Northwestern University

Approving University Official(s): Vice President for Operations
Responsible Office: University Compliance
Sponsoring Office(s): Information Technology
Effective date: September 1, 2022
Next review date: September, 2023

Data Classification Policy

Policy Statement

Northwestern University is committed to protecting data commensurate with laws and regulations on privacy and security that apply to the University community. Appropriate classification of data is fundamental and foundational to data protection. This Data Classification Policy (hereafter "Policy") is established to safeguard all data for which Northwestern University is responsible to an appropriate level of protection.

All Institutional Data, in consideration to the level of sensitivity and criticality of the data and systems that support Institutional Data, must be identified and classified so that protections, oversight, and monitoring are performed in accordance with policies, guidelines, and technical standards defined by the University.

This policy establishes four distinct levels of classification based on the impact of disclosure, loss, unauthorized access, or destruction of data:

Level 1

The unauthorized disclosure, loss, access, or destruction of Level 1 Data would have **no or very limited** adverse impact on the University, its brand, operations, assets, employees, students, or affiliates. Examples of Level 1 Data include: Non-Confidential Data and Public Data.

Level 2

The unauthorized disclosure, loss, access, or destruction of Level 2 Data would have **publicly noticeable** adverse impact on the University, its brand, operations, assets, employees, students, or affiliates. Examples of Level 2 Data include: Personal Private Data (such as employee records or donor information) and Business Sensitive Data (such as internal accounting information, or contracts between the University and third parties).

Level 3

The unauthorized disclosure, loss, access, or destruction of Level 3 Data would have a **serious** or severe adverse impact on the University, its brand, operations, assets, employees, students, or affiliates. Examples of Level 3 Data include: Business Sensitive Data (such as restricted financial information), Personal Private (such as social security numbers), HIPAA PHI data, Contractually/Legally Restricted Data (such as controlled unclassified information (CUI)). A differentiating factor between Level 3 and Level 2 data is the risk of civil or criminal penalties that exist for Level 3 data.

Level 4

The unauthorized disclosure, loss, access, or destruction of Level 4 Data would have a **severe or catastrophic** adverse impact on national security and/or the University, its brand, operations, assets, employees, students, or affiliates. Loss or compromise of Level 4 data has an inherent risk of significant fines or penalties, regulatory action, or civil or criminal violations. An example of Level 4 data is Classified Data.

Given the volume of Institutional Data currently stored and processed at the University, it is understood that the data classification procedures outlined in this Policy will take significant time to implement across the University. All Data Trustees must ensure, however, that any systems, applications, or projects created, implemented, or substantially revised after the effective date of this Policy that interact with Institutional Data conform to the classification, protection and governance standards contained in this Policy.

Purpose

The purpose of this policy is to identify and classify all Institutional Data as well as identify and implement appropriate controls (manual and/or technical) in order to conform with all of the 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," third-party vendors/processors who collect, process, share, or maintain the 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 Northwestern's Institutional Data.

Definitions

Business Sensitive Data: Information about the internal operations, finances, and other non-public information that is sensitive to the operations of the University. This data type is also referred to as Internal and requires Level 2 or Level 3 framework controls depending upon the risk to the University, quantity of data fields, data types, and regulatory requirements that are applicable.

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

Classified Data: Information that is given a classification by an agency of the United States Government and requires the protection of data to an established data protection standard. These data protection standards will equate to Level 4 framework controls. As of the effective date of this policy, data of this type is not permitted at Northwestern University.

Confidential Data: An umbrella term that encompasses all Non-Public Information. In the context of this Policy, Confidential Data includes Personal Private Data, Business Sensitive Data, CUI (Controlled Unclassified Information), Contractually/Legally Restricted Data, and Classified Data.

Contractually/Legally Restricted Data: Unclassified information that is deemed by contractual obligations or regulatory requirements (foreign or domestic) to require a defined minimum level of protection. This data type requires Level 3 framework controls due to risk to the University, quantity of data fields, data types, or regulatory requirements that are applicable.

Data Content: All Institutional Data and Non-Confidential Data within a Unit.

Data Governance Steering Committee (DGSC): A representative group of Data Trustees or their representatives (i.e., Data Stewards).

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 Steward: A person 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) are considered Data Stewards for their research data.

Information Security Advisory Committee (ISAC): Comprised of school/unit leaders and 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.

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

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

Level 1, 2, 3, and 4 Framework Controls: A defined set of control requirements and controls defined by the university in a data protection standard that shall be implemented to protect Institutional Data and ICT commensurate with contractual, regulatory, or industry best practices.

Non-Confidential Data: Any information that is available in the public domain. This type of data may be Public (not licensed) or Public (licensed), and unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of non-confidential data include press releases, course information, research publications, and other materials found on public websites. While little or no controls are required to protect the confidentiality of Non-Confidential data, a minimum level of control is required to prevent unauthorized modification or destruction of Non-Confidential Data. This data type is also referred to as "Public" and requires Level 1 framework control.

Non-Public Information: Any information that is classified as Confidential according to the data classification schema defined in this policy. This data type requires Level 2, Level 3, or Level 4 framework controls depending upon the risk to the University, quantity of data fields, data types, and regulatory requirements that are applicable.

Personal Private Data: Information about a person and requires Level 2 or Level 3 framework controls depending upon the risk to the University, quantity of data fields, data types, and regulatory requirements that are applicable, based on location of where the person is from, where the person lives, and where the data is stored. Personal Private Data includes, but is not limited to, data included in the definition of Personal Identifiable Information (PII): https://csrc.nist.gov/glossary/term/PII.

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 for 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

Institutional Data must be classified in accordance with the definitions provided herein. All data – regardless of platform or source – must be identified, documented, and classified to ensure appropriate protection. The individuals responsible for ensuring compliance with this Policy and their specific responsibilities are described below.

a. Senior Leadership

Senior Leadership is responsible for establishing mechanisms to ensure that data and information and communications technologies within their areas conform to this Policy by:

- Establishing a Data Governance Steering Committee (DGSC);
- Establishing the role of Data Privacy Officer
- Establishing the role of Data Trustees and Data Stewards;
- Ensuring that data has identified Data Trustees and Data Stewards; and
- Ensuring that schools and business units protect all Institutional Data to a level commensurate with the data protection standards defined for the type of data.

b. The Data Governance Steering Committee

- The Data Governance Steering Committee (DGSC), will have the responsibility for monitoring the collection, classification, protection, and dissemination of data, and recommending to the ISAC and IT Executive Committee a prioritization schedule for remediating data and/or technology privacy and security issues with University Institutional Data, with a particular focus on University "Confidential Data."
- Representative leadership from the DGSC will consult with school and business unit Information Security Leads/Designates, Data Trustees, and Data Stewards and will submit approval of exceptions to the application of this Policy and supporting IT and Privacy guidelines or standards to the DGSC for approval.
- Members are a group of Data Trustees, representative of the major types of data (e.g., student, alumni, research, finance and operations, etc.) within the University, and/or Data Trustees from major school/unit business units, and/or Security Leads or their designates, and the University CISO.

c. Data Trustees

- Senior Leadership within each unit will designate Data Trustee(s) with the responsibility for managing the Data Content that falls under their purview commensurate with the obligations set forth in this policy and supporting standards and procedures. Senior Leaders may themselves be Data Trustees if ultimate responsibility for security of Data Content under their purview lies with them. Senior Leaders may also designate Chairs, Unit Leader(s) and/or Director(s) as Data Trustees.

- Data Trustees are responsible for the privacy and security of the systems, applications, and information and communication technologies under their purview. Data Trustees must hold data creators, processors, managers, stewards, and other necessary parties accountable for ensuring data is protected according to University guidelines.
- Data Trustees, coordinating where applicable with unit IT leadership, will designate Information Security Leads, who will be responsible for coordinating and leading privacy and security initiatives within their school or unit
- Data Trustees coordinate with their Data Stewards and Information Security Leads to monitor these protection levels and oversee remediation processes as well as identifying any corrective actions.

d. Data Stewards

- Data Trustee's will designate Data Stewards to assist in the obligations set forth in this policy and supporting standards and procedures.
- Principal Investigators (PIs) are considered Data Stewards for their research data.
- Data Stewards are responsible for assisting the Data Trustees in meeting data protection policies and standards, and specifically coordinating local data privacy and security monitoring and reporting efforts and reporting on progress to the Data Trustee.
- Data Stewards must identify, document, and classify data in accordance with the Data Classification Guidelines supporting this policy.

Reporting and Responding to Data Classification and Protection Issues

a. Reporting

Data Trustees must provide regular updates on the maturity of their program, in accordance with Data Classification and IT Risk Management Guidelines. These reports will include any discrepancies in meeting established data protection standards, and remediation plans for addressing gaps, excluding approved exceptions. Reports will be submitted to the DPO on a schedule specified within the Data Classification and IT Risk Management Guidelines, who will consolidate and report all findings to the DGSC.

If schools or units are unable to address identified issues, the issue will be referred to DGSC for exception. Units will consult with Northwestern Information Technology as to any and all actions taken and will coordinate with Northwestern Information Technology to identify and document an appropriate accommodation, if applicable.

b. Remediation

Each unit's Dean, Vice President, Chair, Unit Leader and/or Director, in partnership with the DGSC, may require Data Trustees in cooperation with Northwestern Information Technology to establish a plan to remediate those portions of data governance that do not conform to the University's data protection standards.

c. Consequences of Violating this Policy

The DGSC is charged with responding to reports of non-compliance of data classification and data protection that do not conform to the University's Data Classification and Data Protection Standards. Non-compliance may be identified through self-reporting and other auditing mechanisms. Absent an applicable exception, the DGSC may require the school or unit that has non-conforming Data Content to be brought into compliance by designated staff or suppliers, and the expense of that work may be charged to the school, unit or department that is responsible for ensuring the privacy and security of

that content. If non-conforming Data Content remains out of compliance after repeated attempts by the DGSC to communicate with the Data Trustees, then, as a measure of last resort, the DGSC will submit to IT Executive Committee a request that Northwestern IT address the discrepancies for all significant violations, including the right to move equipment, services, and data to new platforms or providers.

Related Information

- This Policy is foundational and serves as a base for other Policies, including, but not limited to the following:
    - Privacy Policy
    - Information Security Policy
    - Research Data, Ownership and Retention Policy
- Data Use Agreements
- Level 1, 2, 3, and 4 Framework Controls
- Examples of University Data by Classification Level
- All supporting IT and Privacy Guidance, Technical Standards, and Procedures

Contacts

The following contacts can address questions regarding this Policy:

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

History

Policy Approval Date: January 31, 2022
Policy Effective Date: New, Effective September 1, 2022

Policy URL:

https://policies.northwestern.edu/docs/data-classification-policy.pdf