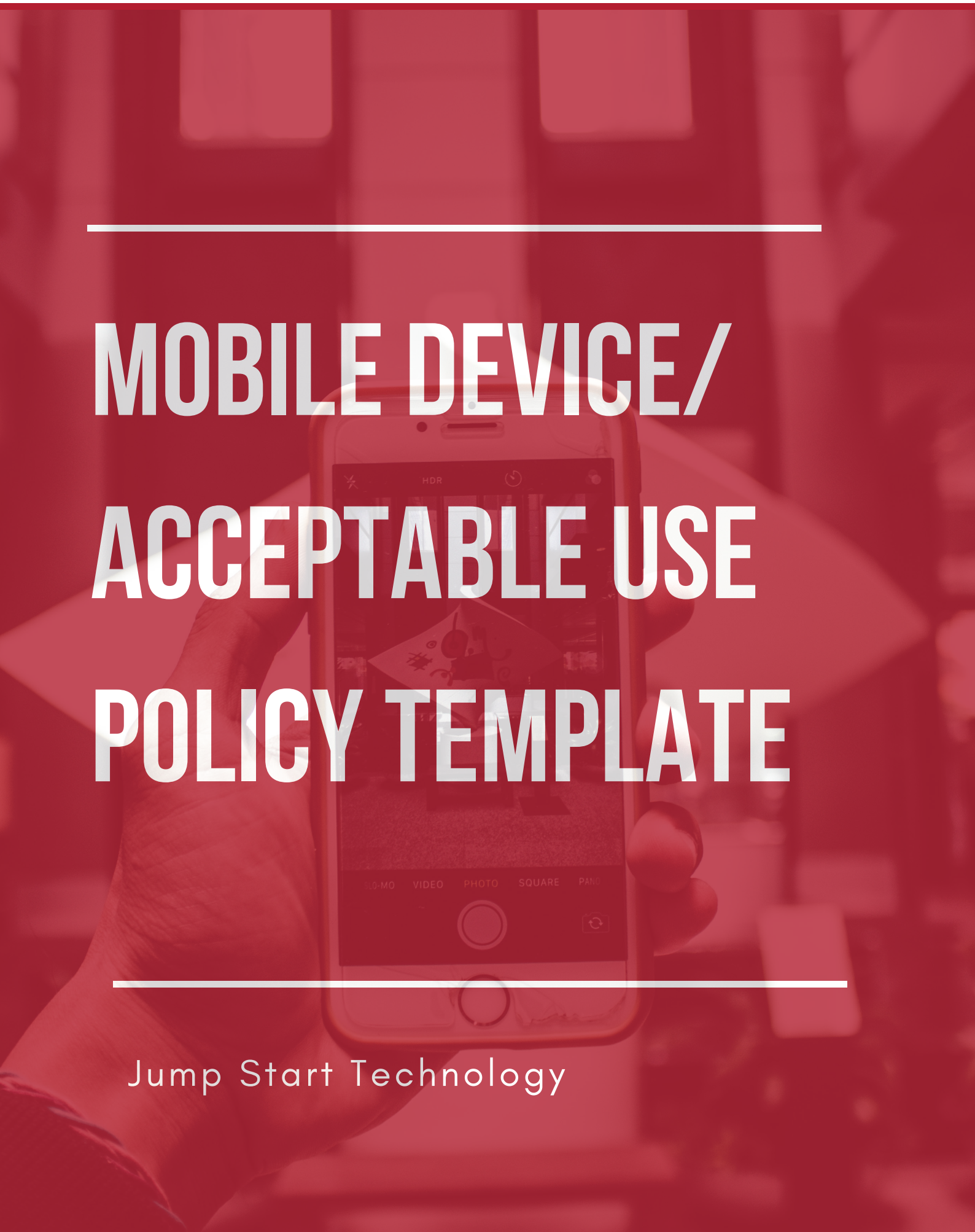
JumpStart TECHNOLOGY



MOBILE DEVICE/ ACCEPTABLE USE POLICY TEMPLATE

Jump Start Technology

Mobile Device Acceptable Use Policy

Introduction: How to Use This Template

This tool outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use mobile devices, including laptop computers, PDAs, mobile phones, smartphones, and ultra-mobile PCs to access corporate resources for business use do so in a safe, secure manner. It is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

To use this tool, fill in the blanks indicated by square brackets and delete the introductory and explanatory text in dark grey.

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of [company name]'s direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers.
- Ultra-mobile PCs (UMPC).
- Mobile/cellular phones.
- Smartphones.
- PDAs
- Home or personal computers used to access corporate resources.
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.

The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within [company name]'s technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can 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 an unmanaged network outside of [company name]'s direct control to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Applicability

This policy applies to all [company name] employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-

owned mobile device to access, store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust [company name] has built with its clients, supply chain partners and other constituents. Consequently, employment at [company name] does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

It addresses a range of threats to – or related to the use of – enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced 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 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 IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the enterprise network.

Responsibilities

The [title, example: VP, Finance] of [company name] has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

The [title, example: VP, Finance], [company name] has delegated the execution and maintenance of Information Technology and Information Systems to the [title, example CIO].

Other IT, IS, and ICT staff under the direction of the [title, example: CIO] are responsible for following the procedures and policies within Information Technology and Information Systems.

All [company name] employees are responsible to act in accordance with company policies and procedures.

Affected Technology

Connectivity of all mobile devices will be centrally managed by [company name]'s IT department and will utilize authentication and strong encryption measures. Although IT is not able to directly manage external devices – such as home PCs – which may require connectivity to the corporate network, 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.

Policy and Appropriate Use

It is the responsibility of any employee of [company name] who uses 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 [company name] business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control

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

2. Prior to initial use on the corporate network or related infrastructure, **all mobile devices must be registered with IT.** [Company name] will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored [file location or URL]. Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact the help desk at [e-mail address] or [phone number]. Although IT currently allows only listed devices to be connected to enterprise 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 enterprise data **must employ**, for their devices and related infrastructure, **a company-approved personal firewall** and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet [company name]'s established enterprise IT security standards.

4. All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by [company name]'s IT department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect. Laptop computers or personal PCs may only access the corporate network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required. Smart mobile devices such as smartphones, PDAs,

and UMPCs will access the corporate network and data using Mobile VPN software installed on the device by IT.

Security

5. **Employees** 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 **strong password**, and all data stored on the device must be encrypted using **strong encryption**. See the [company name]'s password policy for additional background. **Employees agree to never disclose their passwords to anyone**, particularly to family members if business work is conducted from home.

6. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by [company name]'s IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

7. Passwords and other confidential data as defined by [company name]'s IT department are not to be stored unencrypted on mobile devices.

8. Any mobile device that is being used to store [company name] data must adhere to the authentication requirements of [company name]'s IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by [company name]'s IT department before any enterprise data-carrying device can be connected to it.

9. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with [company name]'s overarching security policy.

10. Employees, contractors, and temporary staff will **follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required.** See [file location or URL] for detailed data wipe procedures for mobile devices.

11. In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

[Note: The following policy statement is optional. If the organization is concerned about company locations being identified in employee social media posts sent via GPS-enabled devices, include this statement.]

12. Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both corporate-owned and personal mobile devices being used within the company premises.

Help & Support

13. [Company name]'s IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.

14. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of [company name]'s IT department. This includes, but is not limited to, any reconfiguration of the mobile device.

15. IT 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 enterprise network.

Organizational Protocol

16. IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a PC, 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 [company name]'s networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains [company name]'s highest priority.

17. The **end user agrees to immediately report** to his/her manager and [company name]'s IT department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

18. [Company name] [will/will not] reimburse employees if they choose to purchase their own mobile devices. Users [will/will not] be allowed to expense mobile network usage costs [up to a maximum of $X per month].

19. Every mobile device user will be entitled to a training session around this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

20. Any questions relating to this policy should be directed to [Name] in IT, at [phone number] or [e-mail address].

Policy Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Policy 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 (i) Vice-President of Finance, (ii) Chief Operating Officer, and (iii) immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

Employee Declaration

I, [employee name], have read and understand the above Mobile Device Acceptable Use Policy, and consent to adhere to the rules outlined therein.

_____	_____
Employee Signature	Date
_____	_____
Manager Signature	Date
_____	_____
IT Administrator Signature	Date