Mobile Device Policy & Acceptable Use Guidelines

Policy

Advance will issue mobile devices and appropriate associated equipment to those staff whose job descriptions indicate it is a requirement.

All requests for the issue of mobile devices must be made on the appropriate forms and authorised by the employee's line manager. Completed forms must then be submitted to ICT Service Desk along with confirmation that the user has read and understands to requirements of this policy and the Information Security Policy.

All mobile devices should be returned when an employee leaves Advance, and Advance accepts no responsibility for any personal data that has been stored directly on the device.

Advance will facilitate the use of personal mobile devices for business use, subject to compliance with the controls identified in this document and the Information Security Policy.

Purpose

The purpose of this document is to define policy, standards, procedures, and restrictions for staff, customers, Board members and contractors (end users) that have legitimate business uses for connecting mobile devices to the Advance corporate network and data.

The policy and guidelines apply to, but are not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- PDAs
- Portable gaming devices
- Laptop/notebook/ultrabook computers
- Any other mobile device capable of storing corporate data and connecting to a network

The policy and guidelines apply to any mobile hardware that is used to access corporate resources, whether the device is owned by the user or by the organization.

The overriding goal of the policy and guidelines is to protect the integrity of the confidential customer and business data that resides within the Advance technology infrastructure. The

policy and guidelines are designed to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image. Therefore, all users employing a mobile device connected to the Advance corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes for doing so.

Applicability

The policy and guidelines apply to all individuals, including full, part-time and temporary staff, Board members, contractors, customers and other agents who use a mobile device to access, store, back up, or relocate any organisation or customer-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Advance has built with its customers, supply chain partners, and other partners. Consequently, employment at Advance does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy and guidelines address a range of threats to enterprise data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an end user or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft, data protection and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of ICT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

The policy and guidelines are complementary to any previously implemented policies or guidelines dealing specifically with data access, data storage, data movement, data protection and connectivity of devices to any element of the Advance network.

This document should be read in conjunction with the **Mobile Device Care and Maintenance Instructions** in *Appendix 1* of this document and the **Information Security Policy**.

Responsibilities

The Director of Resources has the overall responsibility for the confidentiality, integrity, and availability of corporate data. The Director of Resources has delegated the execution and maintenance of information technology and information systems to the Head of ICT & Business Systems. All Advance employees and Board members are responsible to act in accordance with company policies and procedures.

Affected Technology

Connectivity of all mobile devices will be centrally managed by Advance's ICT Service Desk team and will use authentication and strong encryption measures. Although ICT Service Desk will not directly manage personal devices purchased by users, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Guidelines for Appropriate Use

It is the responsibility of anyone using a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Advance business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

Access Control

1. ICT Service Desk reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. ICT Service Desk will engage in such action if such equipment is being used in a way that puts the company's systems, data, users and customers at risk.

2. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by ICT Service Desk. ICT Service Desk will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to corporate infrastructure. If the preferred device does not appear on this list contact the ICT Service Desk. Although ICT Service Desk currently allows only listed devices to be connected to network infrastructure, it reserves the right to update this list in future.

3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to corporate data must employ, for their devices and related infrastructure, security measures deemed necessary by the ICT Service Desk. Corporate data is not to be accessed on any hardware that fails to meet Advance's established security standards.

4. All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected using technology centrally managed by ICT Service Desk. Devices that are not approved by ICT Service Desk, are not in compliance with

corporate security policies, or represent any threat to the corporate network or data will not be allowed to connect.

Mobile Device Management (MDM)

1. Advance uses a mobile device management (MDM) system to secure mobile devices and enforce policies remotely. Before connecting a mobile device to corporate resources, the device must be set to be manageable by the MDM.

2. The MDM client application must be installed on any mobile devices connecting to corporate resources. Even personal devices owned by end user's must have the client application installed. The application can be installed by contacting ICT Service Desk.

3. The MDM solution enables ICT Service Desk to take the following actions on mobile devices: remote wipe, location tracking, application visibility, and hardware feature management. If necessary features will be used to control, disable and locate the device when it is reported lost or stolen.

4. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all corporate resources, and there may be additional consequences in accordance with Advance's overarching information security policy.

Security

1. End users using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a PIN and the device will be automatically wiped after multiple failed login attempts. All data stored on the device must be encrypted using strong encryption. End user's agree never to disclose their passwords or PINs to anyone.

2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

3. Any non-corporate computers used to synchronize or back up data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by Advance's ICT Service Desk.

4. Passwords and other confidential data are not to be stored unencrypted on mobile devices.

5. Any mobile device that is being used to store Advance data must adhere to the authentication requirements of Advance's ICT Service Desk. In addition, all hardware security configurations must be pre-approved by Advance's ICT Service Desk before any enterprise data-carrying device can be connected to the corporate network.

6. ICT Service Desk will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt

and will be dealt with in accordance with Advance's overarching information security policy.

