POCD Security Policy for Chicago State University Systems

Policy Statement

In response to the increasing use of personally owned computing devices (POCD) by users of Chicago State University (CSU) Information Resources for CSU business purposes.

Purpose

This policy establishes CSU guidelines for employee use of POCD for work-related purposes.

Scope

Employees of CSU may have the opportunity to use their POCD for work purposes when authorized in writing, in advance, by the employee, their manager and University ITD leadership. POCD includes personally owned cellphones, smartphones, tablets, laptops, and computers.
The use of POCD is limited to certain users and may be limited based on compatibility of technology. Contact CSU ITD for more details.

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 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 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 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 personally owned computing devices (POCD) to work, whether laptop, smartphone, or tablet, in order to interface to the corporate network.
- **Risk** - is the potential for damage an action or condition will have on an organization's ability to achieve its objectives and/or execute its strategies successfully.
- **Threat** – is the action or condition that conducts or enables the carrying out of potential damage.
- **Vulnerability** – is the weakness that is exploited by the threat causing damage.
- **Impact** – is the magnitude of the damage caused by a threat.
- **Likelihood** – is the probability of the threat transpiring.
- **Inherent information security risk** – the information security risk related to the nature of the 3rd-party relationship without accounting for any protections or controls. Inherent risk is sometimes referred to as "impact" and is used to classify third-party relationships as an indicator of what additional due diligence may be warranted.
- **Residual information security risk** – the information security risk remaining once all available applicable protections and controls are accounted for.
- **Internal control** - is any process or action designed to reduce the impact and/or likelihood of a threat.

Responsibility

Any user connecting to CSU Information Resources using a POCD is responsible to adhere to the requirements of this policy and all other CSU Information Security Policies. CSU reserves the right to modify this policy, including eliminating all support for POCD, at any time. CSU ITD may elect to implement additional requirements or processes to safeguard the University's Information Resources (e.g., mobile device management (MDM), enforcing separation of CSU data from personal data, remotely removing CSU data, additional registration processes, or requiring a PIN number to access systems). The most current version of this policy will be posted on ITD website.

Policy

Devices and Support

To ensure the security of CSU information, authorized employees are required to have anti-virus (where technically feasible) and / or mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails, and other applications in one area that is password-protected and secure. CSU's ITD department must install this software prior to using the personal device for work purposes.

University-Related Persons / Employee / Staff may store company-related information only in this area. University-Related Persons / Employee / Staff may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by ITD. University-Related Persons / Employee / Staff may not use unsecure Internet sites.

Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.

Restrictions on authorized use

University-Related Persons / Employee / Staff whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.

While at work, University-Related Persons / Employee / Staff are expected to exercise the same discretion in using their personally owned devices as is expected for the use of company devices. CSU policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Excessive personal calls, e-mails, or text messaging during the workday, regardless of the device used, can interfere with productivity and be distracting to others. University-Related Persons / Employee / Staff must handle personal matters on nonwork time and ensure that friends and

family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management. Managers reserve the right to request employees' cellphone bills and use reports for calls and messaging made during working hours to determine if use is excessive.

Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending, and responding to e-mails or text messages, responding to phone calls, or making phone calls.

University-Related Persons / Employee / Staff may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. CSU reserves the right to deactivate the company's application and access on the employee's personal device during periods of unpaid leave.

A University-Related Persons / Employee / Staff may not store information from or related to former employment on the company's application.
Family and friends should not use personal devices that are used for company purposes.

Privacy/company access

No University-Related Persons / Employee / Staff using his or her personal device should expect any privacy except that which is governed by law. CSU has the right, at any time, to monitor and preserve any communications that use the CSU's networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that CSU's resources in these areas are being use according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

No University stipend

University-Related Persons / Employee / Staff authorized to use personal devices under this policy as a convenience. CSU will not have any stipend or other financial consideration with regard to the use of their personally owned devices to conduct CSU official business.

Safety

University-Related Persons / Employee / Staff are expected to follow applicable local, state, and federal laws and regulations regarding the use of electronic devices at all times.

University-Related Persons / Employee / Staff whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving.

Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations involving traffic, inclement weather, or unfamiliar areas.

University-Related Persons / Employee / Staff who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

University-Related Persons / Employee / Staff who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost, stolen, hacked or damaged equipment

University-Related Persons / Employee / Staff are expected to protect personally owned devices used for work-related purposes from loss, damage, or theft. In an effort to secure sensitive company data, University-Related Persons / Employee / Staff are required to have "remote-wipe" software installed on their personal devices by the ITD department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.

CSU will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. University-Related Persons / Employee / Staff must immediately notify ITD in the event their personally owned device is lost, stolen or damaged. If ITD is unable to repair the device, the employee will be responsible for the cost of replacement.

Termination of employment

Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.

Policy Exceptions and Maintenance

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

Enforcement

This POCD 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
- CSU Telephone Usage Policy
- Joint Committee on Administrative Rules - Section 5030.130 Telephone Usage Policy

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	