Section:	Information Technologies Policies
Policy Name:	Information Security Policy
Policy Owner:	EVP
Responsible University Office:	Vice President for Information Technologies
Origination Date:	July 1993
Revisions:	October 6, 2005, May 2013, February 26, 2018

I. SCOPE OF POLICY

A. This policy expands upon the data governance framework established by the University Data Governance Policy to address requirements, roles, and responsibilities related to the security of IT resources.

B. Privacy and security practices protect University information and allow the use, access and disclosure of such information in accordance with University missions and applicable laws, regulations, contracts, and/or funding agency requirements.

C. This policy establishes responsibility to manage IT resources in accordance with the security standards and controls set forth in this policy. The confidentiality, integrity and availability of University information must be maintained and protected to support the University's missions and to comply with laws, regulations, and contractual obligations.

D. This policy establishes a University-wide information security framework to:

1. Protect against unintentional, unlawful, or unauthorized disclosure, alteration, or destruction of sensitive information that could potentially result in harm to the University, members of the University community, other organizations, or the nation.
2. Protect against anticipated threats to the security of IT resources.
3. Comply with federal, state, and local law; University policies; and agreements that bind the University to implement applicable security controls.

E. This policy applies to all individuals who have access to IT resources used for University purposes and encompasses the safekeeping of University information in any form—including, but not limited to, spoken, printed, audio, video and digital/electronic media—and in all locations—including, but not limited to, in storage media, in e-communications, in the cloud, and on personal devices. **Note:** for the purposes of this policy, "University purposes" do not include students or employees accessing or updating their individual University information.

II. DEFINITIONS

A. "Availability" means ensuring timely and reliable access to and use of University information.

B. “Confidentiality” means preserving authorized restrictions on University information access and disclosure, including means for protecting personal privacy and proprietary information.

C. “Council for Data Governance (CDG)” is the University council responsible for overseeing the appointment and action of data trustees for each of the University’s functional areas. It includes the Chief Information Officer, VP & General Counsel, and other members as appointed by the President and/or his or her delegates.

D. “Data Security Advisory Committee (DSAC)” is the University council responsible for coordinating information security and risk management efforts and monitoring and recommending necessary security actions to the University. It is chaired by the director of IT Security Policy & Compliance and includes delegates as may be appointed from time to time by data trustees and/or the chair.

E. “Data steward” is an individual within the University who is the primary institutional authority for a particular data set and who is principally responsible for the management and security of that data set across the institution.

F. “Data stewardship” is the responsible oversight of a data set, including principal responsibility for the establishment of standards and guidelines for appropriately managing and securing that data across the institution.

G. “Data trustee” is an executive officer of the University who has the highest level of strategic and policy-setting authority and responsibility for his or her functional area.

H. “End user” is any individual who accesses and/or utilizes IT resources.

I. “Functional area” is one or more units that have primary responsibility for managing a core University mission or business function.

J. “Integrity” means guarding against improper modification or destruction of University information, and includes ensuring non-repudiation and authenticity.

K. “IT device” is any device involved in the accessing, processing, storage, or transmission of University information and making use of the University IT infrastructure or attached to the University network. These devices include, but are not limited to, desktop computers, laptop computers, personal digital assistants, server systems, network devices such as routers or switches, and printers.

L. “IT resources” are the full set of University owned or controlled information technology devices and data involved in the processing, storage, accessing, and transmission of information.

M. “Local support provider” is an individual or unit with primary responsibility for the installation, configuration, security, and ongoing maintenance of an IT device.

N. “Privacy” means (1) an individual’s ability to conduct activities without concern of or actual observation and (2) the appropriate protection, use, and release of information about individuals.

O. “Security controls” are the administrative, operational, and technical requirements and recommended best practices for meeting security standards.

P. “Security standards” are the requirements for achieving risk management objectives and compliance with laws, regulations, and policies.
Q. “Unit” means a University department, school, institute, program, office, initiative, center, or other operating unit.
R. “Unit head” is a University official with the highest level of authority over the day-to-day management or oversight of a unit’s operation.
S. "University information" is defined as any information within the University’s purview, including information that the University may not own but that is governed by laws and regulations to which the University is held accountable. University information encompasses all data that pertains to or supports the administration and missions, including research, of the University.
T. “University information classifications” are the categories of University information that have different security requirements based on their potential impact due to a loss of confidentiality, integrity, or availability.

III. POLICY STATEMENTS

A. All IT resources must be managed in compliance with applicable federal, state, and local laws; University policies; and agreements.
B. University of Delaware Information Technologies (IT) is authorized to develop, promulgate, and enforce information security program requirements for the University. These requirements may include policies, procedures, security standards and controls, roles, and responsibilities for the protection of IT resources.
C. All end users must comply with the requirements mandated by this policy, including administrative, operational, and technical security controls.

IV. POLICY STANDARDS AND PROCEDURES

A. All end users are responsible for protecting IT resources by complying with appropriate administrative, operational, and technical security standards and controls commensurate with the requirements for its classification. The University Information Classification Policy establishes the University information classifications.
B. The Secure UD Data Governance & Security Program (Secure UD DGSP) establishes administrative, operational, and technical mandates for the security and management of IT resources.
C. Exceptions to this policy, including exceptions to the requirements of the Secure UD DGSP, must be justified by operational or technical needs and must be submitted to and approved by unit heads.
D. Roles and responsibilities

1. Data trustees
    a. Define risk tolerance related to security threats to University information entrusted to their care.
    b. Are ultimately accountable for the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their functional areas.
    c. Require annual assessments of security controls within their functional areas and report the results to IT.
2. Data stewards
    a. Require the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their stewardship.
3. Information Technologies
    a. Maintain overview responsibility for implementation of this policy.
    b. Establish policy requirements, including security standards and controls, and monitor and enforce compliance.
        1. Develop a comprehensive security program that includes risk assessments, best practices, education, and training.
        2. Having IT assume this responsibility does not abrogate the responsibility of individuals and units to comply with policy requirements.
    c. Train and educate the University community on this policy.
    d. Monitor technological developments, trends, and changes in laws and regulations and update this policy as appropriate.
    e. Conduct annual reviews of minimum technical requirements and update this policy, with appropriate review.
    f. Assist units in understanding risk and in identifying and implementing security controls to protect IT resources.
    g. Issue critical security notices to units.
    h. Develop, implement, and maintain University-level security monitoring and analysis.
4. The Data Security Advisory Committee (DSAC)
    a. Assist in the implementation of this policy.
    b. In consultation with the VP & General Counsel, monitor federal, state, and local laws and regulations affecting information security and privacy.
    c. Stay abreast of evolving best practices in information security and privacy in higher education.
    d. Assess risks to University information and recommend updates to this policy, including the Secure UD DGSP, as necessary.
5. Unit heads

   a. Assume primary compliance responsibility for the IT resources under their control.
   b. Identify local support providers and report those individuals or units to IT.
   c. Develop and implement an information security plan for the unit consistent with the requirements of this policy and commensurate with the specific security needs of the unit.
   d. Thoroughly understand the security risks impacting University information under their control. Security risks should be documented and reviewed with the appropriate data steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. IT can assist unit heads with gaining a better understanding of their security risks.
   e. Ensure the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their units.
   f. Approve exceptions to this policy based on operational or technical needs.
   g. Report to data trustees the unit’s compliance with information security requirements at least annually.

6. Local support providers
   a. Maintain knowledge of the IT devices for which they are responsible.
   b. Implement, at the direction of the unit head, security controls for the IT devices for which they are responsible.
   c. Understand and document the configurations and characteristics of the IT devices for which they are responsible.
   d. Recommend security controls and practices for the IT devices for which they are responsible.
7. End users
   a. Adhere to unit procedures for implementing security controls.