I. PURPOSE:

The Information Technology Division (ITD) at Chicago State University (CSU) will provide security for all ITD/CSU managed Information Technology (IT) resources to ensure confidentiality, integrity and availability of CSU operations. This policy defines the responsibilities and general security measures for data specific to the use of IT resources managed by ITD at CSU. This policy applies to all CSU IT resources including but not limited to desktops, laptops, servers, printers, photo-copiers, tablets, iPads, phones, network devices, among others.

II. DEFINITIONS

1. **Restricted Data:** Data is restricted if disclosure is limited or prohibited by state or federal law or if disclosure would result in the imposition of financial penalties. Included in this definition is data whose disclosure is regulated by federal and state laws, such as FERPA, HIPAA or the Data Protection Act. Payroll, personnel, and financial information are also deemed restricted

   This policy recognizes that other data may need to be treated as restricted because it would cause severe damage to the University if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements after consultation with ITD.

2. **Sensitive Data:** Data that is not restricted, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements for sensitive data.

3. **Public Data:** Information that may be freely disseminated.

4. **IT Resources** are categorized as follows: Physical, Logical and Communications. Physical resources include but are not limited to desktop computers, portable computers, personal information devices, and printers. Logical resources include computer software and data files digitally or optically stored as well as information itself. Communication resources include the capability to send messages either through the CSU internal network or via the Internet.

5. **Administrator:** Users that have administrative level access to IT resources, mainly from ITD and key designated individuals from various Colleges.

6. **Power User:** Users with elevated access to IT resources mainly to support end users in their respective areas.

7. **End User:** Users that have general access to IT resources to perform day to day tasks.

8. **Consultant/Contractor:** Users who are not CSU employees but need access to IT resources for a specific period of time.

9. **Guest:** Users who are not CSU employees but need access to IT resources, mainly in the general purpose computer laboratories.

III. ACCESS CONTROL POLICY

1. Access to University network systems and resources (wired and wireless) should be made using usernames and passwords.
2. Login usernames for use of IT resources to conduct day-to-day operations should not have administrator level access rights.
3. Usernames and passwords should not be shared. ITD should be notified if the password has been compromised so that the account can be disabled or password reset.
4. Passwords should have sufficient level of complexity. The definition of complexity will be established by the Identity Management Team at CSU.
5. Senior management at CSU must have full rights to University owned servers storing or transmitting restricted or confidential data.
6. Users should not install non-standard software applications without informing ITD. These applications open security holes that can potentially attract virus, malware, etc. Please review the "**Guidelines to Purchase Technology Equipment at Chicago State University**" document for the list of standard software applications supported by ITD.
7. Passwords and confidential data should not be sent via emails unless they are encrypted.
8. Default passwords must be changed after the initially installing the application.
9. Terminated employees accounts should be disabled immediately after their last day of official work. Audit reviews should be conducted on regular basis to ensure that terminated employees do not have access to IT systems.
10. Transferred employees access must be reviewed and adjusted as needed.
11. Access rights audit reports should be sent to unit leaders on regular basis requesting feedback.
12. Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons, date and time of logon and logoff.
13. Individuals who have administrative system access should use less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.
14. IT Resources which access or store restricted or confidential information should be encrypted.
15. Every effort should be made to prevent local storing of restricted and sensitive data on end user devices. Data falling under either classification should be stored in the University managed servers in the data center.

IV. INTERNET SECURITY POLICY

1. Transfer of data classified as restricted or confidential should be through secure connections only in order to protect the contents.
2. Transfer of University data over the Internet should be done using University provided accounts and should not be done using personal accounts.

V. EXCEPTIONS

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

1. Required commercial or other software in use is not currently able to support the required features;
2. Legacy systems are in use which do not comply, but near-term future systems will, and are planned for;
3. Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, units must develop a written explanation of the compliance issue and a plan to address compliance with the University's Information Security Policy in a reasonable amount of time. Explanations and plans must be submitted to the CIO.