# Global Information Governance Policy

## Table of Contents

[Data Security & Governance 3](#_Toc488220650)

[Purpose 3](#_Toc488220651)

[Scope 3](#_Toc488220652)

[Applicable Audience 3](#_Toc488220653)

[Benefits 4](#_Toc488220654)

[Defining “Information” 4](#_Toc488220655)

[Responsibility 5](#_Toc488220656)

[Compliance & Enforcement 5](#_Toc488220657)

[Policy Statements 5](#_Toc488220658)

[1. Information Ownership 5](#_Toc488220659)

[2. Program Governance 6](#_Toc488220660)

[3. Information Lifecycle Management 6](#_Toc488220661)

[4. Training & Communications 11](#_Toc488220662)

[5. Information Governance in Messaging Solutions 12](#_Toc488220663)

[Applicable Standards 13](#_Toc488220664)

[References and Mandates 13](#_Toc488220665)

[Legal Conflicts 13](#_Toc488220666)

[Exceptions 13](#_Toc488220667)

[Related Documents 14](#_Toc488220668)

[Document Control Information 15](#_Toc488220669)

[Revision History 16](#_Toc488220670)

## Data Security & Governance

Data Security & Governance develops and implements accountability programs, controls and training designed to manage and protect Hewitt Associates LLC’s (“Alight’s”) information. Data Security & Governance resides within the Global Security Services (GSS) organization, reporting to the Chief Security Officer. GSS and Data Security & Governance are dedicated to driving effective security risk solutions that protect Alight's information while enabling business growth. Data Security & Governance accomplishes these goals through collaboration with the business units, the Law Department, Corporate Compliance, and Alight Technology.

## Purpose

The Alight Global Information Governance Policy (“Policy”) establishes Alight’s rules regarding the creation, storage, access, use, and secure disposal of corporate information, including, but not limited to, business records. It supports efficient business operations, preservation of corporate memory, and compliance with relevant legal and regulatory requirements.

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.

## Scope

This Policy applies to all corporate information, regardless of format or media.

The scope of this Policy is global, which includes all business units, all regions, and all entities of 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.

Specific regions where Alight does business may have unique Information Governance requirements that should be addressed within regional standards related to this policy. All regional standards must be reviewed and approved by Data Security & Governance to be considered finalized and official.

This Policy must be followed in conjunction with Alight’s Records Retention Schedules and other information management processes which apply to colleagues in their respective business units.

## Applicable Audience

This Policy applies to all colleagues, contractors, and vendors 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 “vendor” refers to all other third parties with which Alight does business.

Alight colleagues are expected to inform third parties of this policy and make positive efforts to enable third party compliance. Third parties are expected to make a good faith effort to comply with this policy.

## Benefits

The benefits of adhering to this Policy include better client service, increased operating income, reduced operational expenses, enhanced privacy and intellectual property protection, improved business continuity, compliance with applicable regulations and statutes, enhanced litigation protection, and reduced environmental impact. These benefits will be achieved through:

* **Accountability**: Individual Alight colleagues are accountable for managing, protecting, and disposing of Alight’s information in accordance with this Policy and the applicable Records Retention Schedule.
* **Integrity**: Information is managed consistently, stored securely, and retained in accordance with applicable laws and regulations. Information is maintained in a manner that is efficient and cost-effective and supports timely retrieval and access.
* **Consistency**: Information integrity is maintained regardless of the media upon which the information is stored.
* **Responsibility**: Information disposal is secure, environmentally-responsible, and is performed in accordance with applicable laws and regulations.

The application of these principals results in:

* **Cost Reduction:** Storage volumes are reduced resulting in reduced storage and litigation discovery spend.
* **Risk Mitigation:** Information is stored, handled, transmitted, and disposed of properly, reducing data loss and disclosure risks.
* **Business Value:** Business teams are able to efficiently reference and utilize a practical volume of current, timely information to more effectively run the business, make fully-informed decisions, and meet client requirements.

## Defining “Information”

**Information** is any document or data (whether in physical or electronic form) created, received, or used in connection with Alight’s business operations.

