Acceptable Use Policy for Chicago State University Systems

Policy Statement

Chicago State University (CSU) makes available to its community members information resources, including shared information technology resources that use text, voice, images, and video to deliver information. These resources are to be used in a manner consistent with university policy and the law, and related policies created by specific departments, programs, and offices of the University.

Purpose

This policy details specific requirements for the use of all information resources at the CSU, including electronic and hardcopy data, information, and information assets. Information resources and technology at the CSU support the educational and administrative activities of the University, and the use of these information resources is a privilege that is extended to members of the CSU community. As a user of these services and facilities, you have access to valuable University resources, to information that is meant for internal use only or confidential. Consequently, it is important for you to behave in a responsible, ethical, and legally compliant manner.

In general, acceptable use means ensuring that the information resources and technology of the University are used for their intended purposes while respecting the rights of other computer users, the integrity of the physical facilities, the confidentiality of data, information resources, and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the University may take disciplinary action, including restriction of and possible loss of network privileges or more serious consequences, up to and including suspension, termination, or expulsion from the University. Individuals may also be subject to federal, state, and local laws governing many interactions that occur on the University's networks and on the Internet. These policies and laws are subject to change as state and federal laws evolve.

Scope

This policy applies to all users of information resources owned or managed by the CSU. Individuals covered by the policy include, but not limited to, University faculty and visiting faculty, physicians, staff, students, alumni, Extra Help, HR approved consultants, volunteers, guests or agents of the administration, and external individuals and organizations accessing network services via the University's computing facilities.

These policies apply to technology whether administered in individual departments and divisions or by central administrative departments. They apply to personally owned computers and devices connected by wire or wireless to the University networks and information resources, and to off-site computers that connect remotely to the University's network services.

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, to interface to the corporate network.
- **Risk** - is the potential for damage an action or condition will have on 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 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.
- **Geo**–**Fencing-** the use GPS technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area.
- **Illinois Identity Protection Act** – the act specifically prohibits certain social security numbers at public institutions and agencies, create protection requirements and requires state agencies to enact an Identity Protection Policy for public view and for employees working with social security numbers (SSNs)

Responsibility

The Acceptable Use Policy for CSU Information Resources applies to all active members of the Employees / Staff, Associates / Extra Help or 3rd parties, and Students who use or access University Information Resources. This policy also applies to campus visitors who avail themselves of the University's temporary guest or temporary service resulting in having access to University Information Resources, including those who register their computers and other devices through Conference and Event Services programs or through other offices, for use of the University's network.

Policy

Acceptable Use

Institutional Use

Use of all University information technology and digital resources should be for purposes that are consistent with the non-profit educational mission and the policies and legal requirements (including license agreements and terms of service) of the University, and not for commercial purposes.

Personal Use

Personal use of the University's information resources, except for students enrolled at the University, should be incidental and kept to a minimum.

Prohibited Use

Use of the University's information technology and digital resources should not violate applicable federal, state, and local law, including U. S. copyright law, or applicable University policies, and **Geo-Fencing, if travel is involved outside of the United States the user must inform ITD.** From any location, University resources may not be used to transmit malicious, harassing, or defamatory content. Because of privacy, compliance and legal considerations, the University prohibits the use of its information resources in recording non-public University meetings, activities, and events except when recording is necessary to facilitate University operations and serve institutional needs.

Political Use

As a 501(c)(3) organization, the University is prohibited from participating or intervening in any political campaign on behalf of or in opposition to a candidate for public office, and no substantial part of the University's activities may be directed to influencing legislation (i.e., lobbying). Individuals may not use University technological resources for political purposes in a manner that suggests the University itself is participating in campaign or political activity or fundraising, or for influencing legislation. Any other use with respect to political activity must be permitted by applicable University policy and consistent with applicable laws.

Access and Privacy

The University has the legal right to access, preserve and review all information stored on or transmitted through its electronic services, equipment, and systems. The University endeavors to afford reasonable privacy for individual users and does not access information created and/or stored by individual users on its information resources except when it determines that it has a legitimate operational need to do so.

Protection of University Information Resources

Users of CSU information technology and digital resources are responsible for protecting University data, including its confidentiality, integrity, access, retention, and disposal, in accordance with the University's Information Security Policies, Record Retention Policy, and other applicable University policies. Individuals with University accounts or administrative or custodial responsibility over any University resources should take reasonable measures to protect these accounts and resources. Shared University technological resources should be used for educational purposes and to carry out the legitimate business of the University and should not be used in a way that disrupts or otherwise interferes with any University activities or systems, or that is inconsistent with the University's policies or goals.

Requirements

In making acceptable use of resources, individuals covered by this policy must:

- Use CSU information resources only for authorized purposes.
- Protect their User IDs, digital / electronic signatures, other authentication and authorization mechanisms, and systems, from unauthorized use. Each individual is responsible for all access to university information resources and technology by their User IDs, digital/electronic signatures, and other authentication and authorization mechanisms, and for any activity originating from their systems.
- Access only information to which they have been given authorized access or that is publicly available.
- Protect electronic and hardcopy data, information, and information assets classified as High-Risk or Moderate-Risk (i.e., "confidential"), in compliance with the University's Data Classification and Handling Policy, and other security related policies, and applicable Federal, State, and Local laws.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.
- Restrict personal use of the University's information resources and technology to incidental, intermittent and minor use that is consistent with applicable law and University Policy.
- Include only material germane to university matters in university, school, or departmental electronic communications, such as e-mail, Websites, blogs, etc. Personal web sites, chat rooms, web logs (also known as blogs) and other forms of publicly available electronic communications hosted on or linked from university information resources and technology must comply with this Acceptable Use Policy and prominently include the following disclaimer: "The views, opinions and material expressed here are those of the author and have not been reviewed or approved by the CSU."
- Store internal and confidential data only in university approved secured locations.
- Transmit / transport confidential data, information, and information assets only via university approved secured mechanisms.
- Use Bring Your Own Device (BYOD) in only University approved means.
- Change passwords every 90 days and other authentication and authorization mechanisms suspected of compromise.
- Report identified or suspected security incidents to the Information Security Office or Information Technology (IT) Support/Help Desk.

In making acceptable use of resources, individuals covered by this policy must not:

- Gain access to or use another person's system, files, or data without permission (note that permission from an individual user may not be sufficient – some systems may require additional authority).
- Reveal a password or other authentication and authorization means to any other individual, even those claiming to be an IT support technician (over the phone or in person).
- Use computer programs to decode passwords or access-control information.
- Attempt to circumvent or subvert system or network security measures.

- Engage in any activity that is intended to harm systems or any information stored thereon, including creating or propagating malware, such as viruses, worms, or "Trojan horse" programs; disrupting services; damaging files; or making unauthorized modifications to university data.
- Make or use illegal copies of copyrighted software, store such copies on University systems, or transmit them over University networks.
- Use of e-mail, tools, or messaging services in violation of laws or regulations or to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or User ID. Waste shared computing or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings. ***Please refer to the Sexual Harassment and Sexual Misconduct Policy, The IT Code Of Conduct and the Ethics Compliance policy for more information.***
- Use the University's systems or networks for commercial purposes; for example, by selling access to your User ID or by performing work for profit with University resources in a manner not authorized by the University.
- State or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so.
- Violate any applicable laws and regulations or University policies and procedures that govern the use of IT resources.
- Transmit commercial or personal advertisements, solicitations, endorsements, or promotions unrelated to the business of the University.
- Use "auto-forward" rules to send business e-mail to a non-University e-mail account if the e-mail contains any legally restricted, and/or confidential information.
- Send or receive legally restricted and/or confidential information via the Internet without making reasonable accommodations for the security of such information.
- Modify, without proper authorization, any of the University's information resources and technology, including the work products of others.
- Store confidential data on local drives, flash drives, or other portable or external media.

Policy Exceptions and Maintenance

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

Enforcement

This Acceptable Use 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: DE.CM-3, DE.CM-7
- CSU Sexual Harassment and Sexual Misconduct Policy for more information
- CSU Ethics Compliance policy
- CSU IT Code of Conduct

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/4/2022	11/1/2023	11/6/2022	Donna Hart	
		11/15/2024	11/15/2023	Donna Hart	
	03/19/2024	11/15/2024	03/19/2024	Donna Hart	