VANDERBILT UNIVERSITY

ADMINISTRATIVE POLICY

Data Classification Policy

Approval Authority:	**Chancellor**
Responsible Administrator:	**Senior Director of Information Security, VUIT**
Responsible Office:	**Information Security**
Policy Contact:	**Senior Director of Information Security, VUIT**

Originally issued:
May 11, 2020

Current version
effective as of:
May 11, 2020

PURPOSE

The purpose of this policy is to establish a framework for categorizing Vanderbilt data and information according to its level of risk, value, and criticality to the University. Classification aids in determining the level of security and management required to protect the information.

SCOPE

This policy applies to all persons and entities who access the University's data or computing and network facilities. This group includes students, faculty, staff, researchers, contractors, visitors, and any others accessing the University's data or computing and network facilities. It applies in all locations where the University conducts its activities without geographical limits, subject to applicable local laws and regulations.

This policy applies to all information and data owned by the University, under the University's custody, or otherwise present in the University's network or computing environment. This data may be held on any of the University's premises or in any external or cloud-based IT infrastructure licensed, rented or contracted by the University or on the University's behalf. This policy also includes data held on personal devices on the University's behalf.

This policy applies to the classification of institutional data belonging to the University. It also applies to research data.

DEFINITIONS

Information is defined as all forms and formats of information, including electronic, optical, and paper formats, as well as textual and audio-visual communications.

Data means information held in a structured, logical format, in files, or in a database. Data may be held on local devices, on premises in managed IT infrastructure, or in the cloud.

Institutional data is all data maintained to support delivery of Vanderbilt's central mission of scholarly research, informed and creative teaching, and service to the community and society at large, *except research and teaching data*. It includes data to support the auxiliary services that Vanderbilt delivers.

Research data is data generated by research.

DATA CLASSIFICATION

Data Classification

Classification, in the context of information security, is the categorization of data and information according to its risk impact. The levels of risk are defined with reference to the risk categorization methodology used by the Enterprise Risk Committee (see section “Determining Classification” below).

These definitions account for the sensitivity of the data and the financial, reputational, operational, and/or other impacts to the University should the information be disclosed, altered or destroyed without proper authorization.

Classification helps ensure baseline security controls are commensurate with the risk impact associated with the given class of data. Some data are intentionally public, although frequently managed to avoid amendment by unauthorized users. Some data will require Single Sign-On protection only, while other data may require Multi-Factor Authentication. Some data will require customized security to reflect its unusually sensitive nature. Security controls are defined by Vanderbilt’s Minimum Security Standards, which are separate to this policy.

Vanderbilt requires all information to be classified into one of four classifications, distinguished from each other by the level of security required.

Level 1 - Public

Information should be classified as “Level 1 - Public” when its unauthorized disclosure, alteration or destruction would result in little or no risk to the University and its affiliates. It should also be classified as “Level 1 – Public” if the failure to make the information public would be a risk to the University (e.g., public tax documents).

Examples of “Level 1 - Public” include press releases, course information, and research publications.

Level 2 - Institutional Use Only

Information should be classified as “Level 2 - Institutional Use Only” when its unauthorized disclosure, alteration or destruction could result in a moderate level of risk to the University or its affiliates.

Level 2 is the default classification. Examples of Level 2 could include email lists and internal policies and standard operating procedures.

Level 3 - Restricted

Information should be classified as “Level 3 - Restricted” when its unauthorized disclosure, alteration, or destruction could cause a significant level of risk to the University or its affiliates.

Examples of “Level 3 - Restricted” include information protected by state or federal privacy regulations (e.g., FERPA, HIPAA), or by standard confidentiality agreements. “Level 3 – Restricted” data require high levels of security, but are also frequently used regularly by many people to support the normal activities of the University. Therefore, security needs to be stringent, but not detrimental to normal functioning of the University.

Level 4 - Critical
Information should be classified as “Level 4 – Critical” when its unauthorized disclosure, alteration, or destruction could cause a very high level of risk to the University or its affiliates.

Examples of “Level 4 – Critical” include data or information governed by regulatory or oversight bodies, e.g. US Department of Defense, which identifies and requires the implementation of a comprehensive security standard, e.g., NIST 800-171. Specific examples may include export controlled data such as ITAR or EAR. “Level 4 – Critical” data will frequently be limited to a relatively small number individuals. The consequences for mismanagement of “Level 4 – Critical” data would normally be very high reputationally or financially for the University.

Classification Responsibilities

Vice Chancellors have oversight and accountability for the classification and inventory of data in their areas and ensuring that appropriate information security measures are in place. Vice Chancellors may delegate the determination of classification levels, establishing security measures, and maintaining the information inventory to Data Owners in their areas.

For institutional data, Data Owners (as defined by the Data Governance Framework) are normally responsible for classifying the data in their domain. The Data Governance Committee, including relevant expertise from VUIT and the Office of General Counsel, will review and approve information classification decisions for institutional data.

The process for classifying research data will be overseen by the Office of the Vice Provost for Research, working closely with Principal Investigators, VUIT, the Office for Sponsored Program Administration, and others as required.

Classification of information that is not structured as a database/table (i.e., documents, audiovisual files, etc.) should be done by the individual assigned by the relevant Vice Chancellor to oversee records management in that area.

Determining Classification

Information classification reflects the level of financial, reputational, operational, and/or other impacts to the University should the information be disclosed, altered or destroyed without proper authorization.

For some information and datasets, the classification may be obvious, such as when federal laws require the University to protect specific types of data (e.g. personally identifiable information will not be lower than “Level 3 – Restricted”). Several “predefined” classifications are outlined in the Appendix to this policy.

For other information and datasets, classification may be a matter of judgment. If the appropriate classification is not obvious, the impact table below may help in considering the different sources and levels of risk.

	IMPACT MEASURES		
Impact Areas	**LOW**	**MEDIUM**	**HIGH**

Financial	Loss of less than $5 million.	Loss of $5 to $20 million.	Loss of $20 million or more.
Operational	Localized (single unit/department) disruption of less than 1 week	Campus-level, week-long disruption of critical service or unit	Significant enterprise-wide disruption
Reputational	Unlikely to generate more than limited short-term, local media attention	Likely to generate media attention in major outlets (e.g., Wash Post) or that is longer than short-term	Significant long-term media attention (i.e., national or international)
Compliance/Legal	Minor compliance exposure or legal liability	Significant compliance exposure or legal liability	Serious compliance exposure or legal liability

As the total potential impact to the University increases from Low to High, the classification of data should become more restrictive moving from “Level 1 – Public” to “Level 4 – Critical”. If an appropriate classification is still unclear after considering these points, contact the Data Governance Committee for assistance.

A single classification may be assigned to data that is common in purpose, function, or where/how it is stored, even if different data elements within the data set have different levels of sensitivity. When classifying a set of data, the most restrictive classification of any of the individual data elements should be used. If various data elements can be treated differentially and it reduces cost/effort to assigned varying classifications, then Data Owners may wish to propose this approach.

Minimum Security Standards

Each classification level requires a specific level of technical and procedural security controls to manage the risk impact for the given class of data. VU Minimum Security Standards xxx defines minimum standards security standards that must be adhered to for each class of data. While a number of the security controls will be implemented at the enterprise level by VUIT, it is imperative for Data Owners to understand and implement technical and procedural controls that can only be implemented locally.

APPENDIX A

Predefined Types of “Level 3 – Restricted”
The Data Governance Committee and Systems Security Officer have defined several types of “Level 3 – Restricted” based on state and federal regulatory requirements. They are defined as follows:

1. **Personally Identifiable Education Records**

Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers:

- Name of the student
- Name of the student's parent(s) or other family member(s)
- The address of the student or the student's family
- A personal identifier, such as the student's Social security number or student number
- Other indirect identifies, such as the student's date of birth, place of birth, and mother's maiden name.
- A list of personal characteristics that would make the student's identity easily traceable
- Any other information or identifier that would make the student's identity easily traceable

See Vanderbilt University's Student Privacy Statement (https://registrar.vanderbilt.edu/ferpa/vanderbilt-student-privacy-statement.php) for more information on what constitutes an Education Record.

2. Personally Identifiable Information ("PII")

Information which can be used to distinguish or trace an individual's identity, such as their name in combination with any of the following::

- Social Security Number
- State-issued driver's license number
- Financial account numbers credit or debit card number, in combination with any required security code, access code or password required to access the account.

3. Protected Health Information ("PHI")

PHI is any health information that can be tied to an individual, which under HIPAA means protected health information includes one or more of the following 18 identifiers. If these identifiers are removed the information is considered de-identified protected health information, which is not subject to the restrictions of the HIPAA Privacy Rule.

- Names (Full or last name and initial)
- All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
- Dates (other than year) directly related to an individual
- Phone Numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers

- Certificate/license numbers
- Vehicle identifiers (including serial numbers and license plate numbers)
- Device identifiers and serial numbers;
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

Predefined Types of "Level 4 – Critical"
The Data Governance Committee and Systems Security Officer have defined several types of "Level 4 – Critical" information based on state and federal regulatory requirements. They're defined as follows:

1. **Export Controlled Materials**

   Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State.

2. **Federal Tax Information ("FTI")**

   FTI is defined as any *return*, *return information* or *taxpayer return information* that is entrusted to the University by the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.

3. **Payment Card Information**

   Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

   - Cardholder name
   - Service code
   - Expiration date
   - CVC2, CVV2 or CID value
   - PIN or PIN block
   - Contents of a credit card's magnetic stripe
   - Device identifiers and serial numbers
   - Universal Resource Locators (URLs)
   - Internet protocol (IP) addresses
   - Biometric identifiers, including finger and voice prints
   - Full face photographic images and any comparable images
   - Any other unique identifying number, characteristic or code that could identify an individual

RELATED POLICIES/DOCUMENTS

Vanderbilt Data Governance Framework (in draft)
Vanderbilt Minimum Security Standards (in progress)

HISTORY

Issued: **05/11/2020**

Reviewed: **Approved by Interim Chancellor and Provost Susan R. Wente, 05/11/2020**
Comment

Amended:
Comment