**Business records** represent a subset of Alight information that must be retained for specific time periods per legal, regulatory, business, or client requirements. Applicable business record categories and associated retention periods are defined within Alight’s Records Retention Schedules. Business records may include information stored within operational systems, but does not include back-ups of those systems.

## Responsibility

Alight is obligated to manage its business records in accordance with international and regional laws, regulations, and directives. Examples of relevant laws and regulatory bodies include, but are not limited to, the United Kingdom's Financial Conduct Authority (FCA), the United States' Sarbanes Oxley Act, and Australia's Evidence Act of 1995.

Alight’s Records Retention Schedules define the minimum time period that Alight’s business records must be retained relative to country and region specific laws, regulations, directives and business requirements. Data Security & Governance is solely responsible for defining and managing the process to create and maintain Alight’s Records Retention Schedules and is the sole custodian of the authoritative version of any and all Alight Records Retention Schedules.

All Alight colleagues are responsible for ensuring that business records are identified, retained, protected, and securely disposed of in accordance with this Policy, the Alight Records Retention Schedules, applicable Alight standards, and business unit and/or department specific procedures.

Each Alight business unit should work with Data Security & Governance to identify and document standards that align with this Policy in order to accommodate specific regional laws, regulations, business partnerships, and client requirements. Additionally, business units and departments should establish information management processes relevant to their unique business activities. Once established, these standards and processes should be communicated within the business unit and to the Data Security & Governance team.

Each Alight business unit is responsible for provisioning any and all resources, including, and not limited to, people, technology and financial resources, to establish and execute information management processes to support managing information in accordance with this policy.

## 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 vendors, or termination. Compliance related actions are 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.

## Policy Statements

### Information Ownership

* 1. Alight information is the property of Alight and may not be accessed or used for non-business-related or personal purposes of any kind. Some information, such as information Alight maintains on behalf of our clients in the administration of their plans, may be owned by, or owned jointly with, the respective clients. For the purposes of this policy, Alight considers information owned by our clients to be Alight information and subject to the provisions of this policy.
  2. Alight colleagues are required to return to Alight all Alight information in all formats and media upon termination of employment or engagement with Alight.
  3. Data Security & Governance is responsible for interpreting this policy and issuing any necessary amendments to it. Data Security & Governance will collaborate with the Law Department, Corporate Compliance, Business Units, and Alight Technology as necessary.

### Program Governance

* 1. Oversight for Alight’s Global Data Security & Governance practice is provided via a three-tiered model:
     1. **Tier One** – Information Governance Executive Leadership Team endorses Information Governance program initiatives and approves corporate policies.
     2. **Tier Two** – Information Governance Steering Committee develops and publishes Alight’s Information Governance strategy, policies, and enterprise-level service offerings.
     3. **Tier Three** – BU-Appointed Information Managers facilitate day-to-day Information Governance processes and promote awareness within their respective service area (office, department, or otherwise).
  2. Managers are responsible for how their colleagues capture and maintain information in accordance with established Alight policies, standards, and processes.
  3. When Alight acquires a business, the information of the acquired business will be integrated into Alight’s information environment, where appropriate, and assessed for compliance with Alight policies, standards, and processes.
  4. When Alight divests or discontinues a business, transfer or secure disposal of information associated with that business will be coordinated by Data Security & Governance, Alight’s Law Department, and the impacted business units.

### Information Lifecycle Management

Information lifecycle management is the systematic control of information, including business records, from creation to final disposal. The information management lifecycle includes the following steps: collect/create/receive, organize/store, use/share, and dispose.

