# Mobile Device Security Policy

## Purpose

The purpose of the global Mobile Device Security Policy is to protect the integrity, confidentiality, and availability of data that might reside within Alight’s approved mobile computing platform. This policy intends to prevent business classified data from being deliberately or inadvertently stored in an unsecured manner on a mobile computing device as well as sensitive data being transmitted over an unsecured network. A data breach from a mobile device of any type could result in the loss of business information, damage or exposure to critical applications, loss of corporate revenue, and impact to Alight’s brand and public image. Therefore all users utilizing mobile devices for business use and where the mobile device is connected to Alight’s corporate or guest networks and other related systems must adhere to Alight’s published policies and standards.

Special care must be recognized when using mobile computing devices for business purposes to ensure that Alight business and client sensitive information is not lost or misused. The global Mobile Device Security Policy will define the minimum Information Security requirements that must be met by all mobile devices and colleagues in direct support of Alight’s approved mobile computing platform. These defined requirements must be implemented prior to a mobile device being connected to Alight’s corporate or guest managed networks, the use of Alight resources and related systems, and in support of client systems and stored information.

This policy applies to all mobile devices and accompanying media that meet or relates to the following classifications:

* Smartphones
* Other Mobile/Cellular Phones
* Tablet Computers
* E-Readers
* Personal Digital Assistants (PDAs)
* Portable Gaming Devices
* Ultra-Mobile PCs (UMPCs)
* Mobile devices capable of storing corporate data and connecting to a network

## Scope

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.

## 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 (contractors, 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.

Employment at Alight does not automatically guarantee or provide the initial or ongoing ability to use mobile devices in order to gain access to corporate networks, resources, and related business information.

This policy addresses the range of security threats related to the use of enterprise data:

|  |  |
| --- | --- |
| Threat | Description |
| Device Loss | Devices used to transfer or transport work files and related data could be lost or stolen. |
| Device Theft | Sensitive corporate data is deliberately stolen and then sold by an employee or unsanctioned third party. |
| Malware | Viruses, Trojans, Worms, Spyware and other computing threats could be introduced via a mobile device and therefore any stored or transmitted data is at risk. |
| Compliance | Loss of financial, personal, and other business confidential data could expose the corporation to the risk of non-compliance to local, regional, and global regulatory laws and documented requirements. |

The necessary addition of all new hardware, software, and/or related mobile computing device components that provide corporate connectivity will be managed by the Alight Corporate IT departments and at their discretion. The Alight Corporate IT departments will maintain a list of approved devices with the deployment of required security measures.

Non-approved corporate use of mobile devices to back up, store, transmit, or otherwise use to access business related data owned or managed by Alight is strictly forbidden.

## 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. 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 policy.

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.

## All Colleagues Responsibilities

Each Alight colleague is responsible for using mobile devices appropriately and is required to adherence to Alight’s published policies and standards. This includes Alight’s Privacy Policy, Acceptable Use, and other related Global Security Services policies and standards while using mobile devices that are connected or have access to corporate resources and related systems.

Alight colleagues must comply with the laws and regulations of states and countries in which Alight operates in. Colleagues are prohibited from using electronic communication devices to compose, send, or read electronic messages while driving. Electronic messages include email, text messages, instant messages, and commands or requests to access an internet site. Alight reserves the right to restrict or revoke access to Alight-provided mobile device services issued through the “Mobility Freedom” program or Alight-issued mobile devices at any time. Colleagues who fail to use Alight technologies (including mobile devices) appropriately, may, subject to local laws, be subject to disciplinary action up to and including separation from employment.

## Mobile Device Safety Concerns

Alight prohibits use of mobile devices while driving. Safety should come before all other concerns and colleagues should not place themselves or others at risk to meet business need.

Colleagues are required to comply with all applicable laws regulating the use of mobile phones while driving. Some countries, states, and municipalities prohibit the use of hand-held phones while driving. Colleagues should acquaint themselves with the requirements of the areas through which they travel before using a mobile phone or other electronic mobile device while driving.

Colleagues charged with traffic violations or other criminal offenses resulting from the use of cell phones or other mobile devices while driving will be solely responsible for all liabilities that result from such actions.

