Minnesota State Colleges and Universities
System Procedures
Chapter 5 – Administration
Procedures associated with Board Policy 5.22

5.22.2 Cellular and Other Mobile Computing Devices

Part 1. Purpose

Electronic communication is an important part of contemporary business practices, including the operations of colleges, universities, and the system office. The standards and responsibilities in this procedure are supplemental to other applicable board policies and system procedures including, but not limited to, Board Policy 5.22 and System Procedure 5.22.1. This procedure clarifies college, university, system office, and employee responsibilities associated with system-owned cellular devices and mobile computing devices and use of employee-owned cellular and mobile computing devices for system business.

Part 2. Definitions

Cellular device
A cell phone or a mobile computing device with voice capability.

Mobile computing devices
Portable computing and telecommunications devices that can execute programs. Examples include, but are not limited to: laptops, tablets, and cell phones with internet browsing capability. Use of a mobile computing device may or may not require a wireless communication service plan or incur connection charges.

Department cellular device
A system cellular device purchased and maintained by a college, university, or system office department or division for use by more than one employee or other authorized user while engaged in their assigned duties.

Other wireless communication service
A subscription-based communications service that relies on commercial cellular services for data or voice transmissions. These services are often marketed using names such as mobile content, wireless music services, cellular services, mobile data services, text messaging services, digital cellular services, mobile wireless services, mobile data services, wireless data services, wireless telecommunications services, analog cellular services, cellular data services, etc.

System cellular device or plan
A system cellular device or service plan provided to an employee by a college, university, or the system office for business purposes.

Voice over Internet Protocol applications or VoIP

Voice over Internet Protocol applications and related devices are outside the scope of this procedure. The downloading of VoIP applications onto system-owned equipment is governed by System Procedure 5.22.1, Part 4, Subpart B(4), Acceptable Use of Computers and Information Technology Resources.

Part 3. Eligibility for System-Owned Cellular Device, Mobile Computing Device, or Other Wireless Communication Service Plans

A college, university, or the system office may provide a cellular device or a mobile computing device, or other wireless communication service plans to an employee if it is determined by the college, university, or the system office to be a necessary business expense under one or more of the following criteria:

a. Availability of device and service is integral to the performance of specific duties within the employee's job description.
b. A substantial portion of the employee's work is conducted outside of the building or buildings where the employee is assigned to work.
c. The employee does not have an assigned office or workspace and needs to be contacted on a regular basis by the college, university, or system office constituents for assigned services or to provide needed information.
d. It is a job requirement that the employer be able to reach the employee outside of the employee's normal work hours.
e. The mobile computing device is for use by a faculty or staff member and is intended to replace or complement a desktop computer.

A college, university, or the system office is not required to provide a device or service plan and is expected to periodically review the continued need and finances associated with the devices as a general management practice.

Part 4. Authorization

Authorizing administrators are expected to implement and oversee this procedure for business-related purposes in accordance with board policy, other applicable system procedures and law.

Subpart A. Authorization

To be approved for a system-owned device (and service plan, if applicable) under this procedure, the following procedures are applicable:

1. The supervisor of an employee requesting the device, service and/or service plan must determine if the employee meets the threshold eligibility requirements in Part 3.
2. A device/service/service plan shall be issued only if approved by an authorized administrator of the college, university, or system office.
3. The authorizing administrator must obtain and retain a written verification, signed by the employee, acknowledging receipt of the applicable board policies and system procedures governing the employee's use of the device/service/service plan.
4. Documentation to support the decision to issue the device and plan must be retained by the appropriate administrative unit at the college, university, or system office consistent with the records retention schedule and be available for review and audit.

5. Colleges and universities are encouraged to procure devices, services, and plans under state or system negotiated contracts when possible.

Subpart B. Employee annual review

The supervisor is responsible to annually review and document the continued business need for the device, service, and/or plan. Mobile computing devices issued pursuant to Part 3-e shall not be subject to the requirements of this Subpart.

Part 5. Employee Responsibilities

System employees are responsible for appropriate use of all system-owned cellular and mobile computing devices. Employees are expected to adhere to the highest ethical standards when conducting system business and follow System Procedure 1C.0.1 Employee Code of Conduct and related laws, policies, and procedures.

1. An employee who receives authorization under this procedure is responsible for ensuring that the system owned device is available for service during applicable business hours and as needed.
2. The employee shall immediately return the device upon request by the employee's supervisor or upon the end of employment.
3. The employee shall comply with the provisions of this procedure including participation in the annual review of continued authorization for a system owned device, except as otherwise noted.
4. The employee shall report any changes the employee's eligibility criteria for the authorization; an authorization will be deemed withdrawn when the employee's eligibility criteria is no longer met.

Part 6. Cellular Devices

Subpart A. Personal use

System cellular devices and services are intended for system business. In accordance with Minn. Stat. § 43A.38, Board Policy 5.22, System Procedure 5.22.1, Minnesota Management and Budget Human Resources/Labor Relations Policy #1423, personal use of a system cellular device and plan is allowable only for limited and reasonable incidental and de minimis use. De minimis use is personal use that does not result in any additional costs or loss of time or resources, or results in an incremental cost or loss of time that is so small so as to make accounting for it unreasonable or administratively impractical. Incidental use means personal use that is of minimal duration in length and frequency. Personal use of a system cellular device or service in violation of this procedure or other system work rules may result in revocation of the employee's authorization and possible disciplinary action against the employee.

The system reserves the right to seek reimbursement for excessive personal use of any system-owned mobile computing device. In order to avoid commingling personal and system calls, porting a personal cellular number to a system billing account is prohibited, as is porting a system cellular number to a personal billing account.

Subpart B. Monthly review of invoices
The employee must review and initial the cellular device invoice monthly and identify any use not permitted under this procedure before submitting the invoice to the employee's supervisor or authorized administrator assigned to review and approve the monthly cellular device bill.

Subpart C. Payment options for cellular devices and plans
Colleges, universities, and the system office may pay for business-related cellular devices, services, and/or service plans only through either reimbursement to the employee for occasional, incremental actual expenses or direct payment to a vendor for a cellular device, services and/or service plan owned and managed by the college, university, or system office unless otherwise authorized by a collective bargaining agreement.

Subpart D. Reimbursement for occasional, incremental actual expenses
Occasional business call expenses made from an employee's personal cellular device are eligible for reimbursement if:

1. The employee has not been issued a cellular device by a college, university, the system office, or the assigned cellular device does not receive service in the area from or to which the call was made; and
2. The employee has incremental costs directly attributable to the business calls.

Reimbursement will be made in accordance with guidance provided by the system office.

Subpart E. Personal calls while on travel status
Certain bargaining agreements or compensation plans provide that an employee in travel status overnight may claim expense reimbursement for actual personal telephone calls up to a defined limit. In addition to the incidental and de minimis use provided for in Part 6, Subpart A, employees who are issued a cellular device may make limited personal calls in lieu of claiming such reimbursement for calls while in travel status.

Subpart F. Department cellular devices, services and service plans
A college, university, or the system office may purchase cellular device equipment and service plans if the college, university, or the system office determines the cellular device is necessary for the efficient operation of a department and the cellular device will be used by more than one individual.

1. A department cellular device may be provided to meet the department's business purposes. The equipment is designated as property of the college, university, or system office and must be returned to the department daily or as required. Examples of such department users might include, but are not limited to, parking cashiers, delivery drivers, maintenance, or security personnel who need to be accessible by phone during their work shift.
2. Purchase of department cellular device equipment or service plans must be approved by an authorized administrator. At the time of purchase, the responsible party for each department cellular device must be identified. The responsible party must perform the actions required under this procedure.

Part 7. Employee-Owned Cellular or Other Mobile Computing Devices

Subpart A. Acknowledgement of responsibilities

Employees who use employee-owned devices for system work inevitably create electronic records on those devices relating to their system work. These records, including text messages, voicemails, emails, and other electronic communications are government data, as defined by the Minnesota Government Data Practices Act, Minn. Stat. chapter 13 (heretofore referred to as the the Act). System employees are expected to manage government data in their possession consistent with the Act and applicable retention and security policies, wherever that data are located, including on employee-owned cellular or other mobile computing devices. Government data should not be stored solely on an employee-owned device but should also be saved on a system network drive.

System employees who choose to use their personal cellular or other mobile computing devices for system business do so subject to the following provisions:

1. User shall delete any sensitive business files that may be inadvertently downloaded and stored on the device as soon as possible. Employees should consult with their supervisors, as needed, with questions about the handling of sensitive business information.
2. User shall employ an authentication method to access the device. Acceptable methods include: passwords, pins, or biometric features as available.
3. User shall use device encryption technology where possible to encrypt not public government data stored on the device.
4. User shall make his/her best effort to ensure that government data stored on the employee owned device is not accessible to individuals not authorized to access such data, including, if necessary, by closely monitoring or denying use of the device by individuals not authorized to access the government data stored on the device.
5. User shall keep the software and operating system of the device updated and in good working order.

Additionally, appointing authorities may require the installation of security software on an employee-owned device as a condition precedent for accessing the appointing authorities' email and information technology systems through the device. Appointing authorities reserve the right to reject the use of a personal device for business purposes when it is determined that the device is insufficiently secure.

Subpart B. Privacy

When needed to respond to requests under the Act for data that is not otherwise available to the employer, employees shall to the extent it is reasonably feasible to do so provide a copy of government data that is on their device and be responsive to the request. The employer shall not copy, retain or use for any purpose non-government data provided.

Subpart C. Advisory

Employees should be aware that by using an employee-owned device for system business, the employee's actions may result in the creation and recording of: a) government data as that term is used in the Minnesota Government Data Practices Act, and/or b) education data as that term is defined in the Family Educational Rights and Privacy Act, on the employee owned-device. If such data is created and/or stored on the device it is subject to the provisions of this procedure

and may be subject to other legal requirements. Employees are reminded to carefully consider the implications of creating or storing sensitive private government data on employee-owned devices. Employees are expected to maintain the security and privacy of any such data.

Subpart D. Lost or stolen devices
When an employee-owned device containing government data is lost or stolen, it is important to take steps to protect the security and privacy of the data and comply with applicable breach notification requirements. Once an employee is certain that an employee-owned device used for business purposes has been lost or stolen, the employee must promptly report the incident, usually by the next business day, to his/her human resources office. The employee may be asked to provide evidence that the device has been remotely wiped or otherwise made inoperative in order to assure the security of the government data that may be present on the device. Employees who back up their employee-owned device to a remote storage facility may be asked to make business information stored within the storage facility available to the appointing authority to ensure access to important business information is maintained by the appointing authority.

Subpart E. Technical support and management of employee-owned mobile devices
System IT staff will provide best efforts to support the installation and connection to the system infrastructure and network resources. All other support-related issues must be directed to the mobile device service provider.

Subpart F. Reasonable accommodations
Under applicable law and board policy, the system may be required to accommodate a qualified individual with a disability who uses an employee-owned mobile device at work that enables the employee to perform the essential functions of the job. Employees who wish to request a reasonable accommodation should contact the appropriate campus or system office personnel.

Part 8. Employee Safety

System employees are highly discouraged from using mobile devices to make a phone call while operating a motor vehicle in the conduct of system business, except for the purpose of obtaining or rendering emergency assistance. Employees are reminded that the use of a mobile device for non-telephone communication (e.g., texting) is illegal in Minnesota while operating a motor vehicle per Minn. Stat. §169.475.

Date of Adoption: 04/05/10
Date of Implementation: 04/01/16
Date of Last Review: 03/16/16

Date and Subject of Amendments:
05/25/16 - amended part 7, Subpart B and C to incorporate specific reference to state and federal law.
03/16/16 - Effective April 1, 2016, amended Part 1, to include employee-owned devices. Updated definitions of mobile devices. Amended Part 3 to include mobile devices that replace or compliment computers. Amended Part 4 to require a periodic review of needs

and retention of written verification. Amended Part 5 clarifying employee expectations. Amended Part 6 to clarify personal use. Added new Part 7, Employee-Owned Cellular and Other Mobile Computing Devices and Part 8, Employee Safety. Applied new writing and formatting standards.

04/2/15 - created new Part 2, Subpart E to clarify that devices and plans provided to employees for business purposes are property of the system. Amended Part 6, Subpart A, Subpart E and Subpart F to clarify that personal use of such devices and plans are governed by state statute and are allowable only for incidental and de minimis use; and specify repercussion of improper use.