Identity & Access Management Policy for Chicago State University Systems

Policy Statement

Information is a valuable asset and access to it must be managed with care to ensure that confidentiality, integrity, and availability are maintained. Chicago State University (CSU) provides access to information assets, accounts, systems, and resources based on the principle of least privilege (see Information Security Glossary for explanation). This policy outlines the rules relating to authorizing, monitoring, and controlling access to University accounts, and information resources.

Purpose

Access controls are designed to minimize potential exposure to the University resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the University networks, systems, and applications.

Scope

This policy applies to CSU University-Related Persons / Employees / Staff, Associate / Extra Help, Third-party or 3rd parties and Students that connect to servers, applications or network devices that contain or transmit CSU "Internal" or "Confidential" Data, per the Data Classification and Handling Policy. All servers, applications or network devices that contain, transmit or process CSU "Internal" or "Confidential" Data are considered "High Security Systems".

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.

Responsibility

The Identity & Access Management 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

Identity Management

Formal user registration and de-registration processes are implemented to enable the assignment of identities and accounts on an individual basis. This ensures accountability for all actions taken by employees, students and associate account users.

Authentication Management

All account, service and platform access are managed through secure authentication controls. For more information on this please see the CSU Password Policy.

Segregation of Duties

Access to High Security Systems will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor and the UISO, with a valid business justification. Access controls to High Security Systems are implemented via an automated control system. Account creation, deletion, and modification as well as access to protected data and network resources is completed by the Server Operations group. On an annual basis, the University Information Security Office will audit all user and administrative access to High Security Systems. Discrepancies in access will be reported to the appropriate supervisor in the responsible unit and remediated accordingly.

User Access

All users of High Security Systems will abide by the following set of rules:

- Users with access to High Security Systems will utilize a separate unique account, different from their normal CSU account. This account will conform to the following standards:
    - The password will conform, at a minimum, to the published CSU Password policy.
    - Inactive accounts will be disabled after 90 days of inactivity.
    - Access will be enabled only during the time period needed and disabled when not in use.
    - Access will be monitored when account is in use.
    - For those systems that are capable, require that the user re-authenticate If a session has been idle for more than 15 minutes to re-activate the terminal or session.
- Users will not login using generic, shared or service accounts where it is technically feasible to create unique credentials.
- Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

Administrative Access

- Administrative, Privileged accounts and privileged access must be purpose driven, secure and always adhere to the principle of least privilege.
- Users will abide by the above user access guidelines.
- Administrators will immediately revoke all of a user's access to High Security Systems when a change in employment status, job function, or responsibilities dictate the user no longer requires such access.
- All service accounts must be used by no more than one service, application, or system.
- Administrators must not extend a user group's permissions in such a way that it provides inappropriate access to any user in that group.
- All servers, applications and network devices shall contain a login banner that displays the following content:

"This computer and network are provided for use by authorized members of the CSU community. Use of this computer and network are subject to all applicable CSU policies, including Information Technology Services policies), and any applicable CSU Handbooks. Any use of this computer or network constitutes acknowledgment that the user is subject to all applicable policies. Any other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer, or a network may not be private. Sensitive communications should be encrypted or communicated via an alternative method."

Remote Access

All users and administrators accessing High Security Systems must abide by the following rules:

