Northwestern University

Approving University Official(s): Chief Information Officer
Responsible Office: Information Technology
Effective date: January 1, 2022
Next review date: January, 2023

Information Security Policy

Policy Statement

Northwestern University is committed to securing information and data commensurate with applicable privacy and information security laws and regulations. An information security policy is foundational to this commitment. This Information Security Policy (hereafter "Policy") is established to ensure the protection of all Information and Communication Technologies (ICT) as well as Institutional Data for which Northwestern University is responsible.

All ICT and Institutional Data must be secured with manual and/or automated controls to a level of protection that reduces the University's risk to a level deemed acceptable, in addition to meeting applicable regulatory, legal, and contractual obligations.

All members of the University community, including without limitation, Data Stewards, Data Trustees, faculty, and staff, are responsible for adhering to published information security policies, guidelines, standards, and procedures. Departments and units may impose more stringent procedures, as they deem appropriate and necessary, to comply with specific regulatory, legal, or contractual obligations.

Purpose

The purpose of this policy is to establish the requirement, commitment, and accountability for defining information security policies, guidelines, standards, and procedures that will protect all ICT as well as the Institutional Data for which Northwestern University is responsible, in order to comply with privacy and security, regulatory and contractual requirements bestowed upon or accepted by the University.

Audience

This policy is platform and technology agnostic. It applies to all Northwestern University locations, schools, departments, affiliates, faculty, staff, researchers, workforce members, contractors, vendors, and sponsored affiliates. It encompasses all Institutional Data as well as third-party vendors/processors who collect, process, share, or maintain University's Institutional Data, whether managed or hosted internally or externally, and systems, applications, storage devices, and other technologies (e.g., personally owned devices) that collect, process, share, or maintain University's Institutional Data.

Definitions

Chief Information Security Officer (CISO): A University-wide role responsible for coordinating and overseeing security protection and information security governance across the University.

Data Trustees: Deans, Vice Presidents, Chairs, Unit Leader(s) and/or Director(s) responsible for the Data Content that falls under their purview.

Data Privacy Officer (DPO): A privacy role held within Northwestern responsible for coordinating and overseeing privacy protection and data privacy governance across the University.

Data Stewards: Assigned by a Dean, Vice President, Chair, Unit Leader and/or Director responsible for assisting the Data Trustee in managing the Data Content that falls under their purview. Principal Investigators (PIs) and other researchers are considered Data Stewards for their research data.

Information and Communications Technologies (ICT): An umbrella term used to describe all information and communication technologies, that includes, but is not limited to, the Internet, wireless technologies, software, systems, applications, public/private/hybrid cloud, computers, social networking, as well as other media applications and services. See https://csrc.nist.gov/glossary/term/information_and_communications_technology.

Institutional Data: All data that the University is responsible and accountable for protecting. This data includes, but is not limited to data the University collects, owns, intellectual property owned by faculty or others, staff data, student data, faculty data, research data, alumni data, vendor and contractor data, and data that the university shares or provides to third-parties for storage, processing, and analysis.

Security Leads/Information Security Designates: Roles held within schools and business units who are designated as responsible for coordinating and leading privacy and security initiatives within their school or unit.

Senior Leadership: Designated senior academic and administrative officials within the University who have the authority to take and/or direct the actions set forth in this Policy.

Supplier: Any third-party or vendor with which the University contracts.

University Business: Any activity carried out under the auspices of Northwestern University and in furtherance of the University's mission.

Policy Implementation

This Policy requires the establishment of an information security governance structure across the university, identifying individuals who will have specific responsibilities for maintaining appropriate processes and controls as detailed below.

a. Senior Leadership

Senior Leadership is responsible for establishing mechanisms to ensure that all information, communication technologies and institutional data conform to this Policy and all applicable policies, guidelines, standards, and procedures by:

- Establishing an Information Technology Executive Committee
- Establishing an Information Security Advisory Committee (ISAC)
- Establishing a Research Security Committee
- Establishing the role of University-wide Chief Information Security Officer
- Establishing the Information Security Office

b. Information Technology (IT) Executive Committee

The IT Executive Committee is responsible for all major IT decision-making for the University and provides guidance, as well as sets IT priorities to enable the University to balance its improvement goals with available resources in alignment with the University's strategic goals and mission.

- Members are senior administrators at the University, including the Vice President for Information Technology and Chief Information Officer, along with representation of senior leaders from the Office of the Provost, Office of the Executive Vice President, and Office of the Vice President for Research.

c. The Information Security Advisory Committee

The Information Security Advisory Committee (ISAC), is responsible for monitoring the security maturity and controls of the University, and providing approval for all security vulnerability exceptions that pose a significant or high risk to the University.

- The University CISO will consult with school and business unit Information Security Leads/Designates and will submit exceptions to the application of this Policy as well as any support guidelines or standards to the ISAC for approval.
- Members are a representative group of school/unit business unit leaders, their CIOs, or their designates.

d. The Research Security Committee

- The Research Security Committee is responsible for coordinating the architecture and compliance of tools and technology used for research across the University, and for aligning the strategic priorities of the University around research and information security.
- The Research Security Committee will provide regular reporting to other technology governance groups with regard to the need for or application of cybersecurity controls, initiatives, or technologies for research activities at the University.
- Members are a representative group of leadership related to research-intensive schools, research cores and centers, in addition to participation from the Office for Research, Compliance, and Northwestern IT.

e. The Information Security Office

- The Information Security Office (ISO) is responsible for assisting the University in achieving its University Business with the appropriate controls and protections surrounding data privacy and information security in order to conform with privacy and security regulatory and contractual requirements bestowed upon or accepted by the University.
- The ISO will consult and advise with the DPO, school and business unit Data Trustees, Data Stewards, CIOs, and/or Security Leads, assisting them in threat and vulnerability assessments, contractual and vendor risk assessments, control monitoring and tracking, and any required independent audits or certifications.
- The ISO as directed by the University CISO will define guidelines, standards, and program procedures for the University, so that the University can meet its privacy and security requirements, whether regulatory or contractual.

Related Information

- All supporting IT Policies, Guidance, Standards, Practices, and Procedures (https://it.northwestern.edu/policies)
- Data Classification Policy
- Privacy Policy

Contacts

Questions regarding this Policy:

- Chief Information Security Officer or designate at security@northwestern.edu
- Vice President of Information Technology and Chief Information Officer at vp-infotech@northwestern.edu.

History

Policy Origination Date: New, Effective January 1, 2022

Policy URL:

https://policies.northwestern.edu/docs/information-security-policy.pdf