


# Personal Device Acceptable Use Policy

The policy applies to any hardware and related software that is not owned or supplied by the county, but could be used to access county resources. That is, devices that employees have purchased 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 employee, business and taxpayer data that resides within Sangamon County'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 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 county's public image. Additionally, it is important to note that such a breach could result in the employee's personal device being "wiped clean." It is also critical to note that the use of such personal devices could make those devices subject to FOIA or forfeiture of the device in the event of certain legal action involving the county. All users employing a mobile device connected to Sangamon County's network, and/or capable of backing up, storing, or otherwise accessing county data of any type, must adhere to county-defined processes for doing so.

## Applicability

**This policy applies to all Sangamon County employees**, including full and part-time staff, contractors, interns, and other agents who use a personally-owned mobile device to access, store, back up, or relocate any organization or county data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Sangamon County has with the larger community. Consequently, employment at Sangamon County does not automatically guarantee the initial or ongoing ability to use these devices to gain access to networks and information.




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 network.

# Access and Approval

The Director of Information Systems (I.S.) of Sangamon County has the overall responsibility for the confidentiality, integrity, and availability of county data.

Access will be approved (in writing) by the employee's supervisor who will forward the approval to the I.S. Director (or his liaison). Written approval will be sent back to the supervisor who will inform the employee they have been approved under the policy. **Note:** the Employee MUST sign the "Employee Declaration" indicating they've read the policy and accept the terms therein.

Connectivity of all mobile devices will be centrally managed by Sangamon County's Information Systems department and will use authentication and strong encryption measures. Although Information Systems will monitor personal devices, end users are expected to adhere to the same security protocols when connected to non-county 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 Sangamon County who uses a mobile device to access county 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 Sangamon County 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. Information Systems reserves the right to refuse, by physical and non-physical means, the ability to connect personal mobile devices to county and county-connected infrastructure. Information Systems will engage in such action if such equipment is being used in a way that puts the company's systems, data, and users at risk.

2. End users who wish to connect such devices to non-county network infrastructure to gain access to enterprise data **must employ**, for their devices and related infrastructure, security measures deemed necessary by the Information Systems department. Data is not to be accessed on any hardware that fails to meet Sangamon County's established enterprise Information Systems security standards.

3. All personal mobile devices attempting to connect to the county network through the Internet will be inspected/approved using technology centrally




managed by Sangamon County's Information Systems department. Devices that have not been previously approved by Information Systems, are not in compliance with the county's security policies, or represent any threat to the county network or data will not be allowed to connect.

## Security

4. 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 or PIN.** Employees agree to never disclose their passwords to anyone, even to family members, if business work is conducted from home. **Security Breaches can result in having the user's device "wiped clean." This will result in the complete loss of personal data.**

5. All users of mobile 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-county computers used to synchronize with these devices will have installed **up-to-date anti-virus and anti-malware software**.

7. Sangamon County/Information Systems 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 Sangamon County's security policy.

8. 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**.

9. **In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to Information Systems immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than Information Systems. This action will restore the device to its factory default settings**. If the device is recovered, it can be submitted to Information Systems for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to county business or personal. This data is not recoverable on the device itself, but can usually be restored from a backup on another device (e.g. a personal computer) if the mobile device remains in or returns to the user's possession, or a new device is able to store the backup. It is recommended that users back up their personal data frequently to minimize loss if a remote wipe is necessary. By signing this document the user understands that their personal data may be erased in the rare event of a security breach, must be agreed with before connecting the device to county resources. When a remote wipe is initiated by the Information Systems department, the user's

mobile device will be wiped of all data and restored to its factory default settings. The wipe is not limited to county data. Data that the employee has added to the device for personal use will also be deleted. This data is not recoverable on the device itself, but can usually be restored from a backup on another device (e.g. a personal computer) if the mobile device remains in or returns to the user's possession, or a new device is able to store the backup. It is recommended that users back up their personal data frequently to minimize loss if a remote wipe is necessary. Examples of situations requiring remote wipe include, but are not limited to:

10. Theft of the device.

11. Loss of the device.

12. Termination of employment in which the user has not already cleared county data by another method.

13. 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.

14. Non-Business usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.

## Organizational Protocol

15. Information Systems can and may (at their discretion) 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 county 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 Sangamon County'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 monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties.

16. The end user agrees t**o immediately report** to his/her manager and Sangamon County's Information Systems department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

17. Any questions relating to this policy should be directed to Charlie Stratton in Human Resources, at Charlie.Stratton@sangamonil.gov.




## Policy Non-Compliance

Failure to comply with the *Personal Mobile Device Acceptable Use Policy* may, at the full discretion of the county, result in the **suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment**. The immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action.

## Confidentiality

Any county employee utilizing personal mobility device(s) as defined in this policy to access the Sangamon County network maybe subject to the Illinois Open Records Act and Freedom of Information Act (FOIA).




# Employee Declaration

I, [employee name], have read and understand the above *Personal Device Acceptable Use Policy*, and consent to adhere to the rules outlined therein. I further understand and accept that my personal data may be removed from my device at the sole discretion of Sangamon County.

**Employee:**

| Signature | Print or Type Name | Date |
|---|---|---|

**Elected Official/Dept. Head**

| Signature | Print or Type Name | Date |
|---|---|---|