# Store What Where Standard

## Related Policy

* 700.00 Alight Global Information Governance Policy

## Purpose

This standard communicates to colleagues the generally available and acceptable storage locations colleagues can use to store information that is not stored in Alight’s line of business systems.

## **Standard Statements**

### Acceptable Information Storage Locations

* 1. All Alight information that is stored by colleagues must be classified according to the Alight Data Security Classification Standard and must be stored in locations that meet the requirements defined in the standard.
  2. Acceptable information storage locations are defined relative to the following broad groupings of information
     1. **Client Work Product** consists of completed and in-progress versions of information, and supporting materials, related to serving our clients and/or supporting colleagues that serve our clients. Client work product must be stored separately from, and must not be inter-mixed with, administrative or your information.
        1. Completed versions of Client Work Product, as well as supporting materials, must be stored in a location that is backed up regularly and is not at risk of information loss or inaccessibility with the departure of any colleague.
        2. In-progress versions of Client Work Product, or reference copies (convenience copies) of completed or in-progress client work product, can be stored at locations that are not acceptable for completed versions of client work product for only a short period time that is no longer than necessary to perform specific business related tasks.
     2. **Administrative Information** consists of Alight colleague data that is related to each colleague’s Alight non-client related work experience. Administrative Information must be stored separately from client work product or your information.
     3. **Your Information** consists of information owned by the colleague that does not relate to the business of Alight. Your Information can be stored on an Alight issued device only if the presence of colleague owned information on the device has been explicitly stated by Alight to be acceptable. Your Information must not be stored on or at any other Alight storage location or device. Your information must be stored separately from client work product or administrative information.
  3. The following chart identifies current acceptable storage locations for information that are generally available to and accessible by most Alight colleagues:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Store What Where | | | | |
|  | **Client Work Product**  Information related to serving our clients and/or supporting colleagues that serve our clients (deliverables, contracts, templates, strategy documents, project files, etc.) | | **Administrative Information**  Information related to each colleague’s Alight non-client related work experience. (HR info, finance/expense data, system accounts, etc.) | **Your**  **Information**  Information owned by the colleague that does not relate to the business of Alight. (Your child’s sport team roster, shopping lists, music or personal photo libraries, etc.) |
| ***Completed*** | ***In-progress*** |
| *Digital Information* | | | | |
| Colleague Laptop / Desktop (C: Drive) | NO | TEMPORARY | YES | YES |
| Colleague Network Drive (H: Drive) | NO | TEMPORARY | YES | NO |
| Network Team Drive | YES | YES | NO | NO |
| SharePoint Team Site | YES | YES | NO | NO |
| OneDrive (My Site) | NO | TEMPORARY | YES | NO |
| Enterprise Content Management Systems (ECM) | YES | YES | NO | NO |
| Colleague Outlook Mailbox | NO | TEMPORARY | YES | NO |
| Shared Outlook Mailbox | YES | YES | NO | NO |
| *Physical Information* | | | | |
| Locking Workstation File Drawer | NO | TEMPORARY | YES | NO |
| Locking Team File Cabinet | YES | YES | NO | NO |
| Secured Team File Room | YES | YES | NO | NO |
| Approved Offsite Vendor Storage | YES | NO | NO | NO |

## 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 | 1.2 |
| 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 | September 25, 2015 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2015 September | Original | Document published |
| 1.1 | 2016 July | 2013 Annual Review | Reviewed and validated  Updated Data Security Classification Standard name change  Clarify wording on acceptable use  Replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organization name |
| 1.2 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |