# Clear Desk Clear Screen Standard

## Related Policy

* 300.00 Physical Security Policy

## Purpose

Alight requires that all High Business Impact (HBI) information and Moderate Business Impact (MBI) information as defined by the Alight’s Data Security Classification Standard be adequately protected when unattended. This is best achieved by completely clearing work surfaces of all removable items, where practicable. Work surfaces include, but are not limited to desks, credenzas, tops of cabinets, conference room tables, display boards, and walls. Alight’s goal is to reduce the risks of unauthorized access, loss, and damage to information.

Information assets can be in any form, ranging from paper documents, sticky notes, or digital forms such as data stored on computers. The mandate of this standard is to ensure that unattended work areas, whether in an Alight office or alternate work site, are clear of HBI and/or MBI information whether in digital or physical form.

## Standard Statements

### Responsibilities

* 1. Responsibility of Alight colleagues
     1. It is every Alight colleague’s responsibility to ensure that the availability, confidentiality and integrity of Information that is entrusted to their custody is not compromised through access by unauthorized persons. This standard is to be adhered to when an Alight colleague is away from their workstation for any length of time (momentarily, for a few minutes, or to have a meal or to take a coffee break).
     2. The Alight colleague's need to access data is for defined business reasons. It is the Alight colleague's obligation to ensure that Information is accessed and used only to complete assigned functions. All colleagues are expected to protect the confidentiality of information for which they are responsible. Although not all inclusive, the following items are some examples of what must not be posted in a public or open area:
        1. Passwords
        2. Contracts
        3. Account numbers
        4. Intellectual property
        5. Colleague records
        6. Social Security Numbers (“SSN”) or Government ID Numbers
        7. Medical information
        8. Protected Health Information (“PHI”)
        9. Financial information
        10. Data on business performance
        11. Personally Identifiable Information (“PII”)
  2. Responsibility of Leaders
     1. Supervisors and managers are responsible for:
        1. Ensuring that their team members clearly understand and follow this standard.
        2. Ensuring that appropriate resources (e.g locking file cabinets) are available for team members to comply with this standard in the workplace, whether in an Alight office or when working remotely.
        3. Enhancing awareness about this standard through regular communications, reviews, and update sessions.
        4. Monitoring on a regular basis compliance with this standard and, where required, reinforcing the message of compliance.

1. Clear Desk
   1. Any HBI or MBI information must be removed from the desk and locked in appropriate containers, drawers, or filing cabinets when the desk is unoccupied and at the end of the workday.
   2. While the Alight colleague is at the desk, paper documents containing HBI or MBI information must be shielded from the view of others who do not have permission to access the information
   3. File cabinets containing HBI or MBI information must be closed and locked when not in use or when not attended.
   4. Keys or combinations used for access to HBI or MBI information must not be left at an unattended desk, under keyboards, inside pencil cups, in unlocked desk drawers or other areas accessible to anyone.
   5. Paper and removable computer media containing HBI or MBI information must be stored in secured, lockable storage places, when such media is not in direct control of an authorized individual.
   6. HBI or MBI information such as passwords, authorization codes, or financial information must not be kept under keyboards, attached to computers, retained on sticky notes, or put up on notice or pin up boards.
   7. Any HBI or MBI Information written on white boards must be erased immediately after the meeting is over.
   8. Mobile devices must be password protected and stored in appropriate places.
2. Clear Screen
   1. Computer workstations and terminals must be locked when unattended.
   2. Computer screens (whether desktop or laptop) must be positioned in a manner that unauthorized persons might not easily view information on the system. If this is not possible or practical, use of a monitor privacy screen is required.
   3. Computer workstations must be logged off completely at the end of the workday.
3. Conference Rooms and Meetings
   1. Before beginning a new meeting, all information relating to the previous meeting must be cleared and removed from view.
   2. On finishing a meeting, ensure that the conference room is scrubbed clean of all Information and notes, messages, minutes of meetings, agenda items, etc., are not left behind on the desks, the screen, or the white board. If a conference room is to be used exclusively by specific team over multiple days and removal of information is not practical, the room must be locked and made accessible only to authorized colleagues.
   3. HBI or MBI Information must not be discussed in public, exposed to public view, or left unattended.
4. Printers and Facsimiles
   1. Print selectively and with discretion. Print documents only if necessary, especially if they contain any HBI or MBI information. Do not print emails simply to read them.
   2. Take printed documents out of the workplace only if absolutely necessary, especially if they contain HBI or MBI information.
   3. HBI or MBI information, when printed, must be immediately cleared from printers.
   4. Prior to sending or receiving fax messages containing HBI or MBI information:
      1. Verify that the intended fax machine is secure and/or restricted to individuals permitted to receive the confidential information.
      2. Notify the intended recipient prior to transmittal of the fax. Recheck the recipient's number before transmitting the fax.
      3. Verify that you are the intended recipient of faxes received on your machine.
      4. Require that the sender give advance notice of the imminent transmittal of a fax.
   5. HBI or MBI Information must immediately be cleared from facsimile machines.
5. Document Disposal
   1. Documents must be destroyed in a manner that is compliant with the Alight Data Destruction Standard.
6. Third Party Restrictions
   1. Third parties, including family members, must be restricted from the use of home office equipment and personal computers used for Alight business.
   2. Repairs of PCs used for Alight business must be performed by Alight Technology or an Alight approved vendor.

## Communications

Questions regarding this Standard should be directed to Data Security & Governance at [information.governance@aon.com](mailto:information.governance@aon.com).

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

## Exceptions

Application of the global security policies and standards may vary by region and office, and exceptions and variations may occur, if and when approved by Data Security & Governance. Please contact Data Security & Governance at [information.governance@aon.com](mailto:information.governance@aon.com) for further guidance on any exceptions or variations that may apply.

## Related Documents

* Alight’s Code of Business Conduct
* Alight Data Security Classification Standard
* Alight Personal Information Data Elements
* Alight Mobile Device Policy

## References & Mandates

* None

# 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. Transition of ownership to Global Information Governance |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated – Minor terminology updates to improve referential integrity with other supporting standards |
| 1.4 | 2016 July | 2016 Annual Review | Reviewed and validated |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |