Third Party Security Risk Review Policy for Chicago State University Systems

Policy Statement

Chicago State University (CSU) utilizes third-party technology and technology solutions to support our mission and goals. Third-party relationships carry inherent and residual risks that must be considered as part of our due care and diligence.

Purpose

The purpose of this policy is to define the requirements for how CSU will conduct our third-party information security due diligence.

Scope

This policy applies to all individuals or groups who engage with a third-party provider of technology or technology solutions on behalf of Chicago State University.

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 personal devices 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

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.

Policy

Assessments

- Every 3rd-party granted access to CSU Information Resources must sign the CSU Third-Party Non-Disclosure Agreement.
- All 3rd-party relationships must be evaluated for inherent information security risk prior to any interaction with CSU Information Resources.
- Criteria for inherent risk classifications must be established; “High”, “Medium”, and “Low”.
- All 3rd-party relationships must be re-evaluated for inherent information security risk based on their most current risk. Assessment. The timings for this ere-evaluation process are:
    - Low Risk – Everything 3 years
    - Medium Risk – Every 2 years
    - High Risk – Every Year
    - Any. Material change in that Third Party’s Operations. Examples of such material changes include, but are not limited to:
        - Merger or Acquisition
        - Migration of that third party to a new platform or. Platforms
        - Security Breach involving the unauthorized disclosure of confidential or sensitive data
- 3rd-party relationships with significant inherent risk (classified as “High” or “Medium”) must be evaluated for residual risk using questionnaires, publicly available information, and/or technical tools.
- Residual information security risk assessments must account for administrative, physical, and technical controls.
- Residual information security risk thresholds must be established for 3rd-party relationships with significant inherent risk (classified as “High” or “Medium”).
- 3rd-party relationships that do not meet established residual information security risk thresholds:
    - Must be terminated,
    - Must be formally approved by executive management following an established waiver process, and/or;
    - Changed in a manner that reduces inherent and/or residual information security risk to meet CSU established thresholds.
- 3rd-party relationships concerning industry and/or regulatory requirements (i.e., HIPAA, etc.) must be reviewed on no less frequent than an annual basis.

Management

- 3rd-party agreements and contracts must specify:

  - The CSU information the vendor should have access to, and how it will be used,
  - How CSU information is to be protected by the 3rd-party,
  - How CSU information is to be transferred between CSU and the 3rd-party,
  - Acceptable methods for the return, destruction, or disposal of CSU information in the 3rd-party's possession at the end of the relationship/contract,
  - Minimum information security requirements,
  - Information security incident response and notification requirements,
  - Right for CSU to audit 3rd-party information security protections and controls.
- If the 3rd-party subcontracts part of the information and communication technology service provided to CSU, the 3rd-party is required to ensure appropriate information security practices are followed throughout the supply chain,
- The 3rd-party must only use CSU Information Resources for the purpose of the business agreement and/or contract,
- Work outside of defined parameters in the contract must be approved in writing by the appropriate CSU point of contact.
- 3rd-party performance must be reviewed annually to ensure compliance with agreed upon contracts and/or service level agreements (SLAs). In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met.
- The 3rd-party's major IT work activities must be entered into or captured in a log:
  - Made available to CSU IT management upon request, and
  - Must include events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Any other CSU information acquired by the 3rd-party during the contract cannot be used for the 3rd-party's own purposes or divulged to others.
- 3rd-party personnel must report all security incidents directly to the appropriate CSU IT personnel.
- CSU IT will provide a technical point of contact for the 3rd-party. The point of contact will work with the 3rd-party to ensure compliance with this policy.
- 3rd-parties must provide CSU a list of key personnel working on the contract when requested.
- 3rd-parties must provide CSU with notification of key staff changes within 24 hours of change.
- Upon departure of a 3rd-party employee from a contract, for any reason, the 3rd-party will ensure all sensitive information is collected and returned to CSU or destroyed within 24 hours.
- Upon termination of contract, 3rd-parties must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of CSU, the 3rd-party must surrender all CSU badges, access cards, equipment and supplies immediately.
- Any equipment and/or supplies to be retained by the 3rd-party must be documented by authorized CSU IT management.

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 Third-Party Information Security Risk Review 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.AM-1, ID.AM-6, ID.BE-1, ID.SC-1, ID.SE-2, ID.SE-3, ID.SE-4, ID.SE-5, PR-AT-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	