## Safe Driving Guidelines

Use a hands-free device, even if such use is not legally required. Purchase and cost of a hands-free device is the responsibility of the colleague.

Refrain from placing or receiving unnecessary calls while driving.

Dial a phone or view a mobile device only when the car is not moving, subject to local laws.

Never have stressful/emotionally heated conversations while driving.

Do not use mobile devices while driving in hazardous conditions or areas where extra driving vigilance is required, such as in bad weather, school zones, pedestrian areas, heavy congestion, etc.

Limit conversations or pull off the road to complete conversations.

Keep your eyes on the road at all times.

## Policy Statements

### Mobile Device Responsibility

Alight colleagues must agree to the following mobile device rules and recognize the need to protect business confidential and personal data that is stored on and/or accessed by using a mobile device. This basic code of conduct includes, but is not limited to:

* 1. Doing what is necessary to ensure adequate physical security of the device itself.
  2. Maintaining the software configuration of the device. This includes the operating system and installed applications that are being accessed on the mobile device.
  3. Preventing the storage of sensitive business data in non-approved applications that may be installed on the mobile device unless explicitly approved by Alight’s IT and Global Security Services departments.
  4. Ensuring the device’s required security controls are not subverted via hacks, jailbreaks/rooting, security software changes and/or security setting changes.
  5. Reporting a lost or stolen device immediately to Alight’s Physical Security Department, Employee Management (HR), Mobility Freedom Administrators, or other personnel responsible for safe guarding mobile devices used for corporate computing. Colleagues can also place a call to Alight’s Global Service Desk or local Help Desk for assistance with a lost or stolen mobile device.
  6. Alight is not obligated or responsible for the reimbursement of personal phone and data charges. This includes the loss of a personal device or related peripherals.
  7. Alight is not obligated or responsible for the recovery of personal data in the event the mobile device is lost, stolen, or device failure occurs. It is the colleague’s responsibility to backup business contact information and other data deemed of value on their Alight issued or colleague owned mobile device.
  8. Alight requires all colleagues with mobile devices accessing corporate applications and related systems to notify Alight Management and Alight Corporate IT Services upon termination or any type of employment and/or contract separation from Alight.
  9. Device replacement, upgrade, and/or a change in a colleague’s job responsibility does not ensure the ability to use mobile devices to access corporate applications and related systems.

### Mobile Device Security

The colleague is ultimately responsible for properly securing their mobile device to prevent personal and business data from being lost or compromised. The colleague is also responsible for the prevention of viruses and other related security exposures from being spread from one mobile or computing system to another. This might require the colleague to purchase and deploy additional software on their Alight issued or colleague owned mobile device in order to comply with published Alight policies and standards.

Any removal of Alight deployed or required security controls are strictly prohibited. Colleagues are forbidden from copying business sensitive data from corporate Email, Calendar, Contact, or related corporate managed systems to any other application on the mobile device or to an unregistered mobile device.

Security and Configuration Requirements:

* 1. Every mobile device approved for corporate use must be secured with an authentication password. That password must be of the proper strength and must meet Alight’s documented standards for securing mobile devices.
  2. Every mobile device approved for corporate use must be configured to time-out when the device is not in use with a maximum of 15 minutes of inactivity. This time-out will force user authentication after the time-out duration has been met. The time-out duration and additional configuration items must meet Alight’s documented standards for securing mobile devices.
  3. Business or client sensitive data will not be sent from a mobile device that is not part of the Mobility Freedom Program or that has not been approved by Alight. SecureMail services will be utilized at all times and the colleague is required to use corporate email and other related systems for the proper management and security of business and client data.
  4. The device operating system software must be kept current and up-to-date. This will ensure the latest security patches are deployed and therefore reducing known industry and environmental risks to Alight. Minimal device requirements as well as required updates will be managed by the Alight Corporate IT department and in support of Alight’s Mobility Freedom Program.
  5. All personal and business related applications as well as related data will be removed automatically from the device after a recognized number of failed logon attempts.
  6. The device must be configured to encrypt content with an Alight approved encryption method. Where the device is not capable of meeting this requirement, additional security software may be necessary to meet the encryption requirements or the device will not be approved for corporate use.
  7. The device must be configured to segregate corporate data from personal data. Where the device is not capable of meeting this requirement, additional security software may be necessary to meet the data segmentation requirements or the device will not be approved for corporate use.
  8. Colleagues must agree to random spot checks of their Alight issued or colleague owned mobile device and it’s configuration to ensure compliance with all applicable Alight policies and standards. Non-compliance must be address immediately or the device will be removed from corporate use and will be subject to being wiped (erasing all personal and business data) remotely.
  9. Alight reserves the right to deploy internet web filtering capabilities to further protect Alight corporate systems and business data as well as client data loss.
  10. Colleague is responsible for identifying and managing local mobile device passwords that connect to corporate networks and systems. Failure to change and/or update a corporate user’s password that may be stored on the mobile device could result in user lockouts and account disablement.
  11. The use of cloud computing services to store and/or transfer managed Alight and Alight client data is limited to solutions that have been approved by Alight’s Corporate IT and Global Security Services departments.