- No external modems, Routers, switches, or wireless access points are allowed on high security networks, or other unapproved remote access technology.
- All remote access must be authenticated and encrypted through the University's VPN, CSU Secure Access.
- All remote access will be accomplished through the use of two factor authentication; a username and password or PIN combination, and a second method not based on user credentials, such as a certificate or token, provisioned to the user.
- Any machine used for remote access must have antivirus and host-based firewall software installed, running, and enabled. This requirement is enforced by a host checker component of the University's VPN software, and remote access to the High Security Network is only possible after a machine has passed these configured checks.
- Any third party, non-CSU affiliate that requires remote access to High Security Systems for support, maintenance or administrative reasons must designate a person to be the Point of Contact (POC) for their organization. In the event the POC changes, the third party must designate a new POC.
- All third party access to High Security Systems must be approved by the Information Security Program Leader or their designee.
- Third parties may access only the systems that they support or maintain.
- All third party accounts on High Security Systems will be disabled and inactive when not being used for support or maintenance purposes.
    - Requests for enabling such access must follow be enabled by authorized ITD personnel.
    - Requests for access outside of this policy are expressly denied.
    - Designated ITD personnel will be responsible for enabling/disabling accounts and monitoring vendor access to said systems.
    - All third parties with access to any High Security Systems must adhere to all regulations and governance standards associated with that data (e.g. PCI security requirements for cardholder data, FERPA requirements for student records, HIPAA requirements for Protected Health Information).
    - Third party accounts must be immediately disabled after support or maintenance is complete.
- Data must not be copied from high security systems to a user's remote machine.
- Access will be disconnected automatically after 24 hours.

- Users will abide by the above user access guidelines.

Physical Access

The CSU data center will abide by the following physical security requirements:

- Video surveillance will be installed to monitor access into and out of the CSU data center.
- Access to CSU data center will be accomplished with the use of electronic badge systems.
- Physical access to the CSU data center is limited to ITD personnel, designated approved CSU employees or contractors whose job function or responsibilities require such physical access.
- CSU badges will be prominently displayed.
- Visitors accessing the CSU data center will be accompanied by authorized ITD personnel, and all access will be logged via the CSU Data Center Visitor Access Log.
    - This log will be stored in the CSU data center.
    - Each visitor, and accompanying authorized ITD personnel, must sign in and out of the data center.
    - The log will be kept for at least a period of three months.
- Modification, additions, or deletions of physical access to the CSU data center will be accomplished by request to the Information Security Office and the Director of Infrastructure.
- All terminated onsite personnel and expired visitor identification will have their access revoked immediately.
- Physical access to the CSU data center requires the approval of the Director of ITD.
- The Information Security Office and the Director of Infrastructure will audit physical access to the CSU data center on an annual basis.

Access Governance

A formal user access provisioning process is implemented to assign or revoke access rights for all user types to systems and information assets under the control of the University. This access provisioning is based on the following principles:

Access changes for employees are primarily managed through the CSU user onboarding, change of job role and termination processes:

- All extra requests for or changes to access are documented and tracked.
- All access requests or changes require documented justification.
- Justification will be based on a simple risk assessment and the business need and will be confirmed by the request sponsor.
- Appropriate sponsorship & approval is required and documented for all access requests or changes.
- All access changes granted by administrators are documented and tracked.
- Reviews of access are performed by relevant asset owners periodically.
- These principles are agnostic of account type, service, application, or system.

Removal or Adjustment of Access Rights

The access rights of all employees, students and associate account users to information and information processing facilities will be removed upon termination of their employment, contract, or agreement, or adjusted upon change. For all University employees, this is managed through the CSU user onboarding,

change of job role and termination processes. Additional access to accounts, assets, systems, or services are subject to review and approval on a case-by-case basis, as outlined in the Access Governance section above.

Access Reviews

Access to assets, services and systems will be periodically reviewed. The frequency of these reviews depends on the identified risk surrounding the asset and access in question. It is recommended that the risk relating to each individual asset is measured and given a risk rating in line with the single asset risk assessment process, outlined in the Information Security Risk Management policy. Where an access review identifies an access anomaly it will be treated as a potential incident and investigated by the asset owner and information security team.

Access in Special Circumstances

There are special circumstances where extra or privileged access is needed. For all cases, access to an account, the information contained within an account or information pertaining to the activity of an account, is carefully restricted and must only be carried out with the appropriate authorization and safeguards in place.

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 Identity & Access Management 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.AC-1, PR.AC-2, PR.AC-3, PR.AC-6, 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	