate controls in place related to information security, data privacy, disaster recovery/business continuity, personnel security, and operational risk. Alight’s supplier risk governance program exists to:

* Protect Alight and Alight’s clients’ brand and reputation by assuring the data owner that information is protected as it flows through the chain of custody;
* Comply with Alight’s client contractual requirements by proactively assessing third parties’ controls against Alight’s standards, which are based on applicable industry standards, including data privacy information security, physical security and disaster recovery/business continuity;
* Mitigate risk by partnering with suppliers to implement and/or utilize industry standard controls;
* Provide incident management assistance and act as a liaison between client and supplier;
* Protect Alight’s investment in its supply base, reduce cost and enable growth.

## Scope

The scope of this Policy is global, which includes all business units, all regions, and all entities of the Hewitt Associates LLC (“Alight”). Alight refers to all wholly-owned subsidiaries of Hewitt Associates LLC, all subsidiaries in which Hewitt Associates LLC has a controlling interest, and all agents or authorized representatives of Hewitt Associates LLC or its subsidiaries.

## Applicable Audience

This Policy applies to all colleagues, contractors, and suppliers of Alight. The term "colleague" refers to all full-time employees, part-time employees, temporary employees, and interns who provide services to Alight. The term “contractor” refers to any individual on another company’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.) who provides services to Alight. The term “supplier” refers to all other third parties from which Alight purchases and /or receives products and/or services.

## Compliance & Enforcement

Compliance with this Policy is mandatory.

Potential violations of this policy are subject to review and investigation by Alight and/or its agents. Violations of this policy may result in discipline, up to and including removal of assignment, end of contract for suppliers or termination. This is subject to the procedural requirements of the countries in which Alight operates. Alight reserves the right to refer for prosecution any violations of this policy.

This Policy constitutes the current Policy with respect to its subject matter, and it supersedes and replaces all previous policies relating to its subject matter. Alight reserves the right to modify the Policy at its sole discretion at any time with the intent to update on an annual basis.

## Policy Statements

### General

* 1. The Business is ultimately responsible and accountable for understanding and owning the risk associated with the use of a supplier.
  2. The role of the Global Risk Assessment (GRA) organization is to assess the risk that a particular supplier presents, educate and consult with the business to facilitate an informed risk decision.
  3. Supplier services offered by the Global Risk Assessment practice include the following:
     1. Supplier Risk Assessment (Pre-contract)
     2. Supplier Risk Assessment (Post-contract)
     3. RFP Response Evaluation
     4. Supplier Security Review and Support
     5. Supplier Contract Review
  4. Alight’s supplier risk assessment process is based on internationally accepted industry standards including ISO 27002 and the Shared Assessments Standardized Information Gathering (SIG) questionnaire. The high level process consists of the following:
     1. A Security Assessment Service Request form should be completed by the business owner requiring services from a supplier if a supplier qualifies as a Tier 1-3 supplier (see section 2 below for Tier definitions) and in the following situations:
* New supplier relationship and contracting
* Contract re-negotiation
* Significant change in scope of service delivery
* Supplier merger or acquisition
  + 1. Global Risk Assessment (GRA) completes formal business impact analysis with business owner to place the supplier in the appropriate tier. The tier ranking determines the security baseline the supplier is assessed against.
    2. A customized Supplier Risk Assessment Survey (“Survey”) is sent to a supplier based upon the scope of their service delivery and their tier ranking.
    3. The Survey consists of questions in the areas of data privacy, information security, physical security, disaster recovery/business continuity, personnel security, and operational risk.
    4. The Survey requires the supplier to furnish documentation to support their response.
    5. The SAS risk analyst reviews the supplier response against Alight’s standards and rates the supplier risk.
    6. The Global Risk Assessment analyst writes a risk report and shares the report with the business owner and other internal parties as required.
    7. The Global Risk Assessment analyst shares the risks identified during Alight’s security assessment with the supplier.
    8. The Global Risk Assessment analyst and the business owner will build and manage a mitigation plan with the supplier if required to reduce risk to an acceptable level.
    9. Onsite security assessments or controls reviews are performed, as necessary, to verify a supplier’s security controls.

### Supplier Tiered Framework

* 1. Alight has developed a framework based on a tiered approach in assessing and mitigating risk associated with the supply base. The tier definitions are aligned with Alight’s Data Security Classification Standard. Please reference the Standard for detailed descriptions of the tiers.
     1. Tier One – Highly Confidential/High Business Impact
     2. Tier Two – Confidential/Medium Business Impact
     3. Tier Three – Internal/No Business Impact. Data is not considered confidential however business continuity is of primary concern.
     4. Tier Four - Public/No Business Impact

### Contract Requirements

* 1. GSS’s Global Risk Assessment practice will assist Business Units in assuring the supplier has and maintains a comprehensive information security program.
  2. Administrative, technical, and physical safeguards necessary to protect the confidentiality, integrity, and availability of our clients’ information.
  3. Reasonable restrictions upon physical access to records containing personal information, storage of such records and data in locked facilities and storage areas or containers.
  4. Data destruction capabilities to ensure that all data is properly destroyed when the contract is terminated, to include a certificate of destruction.
  5. Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information safeguards as necessary to limit risks

## Applicable Standards

* None

## Related Documents

* Supplier Security Governance Standard
* Data Security Classification Standard
* Alight Privacy Policy
* Relevant Regulatory Guidance for the Audience

## References & Mandates

* None

## Legal Conflicts

Alight’s 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’s 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 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.

# 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 July | 2013 Annual Review | Reviewed and approved by owners |
| 1.2 | 2014 July | 2014 Annual Review | Reviewed |
| 1.3 | 2015 July | 2015 Annual Review | Reviewed |
| 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 |
|  |  |  |  |