7. Employees, Board members, contractors, and temporary staff will follow all sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.

8. In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to ICT Service Desk immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than ICT. If the device is recovered, it can be submitted to ICT Service Desk for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to company business or personal. By signing this document the end user understands that personal data may be erased in the rare event of a security breach, and has agreed to this before connecting the device to corporate resources.

9. Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace, except for approved business use.

10. Applications that have not been approved by ICT Service Desk and distributed through the MDM solution are not to be used within the workplace or in conjunction with corporate data.

Hardware & Support

1. ICT Service Desk reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the Advance network.

2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jailbreaking, rooting) without the express approval of Advance's ICT Service Desk.

3. ICT Service Desk will support the connection of mobile devices to corporate resources. On personally owned devices, ICT Service Desk will not support hardware issues or non-corporate applications.

Organizational Protocol

1. ICT Service Desk can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to Advance's network may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including tracking application presence or usage, jailbreak detection, data usage, operating system version may also be monitored. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with Advance's policies.

2. The end user agrees to immediately report to his/her manager and/or Advance's ICT Service Desk any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

3. Advance will not reimburse end users if they choose to purchase their own mobile devices. Users will not be allowed to makes expense claims for mobile network usage costs.

4. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of these guidelines, end users are entitled to decline signing these guidelines if they do not understand the guidance or are uncomfortable with its contents.

5. A copy of this guidance, and related information security policies and procedures, can be found on the Advance intranet.

Guideline Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Guidelines may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The Director of Resources will be advised of breaches of these guidelines and will be responsible for appropriate remedial action.

Appendix 1

Mobile Device Care and Maintenance Instructions

1. DEVICE USAGE:

1.1. Your device will be used by you for the purposes of conducting Advance's business and you are responsible for ensuring that it is kept in good working order at all times.

All faults must be reported to the ICT Service Desk as soon as possible.

1.2. The handheld device is to be used for business purposes only and is only to be used by members of Advance staff.

1.3. The Internet connection on this handheld is for accessing Advance's information systems and limited personal use as set out in the Advance Information Security Policy. The data usage of the device may be monitored.

1.4. All devices and associated accessories remain the property of Advance at all times and must be returned if you leave Advance's employment.

1.5. Due to the high cost of mobile communications and the need for increased security private use of the Internet connection on this device is not permitted unless the device is connected to a wifi service.

1.6. The device is set up before you receive it and you must not make any attempt to change security or configuration setting (apart from device passwords), remove corporate installed software, by-pass any security features, or disassemble the device.

1.7. Protection: Always keep the device in the supplied protective case (if supplied). Do not drop the device. Do not let the device get wet or leave it in a damp place. Do not leave the device in the sun or on a heater.

1.8. Cleaning: If the device requires cleaning use a slightly damp cloth. Never attempt to clean the device with solvents.

1.9. Stylus & Screens: Touch screen devices must only be used with the supplied stylus or a fingernail. Any other object may scratch the screen and replacement styluses are available from ICT Service Desk.

1.10. Charging: This device requires charging on a regular basis and mains chargers are supplied. Car chargers can be supplied if required. Do not allow the batteries in the device to run flat; it will issue a warning message when charging is required. Always ensure the device is fully charged before you start work.

2. Security:

2.1. Do not leave the devices in your vehicle overnight.

2.2. If you must leave either device unattended in your vehicle place them out of sight, in the glove box if possible

2.3. PIN codes or passwords will be required to operate the device and access Advance's information systems and these will be issued to you with the device. Time outs will be applied to all information systems and you will be required to re-enter passwords and PINs after periods of inactivity.

2.4. Your PIN code or password must be kept safe at all times. Do not disclose them to anyone other than a member of the ICT Service Desk team and do not write them down.

2.5. The devices should be used discreetly and must not be left unattended at any time.

2.6. If you lose a device or it is stolen you must inform ICT Service Desk immediately and you may be required to provide a statement for the police if the loss has been reported to them.

3. Health and Safety:

3.1. It is against the law and a disciplinary offence to operate a laptop, handheld device or mobile phone whilst driving.

3.2. Do not use this device whilst driving or in your vehicle when the ignition is switched on.

3.3. End Users must not use their device whilst using any type of work equipment, either hand or power operated. Equipment use must stop before accessing any function of the device.

4. Care and Breakages:

4.1. Handheld devices and mobile phones are delicate and must be treated with respect. You are required to take good care of these devices and bring any faults or defects to the attention of ICT Service Desk as soon as they occur.

4.2. The user of the device will be become subject to the Non-Compliance Guidelines (above) for breakages that are considered to have been caused by neglect or reckless use. Breakages caused by failure to store the device in the supplied protective case will be considered to be neglect.

4.3. ICT Service Desk will assess damage to equipment and report all repair costs to line managers who will record each incident and decide whether the Non-Compliance Guidelines (above) apply.