BYOD Acceptable Use Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a personally-owned device to [company name]'s organization network for business purposes. This device policy applies, but is not limited to all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- PDAs
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing organizational data and connecting to a network

The policy applies to any hardware and related software that is not organizationally owned or supplied, but could be used to access organizational resources. That is, devices that employees have acquired for personal use but also wish to use in the business environment.

The overriding goal of this policy is to protect the integrity of the 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 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 personally-owned device connected to [company name]'s organizational network, and/or capable of backing up, storing, or otherwise accessing organizational 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 use a personally-owned device to access, store, back up, or relocate 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 or ongoing ability to use these devices to gain access to organizational networks and information.

The policy addresses a range of threats to enterprise data, or related to its use:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive organizational data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, and other threats could be introduced via devices.

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 device connectivity will be managed at the sole discretion of IT. **Non-sanctioned use of personal 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 devices to any element of the enterprise network.

Responsibilities

The [title, example: City Manager] of [company name] has the overall responsibility for the confidentiality, integrity, and availability of organizational data.

The [title, example: City Manager] of [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 employee-owned devices will be centrally managed by [company name]'s IT department and will use multi-factor authentication and strong encryption measures or alternative compensating controls to isolate and protect any organizational data accessed from or stored on the device where appropriate. Although IT will not directly manage personal devices, end users are expected to adhere to the same security protocols when connected to non-organizational equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Stipend Guidelines

[Company name] will provide a stipend of [$1500] to each eligible employee every 3 years to purchase an appropriate device that can be used for both business and personal purposes. This stipend is intended to cover

- the cost of the device
- operating system
- required business productivity applications
- anti-virus software
- 3-year service contract

All devices must be approved by IT before purchase. A checklist of minimum requirements is located here [file location or URL]. The employee may exceed the stipend amount at their own expense.

In the event of termination, retirement or resignation, the employee must reimburse a prorated amount of the stipend. The prorated amount is based on the number of weeks/months remaining in the 3 year period. For example, if the employee leaves [company name] with 78 weeks left in the stipend period [(@ ~$9.61/week)], the amount due is [$750]. OR For example, if the employee leaves [company name] with 6 months left in the stipend period [(@ ~$41.66/month)], the amount due is [$250]. The amount due will be gathered from the final pay where possible or, if not, charged to the employee to be collected within 30 days of the last day worked.

Policy and Appropriate Use

It is the responsibility of any employee of [company name] who uses a personal device to access business 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 requirement, 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 personal devices to organizational and organizational-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.
2. Prior to initial use on the organizational network or related infrastructure, **all devices must be approved by IT.** [Company name] will maintain a list of approved technologies with associated control requirements, and it will be stored at [file location or URL]. Devices that are not on this list may not be connected to organizational 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-organizational network infrastructure to gain access to enterprise data **must employ**, for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be stored on or accessed from any hardware that fails to meet [company name]'s established enterprise IT security standards.
4. All personal devices attempting to connect to the organizational network through 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 organizational network or data will not be allowed to connect. Devices may only access the organizational network and data through the Internet using an IPSec or SSL VPN connection. The SSL VPN portal web address will be provided to users as required. Smart mobile devices such as smartphones, tablets, and UMPCs will access the organizational network and data using mobile VPN software installed on the device by IT.

Security

Employees using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures. **All devices that are able to store data must be protected by a strong password**; a PIN is not sufficient. All data stored on the device must be encrypted using **strong encryption**. See [company name]'s password and encryption policy at [file location or URL] for additional background. Employees agree never to disclose their passwords to anyone, including family members, or store passwords on personally-owned devices if business work is conducted from home.

5. All users of personally-owned devices **must employ reasonable physical security measures**. End users are expected to secure all such devices 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.
6. Any non-business computers used to synchronize with these devices will have installed **up-to-date anti-virus and anti-malware software deemed necessary** by [company name]'s IT department. See [file location or URL] for anti-virus requirements and recommendations.
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 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 must be pre-approved by [company name]'s IT department before any enterprise data-carrying device can be connected to the organizational network.

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 that security implementation will be deemed an intrusion attempt** and will be dealt with in accordance with [company name]'s overarching security policy.
10. 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.
11. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to **permanently erase company-specific data from such devices once its use is no longer required**. See [file location or URL] for detailed data wipe procedures for eligible devices.
12. In the event of a lost or stolen device, it is incumbent on the user to report the incident 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. **Appropriate steps will be taken to ensure that company data on or accessible from the device is secured - including remote wiping of the device where appropriate. The remote wipe will destroy all data on the device**, whether it is related to company business or personal.

Help & Support

13. Employees who opt in to the BYO program are not eligible for support for device-specific hardware or software from [company name]'s IT department. If the employee-owned device requires maintenance, the employee is responsible for taking the device to an employee-provided third party as covered by the stipend or business-approved third party support provider [support provider name]. IT will provide the employee with a business-owned device [laptop, desktop, thin client] for the duration of the maintenance period.
14. [Company name]'s IT department will triage support calls to determine if the issue is software or hardware related. If the issue is hardware related, the employee will be forwarded to the third-party support provider for maintenance. If the issue is software related or related to virtual or web-based applications, [company name]'s IT department will perform maintenance.
15. Employees, contractors, and temporary staff 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 or "jail-breaking") without the express approval of [company name]'s IT department.

Organizational Protocol

16. IT 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 organizational 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 [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. The employee consents that there is no right to privacy related to use of organizational networks, resources, or data.** This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties.
17. The end user agrees t**o 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. Users [will/will not] be allowed to expense mobile network usage costs [up to a maximum of $X per month]. Reimbursement details are available at [location or URL].
19. While a personally-owned device user will not be granted access to organizational resources 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. By signing this policy, employees acknowledge that they fully understand the risks and responsibilities of the BYO program.
20. Any questions relating to this policy should be directed to [name] in IT, at [phone number] or [e-mail address]. A copy of this policy, and related policies and procedures, can be found at [location or URL].

Policy Non-Compliance

Failure to comply with the *BYOD 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, possible termination of employment, [as well as possible criminal charges]**.

The (i) City Manager, (ii) Chief Information Officer, and (iii) immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action.

Employee Declaration

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

_____	_____
Employee Signature	Date
_____	_____
Supervisor Signature	Date
_____	_____
CIO/IT Administrator Signature	Date