The University of the South
Mobile Device Policy

Purpose

University employees may use mobile technology to access information technology resources of the University. The purpose of this policy is to minimize risk, especially in the event of loss or theft by describing the conditions under which the University permits the use of mobile devices for its employees who wish to access information or conduct University business through the use of a mobile device. This policy is intended to ensure the integrity of University data that might be transmitted or stored on mobile devices used by employees regardless of whether the device is the property of the University or personal property.

Scope

The policy applies to all University of the South faculty, staff, contractors, vendors and others who are granted access to the University of the South resources. All usage must comply with state and federal laws, as well as the University's policies governing appropriate use of technology.

Responsible Party

The Associate Provost of the Library and Information Technology Services division of the University is responsible for maintaining this policy and may be contacted with any questions.

Definitions

Term	Definition
G Suite for Education	The G Suite for Education (formerly called Google Apps for Education) core services are the heart of Google's educational offering to schools. The core services are Gmail (including Inbox by Gmail), Calendar, Classroom, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts and Vault.
Information Technology (IT)	Information Technology is part of the Library and Information Technology Services division of the University. IT is charged with establishing, monitoring and maintaining information technology systems and services. IT includes both the Technology, Access and Support department and the Strategic Digital Infrastructure department.
Mobile Device	A mobile device is a telecommunications and/or computing device small enough to hold and operate in the hand. Often they are referred to as smartphones or tablets. These devices can be used to connect to G Suite for Education, web-based software or apps provided by the University.
Sensitive or confidential Information	Data that carries the risk of adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education or employment records was disclosed as well as any adverse effects experienced by the organization that maintains the PII. Examples include social security numbers, credit card numbers, bank account information or any data that can specifically identify an individual.

Policy

1.0 Mobile Device Security Policy
If an employee, either due to work-related requirements or through their own personal choice, elects to access the University's resources, including email, via a mobile device, they must adhere to the security policies defined by the University. The mobile security policies are designed to accomplish the following primary objectives.

- **Password requirements**
    1) The device must be configured with a password, security gesture or biometrics.
    2) If a password is used, the minimum length of the password will be 4 characters. Longer passwords are encouraged if the device has the capability.

- **Idle device locking**
  After 10 minutes of inactivity, the device will lock and not display data. The user will be required to enter their device password to unlock the device.

- **Remote erasure**
    1) If a device is lost, stolen or taken out of service, the user will have the ability to erase all University GSuite data on the portable device remotely. This is done by logging into your GSuite account and accessing the security settings. The technology helpdesk will also be able to assist users with this.
    2) In the event of 10 failed login events, the device will automatically remotely wipe the device of any University GSuite data.

2.0 Personally Owned Mobile Devices

The University recognizes and allows employees to connect personally owned mobile devices to the University's resources to access and synchronize email data, contacts, and calendar information. All usage must comply with state and federal laws, as well as with the University's own policies governing appropriate use of technology, including but not limited to the security requirements set out in this Moblie Device Policy.

3.0 Sensitive or Confidential Information

Sensitive or confidential information can only be stored on University owned mobile devices when there is a business need and should be removed when the business need no longer exists.

Sensitive or confidential information should not be stored on personal mobile devices.

4.0 Report a Lost or Stolen Mobile Device

The employee must provide prompt written notice to the Associate Provost for Library and Information Technology Services upon becoming aware of, or have reason to believe that University information (including email) has, or may have been, lost or compromised as the result of:

- A third party gaining unauthorized access to data stored on their device; or
- Inadvertent forwarding or sharing data with unintended recipients; or
- The theft or loss of their device or the accidental loss of data stored on their device.

5.0 Employee Termination

Employees using personal mobile devices are required to delete any University of the South data stored on their device immediately upon termination of employment (voluntary or involuntary).

6.0 University Rights

The University of the South reserves the right to disconnect devices or disable services without notification.

Consequences

Anyone found to have violated this policy may be subject to disciplinary action, up to and including immediate termination.

Failure to provide prompt written notice to the Associate Provost of Library and Information Technology Services will hinder the organization's ability to comply with its statutory obligations which may lead to third party legal claims that will expose the organization and the employee to potential liability.

Responsibilities

The Strategic Digital Infrastructure staff is responsible for reviewing security features of the email system and making them available to the faculty, staff and students of the University.

REVISION DATE: August 24, 2021