* 1. All Alight colleagues are required to retain business records for the periods defined in the applicable Alight Records Retention Schedule.
  2. All Alight colleagues are required to preserve and protect information when directed by the Law Department. This process is commonly referred to as “Legal Hold” (see section 3.9).
  3. All Alight colleagues are required to promptly and securely dispose of business records where retention is no longer necessary for legal or business reasons, and not otherwise required under this policy.
  4. All Alight colleagues are required to ensure that business records are adequately labeled, indexed, and organized when placed in physical or electronic storage.
  5. Creating records is an essential part of everyday business. All Alight colleagues must maintain complete and accurate records that adequately document Alight’s business activities, and protect those records from unauthorized access, alteration, or disclosure.
  6. Collection / Creation / Receipt of Records
     1. A record created, collected, or used as part of a business activity must be classified in accordance with the applicable Alight Records Retention Schedule.
     2. Business records must be created and maintained in a manner that ensures information integrity and accuracy.
  7. Management of Records
     1. Alight is legally required to keep certain corporate information for defined periods of time. Alight colleagues must refer to the applicable Alight Records Retention Schedule for more detail on the time periods for which identified records must be kept.
     2. All Alight colleagues are responsible for preserving, maintaining and managing records in their possession in accordance with this policy, the applicable Alight Records Retention Schedule, and any additional client-imposed obligations.
     3. Each region, business unit, office, or department must designate one or more Information Managers to monitor, assess, and facilitate compliance with this Policy and all applicable schedules, standards, and processes.
     4. Alight must request business partners involved in managing information, such as physical records storage and technology outsourcing, to conform to Alight information management policies, standards and processes.
     5. All Alight colleagues are responsible for managing all Alight records that are in their individual possession, custody, and/or control. This includes organizing such records so that only related items with common subject matter and retention periods are assembled together for storage purposes (e.g. in the same file folder, CD, or box).
     6. Business records will be stored in an appropriate manner to ensure record integrity and to enable records tracking for easy access and retrieval.
     7. All Alight information, including and not limited to Personally Identifiable Information (“PII”), must be managed in accordance with Alight’s Information Security and Privacy policies. Any business process that uses, accepts, stores or transmits PII must have a process in place to protect and safeguard the information from unauthorized disclosure and ensure that its usage is consistent with existing privacy policies and legal requirements.
     8. For paper records, Alight colleagues must label all record cartons to identify information that would be pertinent for the retrieval or destruction of such records, including: record category, record date(s), record owner, client name, and a description of the contents.
     9. Alight colleagues must exercise caution if they are uncertain whether a particular information category is subject to a defined retention period. When in doubt, preserve the information and consult either your designated Information Manager or Data Security & Governance.
     10. Alight’s Records Retention Schedules must be reviewed regularly and, if necessary, updated to reflect changes in the statutory, regulatory, business, and/or client environment.
     11. Alight must provide at least one method for authorized individuals to search and retrieve records, regardless of format, structure, or naming conventions.
     12. Where possible, record metadata, audit trails, classification, and indexing should be preserved when a record is moved to another system or media.
     13. Information management controls in designated information systems may be audited in accordance with Alight audit processes. Where controls are not automated in the system, such controls must be assessed as a component of an audit of the environment.
         1. Where a new system is to be implemented, the new system should be assessed for design and implementation of information management controls.
     14. Digital media is the preferred format for storing Alight records. In cases where records are duplicated across electronic and paper media, the paper media is considered transitory, unless the physical copy has a signature, seal, or other additional content not represented in the digital copy. If in doubt as to your obligation to retain paper records when electronic copies are stored elsewhere, please consult Data Security & Governance.
         1. Back-up systems and media are not records and should be retained for no longer than 35 days and only to accommodate business continuity and disaster recovery activities.
         2. Back-up system and media retention guidelines detailed in 3.7.14.1 do not apply to email back-up systems and media.
         3. Examples of corporate information not requiring retention include:

Document copies kept for personal convenience or reference.

Publications, trade journals, and magazine articles that require no action.

Routine correspondence (unless relevant to a client or other business transaction).

Inter-office notices (including email) such as meeting requests and internal announcements.

