Password Policy for Chicago State University Systems

Policy Statement

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of CSU's entire network. As such, all CSU students, and employees (including contractors and vendors with access to CSU systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CSU facility, has access to the CSU network, or stores any non-public CSU information.

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 Password Policy for CSU Information Resources applies to all active members of the University-Related Persons / Employees / Staff, Associates / Contractors or 3rd parties, and Students who use or access University Information Resources.

Policy

General

Under no circumstances should a user divulge their password to another person.

1. All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.
2. All production system-level passwords must be part of the IT Services administered global password management database.
3. All user-level passwords, (e.g., email, web, desktop computer, etc.), subject to the technological constraints of the platform must
    1. Be reset every 180 days
    2. Exhibit complexity by
        1. Not contain all or part of the user's account name
        2. Contain characters from three of the following four categories:
            1. Uppercase characters (A through Z)
            2. Lowercase characters (a through z)
            3. Base 10 digits (0 through 9)
            4. Non-alphabetic characters (for example, !, $, #, %)
    3. Maintain a password history of 12 passwords and not allow reuse
    4. Must be a minimum of 12 characters
    5. Be locked out for a minimum of 15 minutes if more than 3 unsuccessful attempted logons
    6. ***Those platforms that are technologically incapable of those levels of password complexity and restrictions must be configured to require the maximum level complexity allowed by the particular platform up to and including those parameters described in 3.1 through 5.5 above.***
4. CSU systems capable of such functionality will have automatic log-offs after a predetermined period of inactivity; username and password will be required for re-authentication.
5. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
6. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.
7. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
8. All temporary passwords must be changed at first logon.

9. If an account or password is suspected to have been compromised, report the incident to IT Services and immediately change all of the associated passwords.
10. Automated password guessing may be performed on a periodic or random basis by IT Services Management or its delegates. If a password is guessed during one of these scans, the user will be required to change it.

Remote Access Users

Access to the CSU Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Shared Accounts

Passwords should not be shared except where it is technologically infeasible to issue unique credentials to users. For those situations, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

1. Passwords for servers must be changed as personnel changes occur.
2. If an account or password is suspected to have been compromised, the incident must be reported to the CSU Information Security Leader and potentially affected passwords must be changed immediately.
3. Where technically or administratively feasible, attempts to guess a password should be limited to 3 incorrect guesses. Access should then be locked for a minimum of 15 minutes, unless a local system administrator intercedes.
4. Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks.
5. Failed attempts should be logged unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the Information Security Office.

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 Password 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

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	