### Corporate Owned Mobile Devices

Alight Corporate owned smartphone and tablet devices are centrally managed by Alight Corporate IT Services.

Specifically, Alight colleagues are responsible for:

* 1. The use of mobile devices to connect, access, and manage corporate systems must be approved by the colleague’s management and Alight’s Corporate IT department. Approval is subject to proper justification and documented business need. As that need changes, the colleague may be asked to provide additional justification in order to continue use of an approved mobile device to access corporate applications and related systems.
  2. Installation of software updates and security patches. These updates must be made timely to ensure the latest security measures are deployed on each mobile device. Minimal device requirements as well as required updates will be managed by the Alight Corporate IT department and in support of Alight’s Mobility Freedom Program.
  3. Reporting a lost or stolen device immediately to Alight management or other personnel responsible for safe guarding mobile devices used for corporate computing.
  4. Colleagues are responsible for reporting damage to or known issues with corporate devices as a hardware or software malfunction could result in a loss of security controls.
  5. Colleagues are responsible for the timely return of corporate issued devices when the mobile device is no longer required or upon separation from Alight.
  6. Colleagues are responsible for formally reporting any and all known security concerns related to their Alight issued or colleague owned mobile device, applications, and related systems used to conduct Alight business.
  7. Colleagues are responsible for formally reporting abuse by other colleagues that are using corporate mobile devices inappropriately and not for their intended business use. This could include the storing and transmission of inappropriate material that could be found offensive by others and serves no business purpose.

### Colleague Owned Mobile Devices

The use of personal smartphones or other mobile devices will qualify for limited support by Alight’s Global Service Desk (noted in the next section). Colleague owned mobile devices are not centrally managed by Alight and therefore technical user support for hardware/software related issues is the sole responsibility of the device owner.

Specifically, the device owner and/or user are responsible for:

* 1. The use of mobile devices to connect, access, and manage corporate systems must be approved by the colleague’s management and Corporate IT. Approval is subject to proper justification and documented business need. As that need changes, the colleague may be asked to provide additional justification in order to continue use of an approved mobile device to access corporate applications and related systems.
  2. Settling any service or billing disputes with their carrier.
  3. Purchasing any required software that is not provided by the manufacturer or wireless carrier.
  4. Device registration with the 3rd party vendor and/or service provider.
  5. Maintaining and managing any necessary warranty information or claims.
  6. Mobile device battery replacement due to failure or loss of ability to hold a charge.
  7. Backing up all data, settings, media, and required applications.
  8. Installation of software updates and security patches.
  9. Device registration with Alight Corporate IT Services.

### Global Service Desk Responsibility

The following Alight Corporate IT services are related to the use of colleague owned smartphones or other mobile devices for approved business use and through the Alight established Mobility Freedom Program:

5.1 Enabling the use of colleague owned mobile device to access the web-based interface of the corporate email system.

5.2 Enabling the use of colleague owned mobile device to access web-based corporate applications and related systems.

5.3 The configuration of corporate systems such as Email, Calendar, and Contact sync services.

5.4 Corporate Wi-Fi network and internet access must be approved and supported by documented policy. This type of Wi-Fi access is limited to the physical facilities of Alight and Alight managed locations.

