Information Security Risk 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. To understand the likelihood and impact of its information security risks, Chicago State University (CSU) has developed an information security risk management framework. This framework is employed to ensure that the risks associated with any particular asset or activity are consistently measured and addressed. From this measurement appropriate and sustainable treatments can be put in place that align with the University's overall objectives, and risk appetite.

Purpose

To establish a process to manage information security risks to CSU that result from threats to the confidentiality, integrity and availability of University Data and Information Systems.

Scope

This policy applies to all electronic data created, stored, processed, or transmitted by CSU, and the Information Systems used with that data. This Information Security Risk Management Policy and the information security risk management framework described within, will serve as the basis for supporting controls, processes and procedures and will apply to all assets owned and operated by CSU. This includes CSU information processes by any and all external organization or individuals that provide information processing services specifically or transact business ion general with the University.

Definitions

- **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.

- **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, and third-party contractors engaged by the University and their agents and employees.
- **Associate / "Contractor", Third-party or 3rd-party** – is someone officially attached or connected to the College who is not a student or employee (e.g., contractors, vendors, interns, temporary staffing, volunteers.)
- **Information Resources / ITD Resources -** include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, 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 System Owner** - 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.
- **ISO** - is the University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

Responsibility

It is the responsibility of every individual responsible for the use or management of technology or technology solutions in the campus community to take reasonable care to minimize the IT and security related risks inherent with the use of those technologies. Specific responsibilities include:

1. The Information Security Office (ISO) is responsible to ensure that identified information security risks to ITD Resources are assessed, evaluated, and prioritized according to established information security risk assessment process that appropriate plans are developed and implemented to mitigate those information security risks using means most appropriate to the overall operation of the university.
2. Information System Owners are responsible for ensuring that information systems under their control are assessed for information security risk and that identified risks are mitigated, transferred, or accepted.

3. The ISO is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

Policy

Objectives

This policy, its associated procedures, processes, and guidance provide a common framework, methodology and organized approach to information security risk management across the University. This ensures that information security risks can be understood in a reliable and consistent manner.

The University's information risk management objectives are that:

- All University information security risks are identified and assessed.
- All identified information security risks are managed and treated in line with the University's risk appetite.
- Appropriate information security controls are put in place and maintained across all of the University's information resources.
- To align with information security industry best practices and standards, such as the National Institute of Standards (NIST), Cyber Security Framework (CSF).

Risk Management Framework

Information security risks are managed in line with the University's Risk Management process and procedure. Information security risks are identified, managed, assessed, and treated using methodologies consistent with NIST SP 800 30 to the extent possible. When such consistency is not feasible such exclusions will be documented and justified using the standard policy exception process.

The Information Security Risk Management Framework outlined in this document, describes how these individual methodologies are employed to ensure the management of information security risk is comprehensive, appropriate, and consistent.

Risk Governance

Risk Governance & Reporting

This policy and the information security risk framework will integrate with and to a great extent drive the University's IT security risk governance and reporting structure.

The ITD Information Security Risk Review Group, made up of key ITD Stakeholders and University leadership is responsible for the management and oversight of information security related risks in the University environment. This is accomplished through the conduct of periodic group meetings where risks that rise above a risk level of LOW are presented, along with mitigation plans, or exception requests. The ITD Information Security Risk Review Group will opine on these plans and requests and render a decision. In the event that the group cannot come to a decision, those items will be escalated for a decision to the CIO in consultation with ITD leadership. At the

discretion of the CIO mitigation plans and/or exceptions can be escalated further to the University President for a decision.

An information security risk register must be maintained by the Information Security Office and kept up to date based on the decisions rendered by the ITD Information Security Risk Review Group, CIO, or University President as appropriate.

Information Security Risk Governance & Reporting

The results and actions of information security risk assessments are products of the ISO and will be recorded in a standalone Information Security Risk Register to ensure visibility of all risks relating to information and cyber security.

The results and actions of information security risk assessments, risk registers and treatment plans, where appropriate, will then also feed into the departmental and faculty risk registers to be managed and owned accordingly, in line with the University's overall information security risk governance and reporting structure.

This will occur through reporting of information security risks to the relevant information resource owner. From here the relevant owner will be responsible for developing a treatment plan to address the identified information security risks and present those treatment plans to the ITD Information Security Risk Review Group (Internal Auditors/ITD) for review.

All information resources must be assessed appropriately for information security related risks in conjunction with the following CSU Information Security Policies:

- CSU Third Party risk Review Policy.
- CSU Change Control Policy.
- CSU Path Management Policy.
- CSU SDLC Policy.

Risks identified by an information security risk assessment in any of these areas must be mitigated or accepted prior to the activity in question taking place.

Residual risks that still exceed information security risk appetite may only be accepted on behalf of the university by the ITD Information Security Risk Review Group.

Each Information System must have a system security plan, prepared using input from information security risk, security, and vulnerability assessments.

Risk Thresholds

A very important aspect of a reliable and consistent information security risk framework is the establishment of risk thresholds. Information Security Risk thresholds at CSU are as follows:

High Risk – Any identified information security risk whose impact exceeds at least one of the following conditions:

- May negatively impact at least one mission critical system of the University for more than 24 hours
- May result in the unauthorized disclosure of more than XXXX "Confidential" records
- May impact more than 25% of students and faculty in the University

Medium Risk - Any identified information security risk whose impact meets at least one of the following conditions:

- May not impact any mission critical system of the University
- May result in the unauthorized disclosure of less than 100 "Confidential" records.
- Impacts more than 5% but less than 25% of the students and faculty in the University.

Low Risk – Any identified information security risk whose impact is less than all of the following conditions:

- May not negatively impact any mission critical system of the University.
- May not result in the unauthorized disclosure of any "Confidential" records
- Impacts less than 5% of students and faculty of the University

Risk Appetite

Risk appetite is the level of tolerance the University has for threats and vulnerabilities in relation to how those threats and vulnerabilities may impact University activities and operations. The University has a stated low appetite for risks, however, in order to conduct those activities and operations there may be occasion to exceed that risk threshold. It is the purpose of the risk governance capability to relate those excesses in risk to reward associated with the conduct of those activities to allow the various levels of governance structure to make informed decisions.

The ISO has a risk appetite of "LOW" that reflects both ITD's and the University's approach. With this in mind, Information security risks that exceed this threshold may be tolerated, or accepted, in line with the risk treatment options outlined in the Information Security Risk Management Framework.

In all cases information security risk treatments must be documented, justified, and approved, by the ITD Security Risk Review Group. Treatment plan approval must be obtained from relevant staff in line with the Information Handling Decision Matrix. If the given information security risk is considered "LOW", then the information resource owner and risk owner can approve their own treatment plans.

Policy Exceptions and Maintenance

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

Enforcement

This Information Security Risk 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: ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.MI-3,

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	