* + 1. Colleagues may keep information that is not required to be kept, but as a general rule, this information should not be kept more than six months after the completion of the matter to which it relates or the termination of the client relationship.
    2. Managers will take reasonable steps to confirm that information controlled by departing colleagues is appropriately transitioned in order to support business continuity.
    3. Data Security & Governance is solely responsible for defining and maintaining the processes and supporting standards that relate to providing existing Alight colleagues with access to critical information or information controlled by departed or departing colleagues. Data Security & Governance will consult with Alight’s Law Department, Human Resources, Internal Audit, and Alight Technology teams to develop, maintain, and implement these processes as needed.
  1. Disposition
     1. Alight colleagues are responsible for reviewing Alight business records on an annual, or more frequent, basis to determine if they are eligible for disposition according the following “ROT” (**R**edundant, **O**bsolete, and **T**rivial) guidelines:
        1. Redundant copies of business records can be destroyed on or before the date the record is to be destroyed in accordance with the applicable Alight Records Retention Schedule.
        2. Information that no longer must be retained according to the applicable Alight Records Retention Schedule and this Policy must be disposed of in accordance with Alight’s Data Destruction Standard.
     2. Trivial information will be destroyed as soon as this information demonstrates no further business value. Pending or anticipated litigation or investigations and other relevant circumstances may prevent or delay the disposition process and must be considered before destroying information.
     3. When an information system is retired, the information contained within that system must be securely disposed of in accordance with this Policy, Alight's Records Retention Schedules, and Alight’s Information Security Policy. Records contained in retired systems must be maintained in a reasonably accessible format until those records are eligible for destruction.
     4. Any IT asset scheduled for disposal or transfer outside of Alight must be cleansed of corporate or personal information prior to transfer. For assistance related to IT asset transfers, contact Data Security & Governance.
     5. In order to reduce corporate risk, Data Security & Governance may consult with Alight’s businesses and with the Law Department to plan and execute defensible destruction programs aimed at Alight’s abandoned, unindexed, and/or expired information.
  2. Legal Hold
     1. When information needs to be placed on Legal Hold, the Law Department will issue a notice to colleagues who may be in possession of the relevant information.
     2. Corporate information destruction otherwise permitted under this Policy will be immediately suspended when the Law Department considers that business information should be placed on “Legal Hold.” Any scheduled disposal or modification of information subject to Legal Hold must be suspended immediately and until further notice by the Law Department.
        1. Legal Hold may occur when litigation is reasonably anticipated or has already commenced, or when Alight receives subpoenas or other formal requests for information. It is Alight’s policy to comply fully with such lawful requests.
        2. If Alight colleagues have any knowledge of a pending, threatened, or reasonably anticipated litigation, or government or internal investigation involving Alight, they must preserve documents related to the matter and immediately contact the Law Department to determine whether a Legal Hold has, or should be, issued.
        3. The legal penalties for the destruction of information sought in connection with legal proceedings are potentially significant. Colleagues should immediately contact the Law Department if they believe that litigation is reasonably anticipated or has commenced.
     3. Colleagues found to have knowingly destroyed or directed the destruction of information with the intention of preventing that information from being used in legal proceedings or investigations (whether commenced, threatened, or reasonably anticipated) will be subject to disciplinary action up to and including termination, and may be subject to civil and/or criminal prosecution.
     4. Alight colleagues must seek advice from the Law Department if there is any doubt about your legal obligations regarding the destruction of information.
     5. Alight may be required to search its information, including individual email mailboxes, in response to legal, regulatory, and/or security concerns.
     6. Colleagues in possession of information covered by a Legal Hold must locate and protect that information. Any information covered by a Legal Hold must be retained and preserved until the Legal Hold is formally released in writing by the Law Department.
     7. Managers, in consultation with the Law Department, are responsible for ensuring all Legal Hold instructions continue to be followed for departed Alight colleagues.
     8. Relocation of records subject to Legal Hold must be approved by the Law Department.
     9. The Law Department will notify you when a Legal Hold has been lifted, at which time information lifecycle activities pursuant to this Policy may resume as normal.
     10. Any colleague who believes that a Legal Hold is not being complied with must immediately contact the Law Department.

### Training & Communications

* 1. This policy must be made available to all Alight colleagues.
  2. Alight colleagues who create, maintain, or dispose of business records must complete information management training. Training must be appropriate to the individual’s responsibilities for managing business records.
  3. Training and other resources are available via the company intranet and Alight’s learning portal.
  4. Training certification and assurance of policy compliance will be documented for all Alight colleagues who successfully complete the information management training.
  5. Managers are responsible for ensuring that colleagues they supervise review this Policy, successfully complete required training and manage their information in compliance with this Policy.
  6. Information Managers and others who interact with off-site storage providers must complete training specific to managing hardcopy information.

### Information Governance in Messaging Solutions

* 1. Email sent and received via Alight supported systems (e.g. Microsoft Outlook, Proofpoint, Lotus Notes, and mobile devices) are subject to this Policy.
  2. Alight limits standard email mailbox size.
     1. You must actively manage your mailbox to ensure business records are stored outside of your mailbox in accordance with the applicable Alight Record Retention Schedule and the Store What Where Standard.
     2. Email attachments are considered part of the email content and should be managed along with the parent email itself.
     3. Email not filed as a business record outside of the Microsoft Outlook Inbox is automatically destroyed in accordance with the email system’s disposal settings as defined in the Alight System Data Deletion Standard.
  3. Email that is transitory should be disposed of as soon as there is no further business value. Copies of email records, including electronic or paper copies, must be destroyed on or before the date the email record is to be destroyed in accordance with applicable Alight’s Records Retention Schedule.
  4. In cases where an email message is printed to hardcopy, the electronic version of the email should be considered the official copy, unless the physical copy has a signature, seal, or other additional content that is not appended to the electronic copy.
  5. Except when subject to specific regulatory obligation, Alight does not log, record, archive, save, or otherwise backup instant message (IM) communications and you must not do so either. Accordingly, you must not use IM for:
     1. Any internal or external communications about colleagues or finance-related matters;
     2. Anything that is the subject of a Legal Hold Notice;
     3. Confidential, proprietary, or otherwise sensitive matters involving Alight, clients or any of their colleagues.
  6. Except when subject to specific regulatory or legal obligation, Alight does not archive or otherwise save recorded voice messages. This policy applies to all Alight owned or Alight approved messaging platforms.
  7. Access to email stored in Alight’s email systems is managed by, and is subject to the approval of, Data Security & Governance. Data Security & Governance consults with Alight’s Law Department, Human Resources, Internal Audit, and Alight Technology teams to provision access as needed.
  8. The use of personal or other third party email accounts to conduct Alight business is strictly prohibited. Alight personnel must not forward or otherwise transfer Alight information from Alight’s messaging systems to personal email or storage accounts. Alight data must be stored and managed in Alight-approved systems.

## Applicable Standards

* 100.01 Data Security Classification Standard
* 100.02 Data Destruction Standard
* 700.02 System Data Deletion Standard
* 700.03 Store What Where Standard

## References and Mandates

* None

## Legal Conflicts

Alight’s Security Policies and Standards were designed 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’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 of Alight shall take precedence over the more general provisions contained in Alight’s Security Policies and Standards.

## Exceptions

Alight conducts business across many countries and jurisdictions. Circumstances may arise where this policy does not align with local information management obligations or business circumstances. Employ the following guidelines and notify Data Security & Governance when such circumstances occur:

* All exceptions to this policy must be reviewed by Data Security & Governance. Exception requests may be emailed to [Information.Governance@Aon.com](https://one.aon.net/sites/SRM_ISPM/Shared%20Documents/Policy%20Lifecycle/Annual%20Review/2016/2016%20Final/DPG/Information.Governance@aon.com)
* Follow local regulations when local expectations exceed those outlined within this policy.
* Follow the Alight Global Information Governance Policy when the Alight policy exceeds local legal obligations. Contact Data Security & Governance should the Alight Global Information Governance Policy directly contradict local information management laws.

## Related Documents

* Alight Records Retention Schedules
* Code of Business Conduct
* Global Privacy Policy
* Social Networking Policy
* Social Media Guidelines
* Alight Security Policies and Standards

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Data Security & Governance | [information.governance@aon.com](mailto:information.governance@aon.com) |
| Version Number | 1.6 |
| Owner | Alight Global Security Services | Data Security & Governance |
| Author(s) | Alight Global Security Services | Data Security & Governance |
| 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 | 2012 August | Updated | Updated back-up retention period policy statement. |
| 1.2 | 2013 July | 2013 Annual Review | General updates for grammar, phrasing; information-centric focus. |
| 1.3 | 2014 June | 2014 Annual Review | Reviewed and validated. General updates relating to information-centric focus and responsibilities of parties. |
| 1.4 | 2015 August | 2015 Annual Review | Reviewed and validated. General updates to reflect organization structure changes. Addition of a minimum period for backup data persistence. |
| 1.5 | 2016 July | 2016 Annual Review | Reviewed and validated. General updates to reflect organization structure changes. |
| 1.6 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |