Policy # 56015

MOBILE DEVICE, CELL PHONE & HOT SPOT POLICY

Effective Date: February 1, 2024
Responsible Office: Information Technology and Human Resources Management
Division: Operations

I. PURPOSE/OBJECTIVE

Using mobile devices, including cell phones, in the workplace can potentially introduce risks to Grambling State University's (GSU) security environment. Mobile devices are those that provide convenient access and flexibility to GSU network and computer resources, and they can be personally owned, or they can be GSU managed, owned, and maintained.

Mobile Devices are commonly used to access GSU's networks and other information resources by employees, faculty, guests and other affiliates. In an effort to minimize potential security threats and to provide guidance on proper use and expectations, this policy outlines requirements for use of such devices.

II. Definitions

Mobile Device: a piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer.

Cell Phone: portable telephone that can make and receive calls over a radio frequency link while the user is moving within a telephone service area.

Hot Spot: a physical location where people can access the Internet, typically using Wi-Fi, via a wireless local area network (WLAN) with a router connected to an Internet service provider.

Wi-Fi: a wireless networking technology that uses radio waves to provide wireless high-speed Internet access.

III. STATEMENT OF POLICY

A. Personal and GSU Owned Device Requirements

The following provides security measures and requirements for the use of personal and GSU owned devices used to access GSU's resources, including mobile phones, tablets, laptops, etc.

1. Users of mobile devices utilizing University information resources have the responsibility to take appropriate measures to protect such devices for the prevention of theft, data loss, etc**.**

2. While using mobile devices on GSU resources, regardless of personally owned or GSU owned, user must abide by all applicable University computer and information security policies.

3. Company passwords and email accounts cannot be used for obtaining or accessing personal services, accounts, personal subscriptions, etc. (Facebook, LinkedIn, etc.) Access to mobile devices must be secured using a strong password or a security passcode/pin of 6 or more characters as this enforces encryption and protects GSU's data and information in case of physical loss or theft of such device. Any laptop or tablet, owned by GSU or personally owned must have an appropriate password adhering to industry standards for secure password management. MFA (Multi-factor Authentication) is required for any app or service that offers this capability. MFA will require at least two factors of authentication before access to device or app is granted. Factors of authentication may include a password and/ or a code sent to a different cellphone, email address, etc. than the one you are attempting to access.

4. GSU's email, files, data, etc. are the property of the institution and may not be copied, transferred, etc., in a manner that is inconsistent or violates University policies.

5. Refrain from taking pictures with any device that may disclose inside look at trade secrets, inventions, technical, data, confidential data, etc.

6. Devices must be properly secured at all times to prevent theft or loss. Loss or theft must be reported to IT and Safety and Risk Management as soon as possible.

7. All mobile devices should have proper anti-virus, end point detection and response, or other security software installed and updated regularly.

8. All devices should have regular Operating System (OS) updates installed promptly and in a reasonable time after release by the manufacturer.

9. Devices should be configured to auto-lock after a reasonable time of inactivity.

10. All GSU issued Cell Phones, Mobile Devices, Laptops and accessories must be turned in to ITC, prior to last day of employment or immediately upon separation or affiliation with GSU. Once equipment is collected, ITC will terminate service.

B. GSU Assets Use Requirements

GSU understands and recognizes that incidental personal use of GSU assets and mobile devices may occur. Such use must be limited in nature so as to not jeopardize the confidentiality, integrity or availability of GSU network and computer resources. The following section provides security measures and requirements for the use of GSU issued cell phone services, mobile devices, peripherals, hot spots, etc.:

1. Users of GSU assets must abide by all applicable University policies.
2. All employees will be required to review and acknowledge this policy upon onboarding and on an annual basis by the Human Resource's department.
3. Unauthorized use of GSU devices by non-employees is strictly prohibited.
4. Lost or stolen GSU assets or mobile devices must be reported to the employee's supervisor and the IT Department immediately. Specific facts may require, a police report and/or a claim with GSUPD and the Department of Safety and Risk Management.

C. GSU Asset, Mobile Device, Cell Phone or Hot Spot Request Process

1. Issuance of a GSU owned mobile device will begin with a work order ticket by the requesting department.
2. Review of such request will be based on justification of work responsibilities, travel, emergency services and operational needs.
3. Upon review of request, an employee will be required to read and attest to the Mobile Device, Cell Phone & Hot Spot Policy prior to receiving mobile device.
4. All equipment and acknowledgements will be tracked and documented by ITC.
5. After initial acquisition, all individuals in receipt of a GSU Mobile Device, Cell Phone or Hot Spot will be required to acknowledge and attest to this policy on an annual basis.
6. Employees are responsible for returning equipment prior to departure or upon termination of employment or affiliation with GSU.
7. Monthly service fees must be approved for payment by department. It is the responsibility of the department that purchases the devices to ensure payments are made.

IV. APPLICABILITY

This policy applies to employees, faculty, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties that may access GSU's network. This policy applies to any device, individual, peripheral or service, both owned or not owned by GSU, that is used to access information resources, networks and systems (i.e. WIFI, Email, Cell Phone, Hot Spot, etc.). There is no expectation of privacy while using GSU owned cell phones or mobile devices.

V. MONITORING

GSU reserves the right to monitor cell phone usage including minutes, data, and the contents of voicemail for any person/s utilizing GSU issued devices in accordance with University policies.

VI. ENFORCEMENT

Violations of this policy by an employee may result in disciplinary action, in accordance with GSU's information security policies and procedures and human resources policies. Use of any device utilizing or accessing GSU's networks or its information resources is a privilege and not a right. Disciplinary action may include but is not limited to, termination, referral for prosecution or restitution of costs incurred for fees or damaged university property.

VII. REVISION/REVIEWED

Signatures

Employee _____ Date _____

Human Resources _____ Date _____

Information Technology _____ Date _____