# Data Security Classification Standard

## Related Policy

* 100.00 Global Information Security Policy

## Purpose

The purpose of the Data Security Classification Standard is to establish the rules for handling Alight data to maintain the integrity, confidentiality, and availability of Alight’s [data assets](file:///D:/Profiles/dgochena/Fishnet/2010/AON/Deliverables/Policy_Standard%20content/InformationSecurityTerms&Definitions.htm#InformationAssets).

Alight's data is important to its business and all Alight colleagues. All Alight colleagues and contractors are expected to protect and handle Alight's data in accordance with its classification.

The Data Security Classification Standard is based on the principles of “least privilege” and “need to know”. These principles state that data is not to be disclosed to any person who does not have a legitimate and demonstrable business need to receive the data, and that they will have only the minimum privileges needed to interact with the data in order to perform their job responsibilities for only the period of time required to execute these responsibilities. Data should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. These concepts, when combined and applied with the other requirements of Alight Policies and Standards, enhance the integrity, confidentiality, and availability of Alight data and enhance protections against unauthorized use, modification, deletion, or disclosure.

Potential violations of this Standard are subject to review and investigation by Alight and/or its agents. Violations of this Standard may result in disciplinary action, up to and including removal of assignment, end of contract for vendors, 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 Standard.

## Standard Statements

### General

* 1. All Alight colleagues and contractors are responsible for the protection of data that has been entrusted to their care, and to adhere to the Data Security Classification Standard.
  2. All Alight data must be handled based on the assigned classification level.
  3. All Alight data must be assigned a custodian who is responsible for data across its entire lifecycle as defined by the Global Information Governance Policy.

### Classifying Data

* 1. All data generated by or for Alight, in whatever form (hard copy, written, verbal, or electronic) must be classified according to the level of confidentiality, sensitivity, value, and criticality. The classification of Alight data is essential to ensuring that the appropriate security controls are in place to safeguard Alight’s data assets.
  2. The default classification for unmarked Alight data that does not include personal information is Moderate Business Impact (MBI).
  3. The default classification for Alight data which contains personal information is High Business Impact (HBI).
  4. The data owners are responsible for assigning the classification of data, reviewing it, and ensuring it is kept up to date and at the appropriate classification. Data owners may delegate authority, but not their responsibility.
  5. Alight requires all data assets, whether generated internally or externally, to be categorized into one of the following four data classifications (listed in order from highest to lowest level of confidentiality/business impact):
     1. Highly Confidential / High Business Impact (HBI): This classification category must be assigned to data assets where unauthorized disclosure could cause severe or catastrophic loss to Alight, the data asset owner, or relying parties.
     2. Confidential / Moderate Business Impact (MBI): This classification category must be assigned to data assets where unauthorized disclosure could cause serious material loss to Alight, the data asset owner, or relying parties.
     3. Internal / Low Business Impact (LBI): This classification category must be assigned to data assets where unauthorized disclosure could result in limited or no material loss to Alight, the data asset owner, or relying parties.
     4. Public / No Business Impact (NBI): This classification category must be assigned to data assets that are unrelated to the Alight business or have been officially released by Alight for widespread public disclosure. The disclosure of this data would not provide a business or competitive advantage.

### Multiple Classifications

* 1. When data of multiple classifications is combined, the resulting collection of data must be classified at the highest level classification applied to any data asset in the collection.

### Need-to-Know / Need-to-Use

* 1. Access to data classified as HBI, MBI, or LBI must only be granted to authorized users with a legitimate business need-to-know or the need-to-use basis.
  2. Alight colleagues must not attempt to access HBI or MBI data unless they have been granted access rights by the relevant data owner or custodian.
  3. Alight data must be used only for the business purposes expressly authorized by the data owner or custodian.

### Data Labeling

* 1. All data leaving Alight’s custody must be classified and labeled prior to leaving Alight’s custody.
  2. Alight’s Data (hardcopy or electronic) and media containing data must be clearly labeled so that all users are aware of its ownership and classification.
  3. Document authors are responsible for labeling data with the appropriate classification.
  4. Where applicable, corporate document templates must be used that already include the appropriate classification markings.