Please note that colleague owned mobile devices that are not compliant with the required Alight Security and Corporate IT standards will be restricted from their use of any and all corporate mobile device services. In some cases, removal of a colleague owned mobile device may be performed without notification or advanced warning due to a known security risk to Alight.

### Colleague Owned Access Registration Requirement

To comply with this specific policy, the mobile device user must agree to:

* 1. Device must be registered and be properly managed in the Mobility Freedom Program that is being governed by Alight’s Corporate IT department.
  2. Device Reset and Data Deletion rules that are documented in this policy.
  3. Device must support data encryption or user must purchase software to ensure data on the mobile device is properly encrypted and protected.
  4. The installation of Alight’s approved Mobile Device Management solution for the proper management and security of colleague owned mobile devices.
  5. Acceptance of Corporate Mobile Device Acceptable Use and all other published Global Security Services policy and standards.

### Wi-Fi Network Access

All Wi-Fi LAN access provisioned to Alight’s corporate or guest networks must use approved vendors, products and security configurations, to meet Alight published policy and standards. Alight owned assets and those explicitly allowed per this policy are the only devices that can be approved and authorized for use on Alight’s corporate or guest networks and related infrastructure.

Colleagues who are approved to use an Alight issued or personal device for business can connect to the Alight guest Wi-Fi network to access corporate systems and resources that are available via the internet. Corporate (internal) Wi-Fi network access is not allowed for Alight owned or personal mobile devices.

Home-based Wi-Fi networks are not supported by Alight or by Alight’s Global Service Desk. If a home-based wireless network is encrypted using WPA or using later technology, Alight equipment may be configured for access to the home-based wireless network.

### Monitor and Protect

Alight has the right to monitor the use of any and all mobile devices when used to access corporate applications and related systems. This is to further protect Alight from a data loss or other known corporate security risks.

* 1. Alight will monitor corporate messaging and other owned systems to ensure proper use as well as identify risks associated with business or client data that may reside on Alight issued or colleague mobile devices.
  2. Alight reserves and protects the right to modify, delete (including remote wipe procedures), and/or reset to hardware factory defaults any and all mobile devices that access corporate applications and related systems. In most cases, this level of administration can be performed remotely and with limited to no notification to the colleague.

### Device Reset and Data Deletion

Colleagues must understand and accept that Alight owned applications and related data that might reside on a mobile device will be physically removed or deleted remotely under the following circumstances:

* 1. The mobile device is reported lost, stolen, or believed to have been compromised.
  2. The mobile device is found to be non-compliant with this policy or the business need for use of the mobile device has expired.
  3. The mobile device inspection is not granted in a timely manner or in accordance with this policy
  4. The mobile device was determined to have been used inappropriately with or without the knowledge of the colleague.
  5. The mobile device belongs to a colleague that no longer is employed or has a working relationship with Alight.
  6. The colleague or their management requests the removal of the mobile device from the approved Mobility Freedom Program.

### Applicable Standards

* None

## References and Mandates

* None

## Legal Conflicts

Alight 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 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 Security Policies and Standards.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact Alight Global Security Services at global.security.services@aon.com for further guidance.

## Summary

This policy is meant to further protect Alight colleagues, corporate applications and related systems, and client data by defining the minimum level of required security controls for allowing mobile devices to gain access to corporate or guest networks and systems. This policy covers Alight issued and colleague owned mobile devices that participate in the Alight’s Mobility Freedom Program. Mobile devices considered out-of-scope or that are not specifically specified as included in Alight’s Mobility Freedom Program must be deemed unauthorized and therefore prohibited from corporate use.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_204.00 Mobile Device Security Policy |
| Primary Contact | Alight Global Security Services | [global.security.services@Aon.com](mailto:global.security.services@Aon.com) |
| Version Number | 1.4 |
| Owner | Alight Global Security Services | Information Security |
| Author(s) | Alight Global Security Services | Information Security |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | June 1, 2013 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2013 September | Original | Document published |
| 1.1 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.2 | 2015 June | 2015 Annual Review | Reviewed and validated– updated SRM to Global Security Services in the following sections: All Colleagues Responsibilities, 1.3, 2.11 and 6.5. |
| 1.3 | 2016 July | 2016 Annual Review | Information Risk and Security Services changed to Global Security Services |
| 1.4 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |