Personal Device Security Policy for Chicago State University Systems

Policy Statement

Various types of personal devices at Chicago State University (CSU) allow faculty and staff to be more mobile and productive in meetings, classroom lectures, off campus, and conducting university business from those devices. While computing technology is constantly evolving, it presents new vulnerabilities and risks in securing sensitive data and information in the use of personal devices and mobile devices. CSU, in compliance with the State of Illinois, creates a personal device security policy to minimize sensitive data and information that potentially can be exploited as a result of a theft or a lost device. The policy and procedures apply to all faculty and staff who use a university owned personal device. Individuals assigned to a university personal device are responsible for securing the personal device and adhering to these procedures, regardless of whether the personal device is used in the office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport.

Purpose

The purpose of this policy is to define the use of university supplied desktop, laptop computers and mobile devices such as, but not limited to tablets and smart phones and smart devices when accessing CSU Information Resources.

Scope

This policy, and all policies referenced herein, shall apply to all University-Related Persons / Employees / Staff, Associates / Contractors or 3rd parties, and Students who use a University supplied personal device to access, or otherwise employ, locally or remotely, CSU's Information Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions

- **University-Related Persons / Employee / Staff** are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University.
- **Associate / "Extra Help", Third-party or 3rd party** is someone officially attached or connected to the College who is not a student or employee (e.g., Extra Help, vendors, interns, temporary staffing, volunteers.)
- **ITD Resources / Information Resources** - include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, security, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
- **Information System** is a major application or general support system for storing, processing, or transmitting University Information. An Information System may contain

multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

- **Information Technology Department** is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.
- **Unit** is a college, department, school, program, research center, business service center, or other operating component of the University.
- **A patch** is a software update comprised of code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:
    - Updating software
    - Fixing a software bug
    - Installing new drivers
    - Addressing new security vulnerabilities
    - Addressing software stability issues
- **Patch management cycle** is a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. Patch management occurs regularly as per the Patch Management Procedure.
- **University Information** is any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.
- **Security Awareness Training** - The formal process for educating employees about the internet and computer security. A good security awareness program should educate employees about institutional policies and procedures for working with information technology (IT).
- **Personally Identifiable Information (PII)** - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
- **Education records under FERPA**, which - with limited exceptions - means all records in any format or medium that are directly related to a student and are maintained by the College.
- **Health Insurance Portability and Accountability Act (HIPAA)** - Demands that all HIPAA covered businesses prevent unauthorized access to “Protected Health Information” or PHI. PHI includes patients' names, addresses, and all information pertaining to the patients' health and payment records.

- **Gramm-Leach-Bliley ACT (GLBA)** - Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data.
- **Functional Lead** - Technical lead point person for a department. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to ITD.
- **The Family Educational Rights and Privacy Act (FERPA)** - a Federal law that protects the privacy of student education records.
- **Information Owner** - is a person responsible for the management and fitness of information elements (also known as critical data elements) - both the content and metadata.
- **Backup** is saving or copying information onto digital storage media.
- **Restore** is performed to return data that has been lost, stolen, or damaged to its original condition or to move data to a new location.
- **Recovery Point Objective** (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.
- **Recovery Time Objective** (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.
- **Electronically stored information (ESI)** is the general term for any electronic information stored on any medium (i.e. hard drive, back-up tapes, CDs, DVDs, flash drives, external drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
- **Archive** is defined as the saving of old or unused files on off-line mass storage media for the purpose of releasing on-line storage space.
- **Disaster Recovery** is a combination of the policies, process and procedures related to preparing for recovery of technology infrastructure critical to CSU operations after a natural or human induced event. Disaster recovery focuses on the restoring technology systems that support business functions that fail in the event of a disaster.
- **Bring Your Own Device (BYOD)** refers to employees who bring their personal devices to work, whether laptop, smartphone, or tablet, in order to interface to the corporate network.

Responsibility

The Personal Device Security Policy for CSU applies to all active members of the University-Related Persons / Employees / Staff, Associates / Contractors or 3rd parties, and Students who use a University supplied personal device to access University Information Resources.

Policy

General

- New personal device purchases are performed by respective department using "CSU Buy". The three acceptable hardware manufacturers for computing purchases are Apple, HP, and Dell. The ITD hardware template listing the components to include when ordering a new laptop can be found on ITD Network website @ http://www.csu.edu/itd/networkInfrastructure/networkSupport/internetaccess.html.
- Newly purchased personal devices will be tagged by Property Control (PC). Central Receiving will deliver all computing devices to ITD – Network Infrastructure in DH -122 after Property Control completes the tagging of the personal device. Property Control will create a "property control card", that contains the devices' serial and tag numbers. The "property control card" will be attached to or packaged with the device and delivered to the end-user for record purposes. The card must remain in the possession of the user assigned to the personal device at all times.
- ITD –Network Infrastructure, will call the department that purchased the personal device to request the name of the user(s) and provide a tentative date for delivery to the receiving department.
- ITD – Network Infrastructure will image the device with the basic office suite, anti-virus software, place security and authentication applications on laptops. Upon completing these tasks, ITD will make arrangements to deliver the hardware to the department that purchased the hardware.
- University owned personal devices in circulation prior to the establishment of this policy, must be brought to the ITD Help Desk (1st floor of the library), so that updates can be made to meet the university's servicing requirements. Department/individuals must provide specific name of the user that will be assigned to the laptop.
- The department must contact Property Control to obtain a "property control card" for university owned personal devices in circulation prior to the establishment of this policy.
- If an employee's personal devices is lost or stolen while off campus, it's the responsibility of the owner to immediately file a report with the local Police Department and to notify the University Police Department of the theft. The University Police will need to know the name of the local Police Department, the serial and tag number assigned to the personal device, and the Police report number where the theft report was filed. The University Police Department will notify Absolute Theft Recovery Team to activate the recovery process of the device. The serial and tag number must be provided to the Police Department when reporting a lost or stolen device.
- If an employee's personal device is lost or stolen on campus, it is the responsibility of the owner to immediately file a report with the University Police Department. The University Police Department will provide the user with a theft number and will notify Absolute Theft Recovery Team to activate the recovery process of the device. The serial and tag number must be provided to the Police Department when reporting a lost or stolen device.
- It is the department's responsibility to notify ITD Help Desk (extension 3963) each time the ownership of a personal device is changed so that it can be re-imaged and re-registered to the new owner.

- University users whose roles require them to store or work with "Internal" or "Confidential" information as defined in the CSU Data Classification and Handling Policy must enable encryption on the personal device to the extent that such functionality is available.
- No personal information (as defined by the personal information protection act – 815 ILCS 530) shall be stored on mobile devices unless it is encrypted, and permission is granted from the data owner.
- All personal devices purchased with State or Grant funds must have the University's configuration management and security software installed and activated.
    - Examples of such software include but is not limited to MDM (mobile device management) software download and/or Absolute Computrace software downloaded for laptops before using the device for University's business.

User Responsibility for Personal Device Security

- Users must regularly check for vendor security updates and apply them.
- Personal device owners must have it checked by ITD every six months (October and April) to ensure that the latest patches, security holes and other software remain current and consistent with CSU configuration requirements.
- Establish strong passwords as defined in the CSU Password Policy.
- Create regular backups of your data and files. (It is recommended that you use an encrypted USB flash or thumb drive, for those devices that will accommodate such a device, that can be purchased from CDW-G, Zones, etc. in CSU Buy).
- The physical security of these personal devices is the responsibility of the employee to whom the device has been assigned. Personal devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.
- The "property control card" delivered with the personal device to the end-user must remain in the possession of the user assigned to the personal device at all times.
- Whenever possible all personal devices should enable screen locking and screen timeout functions.

Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU ITD approval Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted by ITD.

Enforcement

This Personal Device Security Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of CSU for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References

- NIST CSF: ID.AM-1, ID.RA-1, PR.AC-1, PR.AC-3, PR.AC-7
- The Illinois State Auditing Act (30 ILCS 5/3-2.4)

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/3/2022	11/1/2023	11/6/2022	Donna Hart	
			11/1/2023	Donna Hart	