# Data Destruction Standard

## Related Documents

* 201.00 [Asset & Data Protection Policy](http://security.aon.com/Docs/Template.htm?url=Policies/InfoSec/INFOSEC_201.00%20Asset%20Data%20Protection%20Policy.htm)
* 100.01 [Data Security Classification Standard](http://security.aon.com/Docs/Template.htm?url=Standards/InfoSec/INFOSEC_100.01%20Information%20Classification%20Standard.htm)

## Purpose

This standard defines the destruction method requirements all Alight colleagues must follow to destroy 1) redundant, outdated, or trivial business related data or 2) data residing on, or contained within, Alight assets that are being turned over to a third party that Alight has approved to receive only the assets, and not the data stored on or within the assets.

This standard applies to all Alight data classified as High Business Impact (HBI), Moderate Business Impact (MBI) or Low Business Impact (LBI) per the Alight Data Security Classification Standard.

## **Standard Statements**

## General

* 1. All data must be disposed of in accordance with the Alight Global Information Governance Policy. Colleagues must contact Data Security & Governance with any questions related to information destruction prior to commencing any data destruction activity.
  2. Alight approved media specific data destruction methods must render all data contained on the media unreadable, unrecoverable, and undecipherable by any data recovery technique.

## Disposal Techniques

* 1. Paper Media Destruction: Paper media must be securely shredded using a cross-cut shredder that meets the National Association for Information Destruction (NAID), or equivalent, requirements for maximum particle size.
     1. Secure shredding performed by a NAID, or equivalent, certified and Alight approved secure shred vendor is the preferred disposal mechanism.  A trusted employee from the office must oversee all on-site vendor activities to ensure that there is no disruption of the chain of custody of the information the vendor is processing while the vendor is on site.
  2. Digital Media Destruction: Digital media must be physically destroyed or forensically erased in a manner that renders the data on the media unreadable, unrecoverable, and undecipherable by any data recovery technique. Colleagues must contact Global Security Services (GSS) with any questions relating to the suitability of any digital media destruction technique.

## Using Third-Party Vendors to Destroy Media

* 1. Media destruction must be done using a NAID, or equivalent, certified and Alight-approved vendor that has signed a non-disclosure agreement and has required security controls in place to assure the protection of the media prior to destruction.
  2. Alight prefers that approved vendors perform destruction of physical media and portable digital media on-site wherever possible. Otherwise, vendors may transport the media to their facilities for destruction as long as there is a documented chain of custody for the transfer and required security controls are in place and documented within the vendor’s Alight approved service contract.
  3. A certificate of destruction must be returned to Alight by the vendor after the destruction of the media is complete that attests to the media destruction and includes the time of destruction, serial number of disposed media (where available), witness (if applicable) and the method of destruction.

## Removal of Assets from Alight’s Custody

* 1. Any asset transfer to a third party in which Alight is approving the transfer of the asset, and not the data stored or contained in the asset, must be conducted in a manner that ensures no data stored on, or contained within, the asset is transferred to the receiving third party.
  2. Digital storage media must be forensically erased prior to leaving Alight’s custody and/or control. Examples include, and are not limited to, computer systems’ hard drives, printers, phone switches, multi-function devices, and digital media (for example, USB drives).
  3. Real estate and physical assets, including but not limited to Alight-occupied office space, desks, file cabinets, equipment and office furniture, must be inspected prior to leaving Alight’s custody and/or control. All Alight data must be removed (such as paper in a desk, in boxes, or in cabinets) and properly stored or destroyed prior to the asset leaving Alight’s custody.

## 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 | June 12, 2012 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 July | Original | Document published |
| 1.1 | 2013 June | 2013 Annual Review | Removed compliance framework references to match format of other standards |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated. Updated to provide greater detail and clarity with respect to destruction services vendor, digital media destruction, and transfer of assets to third parties. Legal Conflicts Section added. |
| 1.4 | 2016 July | 2016 Annual Review | Reviewed and validated  Updated to reflect name change of Data Security Classification Standard.  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 |