### Data Loss Prevention

* 1. Data that is classified as HBI and/or MBI that leaves Alight’s custody must be monitored by a data loss prevention tool.
  2. Data that is classified as HBI and/or MBI that can be identified thru a data loss prevention content inspection process must be prevented from leaving Alight’s custody unencrypted.
  3. Data loss prevention alerts must be reviewed by a representative of the data owner and all violations of data loss prevention policies must be reviewed by a business unit incident response leader.
  4. All data loss prevention alerts that the incident response leader may suspect as malicious activity must be reported to the [Global.EOC.Mailbox@Aon.com](mailto:Global.EOC.Mailbox@Aon.com) for further investigation.

### Destruction of Data and Media

* 1. Data classified as HBI, MBI or LBI that is no longer useful or needed, must be disposed of following Alight’s data disposal standards. Please refer to the Data Destruction Standard document for specifics.

### Classification Framework

* 1. The table below outlines the criticality and impact to Alight if data is not handled with the appropriate level of care.

| **Criteria** | **HBI - RED** | **High Business Impact** | **MBI - YELLOW** | **Moderate Business Impact** | **LBI - GREEN** | **Low Business Impact** | **NBI - BLUE** | **No Business Impact** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **High-level definition** | Highly confidential data restricted to specifically named individuals with a need-to know or use | | Confidential data restricted to small groups (e.g., project team) of people with a need-to know or use | | General company data intended for use by colleagues when conducting company business | | Data for widespread public disclosure | |
| **Confidentiality** | Highly confidential | | Moderately confidential | | Low confidentiality | | No confidentiality | |
| **Disclosure impact** | Severe or catastrophic material loss if data disclosed | | Moderate damage if data disclosed | | Some damage if data disclosed | | No damage if data disclosed | |
| **Data value** | High value data | | Moderate to high value data | | Low to moderate value data | | Low value data | |
| **Data Examples**  **Please note: this is not an exhaustive list. They are intended to help guide the classification of data.** | - Client Lists  - Personnel records  - Social Security Numbers  - Financial Account Numbers  - Credit Card Numbers  - National Insurance Numbers  - Medial & Claims Data  - Litigation related Data  - Regulated Data  - Password & Passphrases  - Participant data covered under HIPAA  - Full Date of Birth | | - Client Data  - Account Numbers  - Mailing Lists  - Financial Reports & Transactions  - Proprietary Processes  - Data under NDA | | - ke.aon.com  - General Internal Memos  - Training Materials  - Policies, Standards and Procedures  - Alight Phone & Address Books | | - [www.aon.com](http://www.aon.com)  - Marketing Brochures  - Advertising Media  - Annual Report  - 10K Report  - Product Brochures  - Press Releases | |

Handling Standards

The table below defines how data will be handled based on the classification level assigned to it.

| **Description** | **HBI - RED** | **High Business Impact** | **MBI - YELLOW** | **Moderate Business Impact** | | **LBI - GREEN** | **Low Business Impact** | **NBI - BLUE** | **No Business Impact** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Access Request** | Access request must be documented and managed in a centralized repository (either local, regional or global) | | Access request must be documented and managed in a centralized repository (either local, regional or global). | | | Access request must be documented. | | No special precautions necessary. | |
| **Access Review** | Data access must be reviewed by data owner quarterly with the review documented | | Data access must be reviewed by data owner quarterly with the review documented | | | Data access must be reviewed by data owner annually with the review documented | | No special review necessary | |
| **Internal Sharing (Which Alight Workers Can Have Access)** | Access restricted to authorized individuals by name on a need-to-know or use basis | | Access restricted to authorized groups (e.g., project team) on a need-to know or use basis | | | Unrestricted access within Alight – available to any employee or contracted staff. Not to be shared with the public. | | Share with anyone. No restrictions. | |
| **External Sharing:**  **Which non-Alight entities can have access** | Scope of access granted to authorized 3rd parties must be on a need-to-know basis. Data owner must approve. An NDA MUST be in place. *Verify that documented permission from the applicable clients has been provided, when appropriate.* | | Disclose to authorized business partners only on a need-to know basis and with a signed non-disclosure agreement. Data owner must approve. | | | | | Share with anyone. No restrictions. | |
| **Storage** | Data must be in your control. Move all restrictive and confidential data from your work area into a secure location at the end of each workday. Cryptographic protection may be required for the storage of electronic data. | | | | Take reasonable precautions to restrict access to electronic and hard copy data. | | | No special precautions necessary. | |
| **Copying and printing** | Users must use secure printing or print to their own local printer. Printers and copiers must not be left unattended when HBI data is printed/copied or will soon be printed/copied. Take reasonable precautions to restrict unauthorized access to copies. | | In-house printing/copying is preferred. Destroy spoilage, overruns, etc. take reasonable precautions to restrict unauthorized access to copies. | | Take reasonable precautions to restrict unauthorized access to copies. | | | No special precautions necessary. | |
| **Disposal** | Dispose in accordance with the Record Retention Policy. Destroy electronic data by completely overwriting or by physically destroying media. Paper and CDs must be shredded with a crosscut shredder or stored in locked security trash containers for secure shredding. If offsite, return to Alight for disposal. | | | | Dispose in accordance with the Record Retention Policy. Delete electronic data. Paper and CDs must be shredded with a crosscut shredder or stored in locked security trash containers for secure shredding. | | | No special precautions necessary. | |
| **Encryption inside Alight** | If data must be encrypted in order to meet specific statutory, regulatory, and/or client requirements, only use encryption solution that meets solutions in the encryption standard to encrypt data in motion and, when applicable, at rest. Please refer to Alight’s Encryption Standard for more information. | | | | No special precautions necessary. | | | | |
| **Encryption outside Alight** | Data must be encrypted in a manner that meets or exceeds Alight’s Encryption Standard to encrypt data in motion and, where applicable, at rest. Alight data MUST ALWAYS be encrypted when resident on mobile devices. | | | | | | | No special precautions necessary. | |
| **E-mail** | Always use secure email solution approved by Alight’s Security Team when sending outside of Alight. Do not send to recipient and email address you are not familiar with. Only send/forward to individuals authorized by data owner to access data. | | | | Always use secure email solution approved by Alight’s Security Team when sending outside of Alight. | | | No special precautions necessary. | |
| **Fax** | The authorized Alight sender/receiver must be at the fax machine until the transmission is complete. Alight sender/receiver must immediately confirm receipt of fax. Always have data owner approval to fax, remove documents from fax machine when complete, and verify correct number before faxing. | | | | Take reasonable precautions to prevent unauthorized disclosure. Verify correct fax number before sending. Attach fax cover sheet. | | | No special precautions necessary. | |
| **Electronic File Transfer**  **An example would be ftp** | Always use secure transmission solution approved by Alight’s Security Team when sending/receiving data outside of Alight. Do not send to destination you are not familiar with. Only transmit to destinations authorized by data owner. | | | | | | | No special precautions necessary. | |

### Auditing Requirements

* 1. At a minimum, auditing requirements for data access events for HBI, MBI, and LBI data include:
     1. Identify events which require audit trails.
     2. Identify events which require auditing, including frequency.
     3. Generation of audit record data.
     4. Provide sufficient audit record storage capacity.
     5. Respond to audit processing failures.
     6. Perform regular reviews and analysis of audit records for suspicious activities.
     7. Identify the dates and times of usage.
     8. Protect audit data from unauthorized access.
     9. Associate a specific individual with a particular activity or event.

## References and 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 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.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | [Data](mailto:Data) Protection & Governance | [Information.Governance@aon.com](mailto:Information.Governance@aon.com) |
| Version Number | 1.5 |
| 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 1, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 July | 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  Policy Owner changed from InfoSec to DPG.  Change standard name, change owner and approver.  Legal Conflicts Section Added. |
| 1.4 | 2016 July | 2016 Annual Review | Reviewed and validated  Changed name of standard. Disambiguate this aspect of data classification from other forms of classification such as record classification.  Clarified wording and replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organization name. |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |