Change Control Policy for Chicago State University Systems

Policy Statement

During the course of normal operations, the Chicago State University (CSU) Information Technology Department (ITD) makes changes, such as installations, enhancements, upgrades, patching, etc., to the technology landscape of the University. This policy defines the guidelines by which those changes are governed and managed.

Purpose

The purpose of the CSU Change Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to CSU Information Technology Resources.

Scope

The CSU Change Control Policy applies to any individual, entity, or process that creates, evaluates, and/or implements changes to CSU Information Technology Resources.

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 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 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.

Policy

- Changes to production CSU **Information Resources** must be documented and classified according to their:
  - Major
  - Standard
  - Minor
  - Emergency
- A Change Control Board must be established to institute a reasonable governance and escalation process and set of activities relative to the management of. Changes in the CSU IT environment.
- Change documentation must include, at a minimum:
  - Date of submission and date of change,
  - Owner and custodian contact information,
  - Nature of the change,
  - Change requestor,
  - Change classification(s),
  - Roll-back plan,
  - Change approver,
  - Change implementer, and
  - Testing outcome
  - Communication plan
  - An indication of success or failure
  - Post- Implementation Review (60 Day Review)
- Changes with a significant potential impact to CSU **Information Resources** must be scheduled.
- CSU **Information Resource** owners must be notified and approve of changes that affect the systems for which they are responsible.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance with the CSU Information Retention Schedule.
- Changes made to CSU customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
- All changes must be approved by the Information Resource Owner or the Director of Information Technology, and the Change Control Board.
- Emergency changes that require an immediate implementation (i.e., break/fix, incident response, etc.) may be implemented without following the formal change control process, but may not circumvent documentation requirements, and must be documented after the change.
- To be compliant with Illinois State requirements (The Illinois State Auditing Act (30 ILCS 10/3001)), internal auditors are mandated to conduct a pre-implementation review for all major

system changes. The need to perform such a review is determined by a risk assessment of the change.

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 Change Control 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:PR.DS-7, PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4
- The Illinois State Auditing Act (30 ILCS 10/3001)

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	
2.0	04/06/2023/drh	11/1/2023			