THE TRUSTEES OF TRINITY COLLEGE
POLICY ON INFORMATION SECURITY

Trinity College Policy No. 11.2.1

Policy Statement

Maintaining the security, confidentiality, integrity, and availability of data stored within Trinity College technology resources is a responsibility shared by all users of those systems. This policy on information security sets forth the requirements for managing and protecting the security, confidentiality, integrity, and availability of college technology resources and data. This policy applies to all Trinity College technology resources that are owned or managed by the college, that connect to the college network, that connect to another college technology or service, or that store college data or information. This policy applies to all college faculty, staff, students, contractors, and any other individual using college technology resources or data. To effectuate this policy, the college has adopted an information security program as described in detail below.

Definitions

Information Security Program

The Trinity College information security program is a set of coordinated services and activities designed to protect college technology resources and data, and manage the risks associated with the use of technology resources. The program includes the policies, standards, assessments, protocols, controls, and training needed to protect Trinity College's technology resources and data.

Data

"Data" means any data or information, regardless of format - electronic or printed - or location, that is created, acquired, processed, transmitted, or stored on behalf of Trinity College. College data includes the data processed or stored by the college in hosted environments in which the college does not own or operate the technology infrastructure.

Technology Resources

"Technology resources" means:

- any computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of Trinity College data;
- any technologies or services that are owned or managed by the college, that connect to the college network, connect to another college technology or service, or store college data or information; and
- any services or applications used by the college in hosted environments in which the college does not own or operate the technology infrastructure.

Information Security Program

The college will develop, document, implement, and periodically update an information security program to protect its technology resources and data ("the Program"). The Program will describe the security controls in place or planned and the rules of conduct for individuals

accessing college technology resources or data. The Program is intended to comply with the requirements of the "safe harbor" provided pursuant to Connecticut Public Act No. 21-119 Section 1(b)-(d). In particular, the Program will apply security standards and protocols that, at a minimum, are consistent with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), enhanced where applicable by specific controls from the family of NIST information security controls, including NIST Special Publication 800-171 and NIST Special Publication 800-53, as the foundation for its information security program.

Specific Program Requirements

A. *Risk and Compliance*

1. The Program will require periodic written risk assessments to evaluate the security risk to college operations, assets, technology resources, college data, and individuals resulting from the operation of college technology resources and the associated storage, processing, or transmission of college data. For each risk identified, the risk assessment will describe whether or how such risk will be mitigated or accepted, based on the risk profile established by the college.

2. The Program will develop and maintain classification levels for the college's data that are correlated to risk.

3. The Program will comply with relevant laws and regulations pertaining to its operation of technology resources and use of data, including, but not limited to, the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Gramm Leach Bliley Act (GLBA).

4. The Program will require that members of the college community, including information technology and information security personnel, are adequately trained to carry out their assigned information security-related responsibilities, as applicable.

B. *Identification, Authentication, and Protection*

1. The Program will uniquely identify and authenticate college technology resource users, processes, and/or devices. Authentication credentials must never be shared or revealed to anyone else besides the authorized user.

2. The Program will limit access to the college's technology resources and data to authorized users, processes, and/or devices with legitimate business needs.

3. The Program will allocate sufficient resources to adequately protect the college's technology resources and data throughout their respective lifecycles, and ensure that third-party providers employ adequate security measures to protect the college's technology resources and data.

4. The Program will establish and maintain baseline configurations and inventories of the college's technology resources and establish and enforce security configuration settings for college technology resources.

5. The Program will require periodic and timely maintenance on the college's technology resources and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

6. The Program will require periodic reviews of third-party technology providers and services to ensure that security agreements are being adhered to and enforced.

7. The Program will direct college personnel to monitor, control, and protect college communications (e.g., college data transmitted or received by college technology resources) at the external boundaries and key internal boundaries of the college network and employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within its technology resources.

8. The Program will require data encryption wherever practical to protect college data.

9. The Program will require the secure destruction or wiping (sanitizing) of college technology resources before reuse or disposal.

10. The Program will establish college security protocols and training that are appropriate for and commensurate with each employee's level of privilege and access to the college's technology resources and data. Privileged access control rights will be appropriately evaluated, approved, periodically reviewed, and limited to only those users and applications with legitimate and authorized business needs.

11. The Program will establish adequate protocols to protect the college's data and technology resources during and after personnel actions such as separations, terminations, and transfers.

12. The Program will limit physical access to the college's technology resources to authorized individuals, protect the physical plant and operating environments for college technology resources, and implement appropriate environmental controls in facilities containing college technology resources.

C. *Monitoring, Detection, Response, and Recovery*

1. The Program will identify, report, and correct technology resources vulnerabilities and system flaws promptly and protect against malicious code at appropriate locations within the college's technology resources.

2. The Program will continuously monitor information system security alerts and advisories and take appropriate actions in response.

3. The Program will create, protect, and retain the college's technology resource audit records to the extent needed to enable the monitoring, analysis, investigation, and

reporting of unlawful, unauthorized, or inappropriate activity on college technology resources, and ensure that the actions of individual technology resource users can be uniquely traced for all actions impacting college data.

4. The Program will continuously monitor the security controls implemented in the college's technology resources or applied to college data to determine if the controls are effective and to develop and implement appropriate plans to correct deficiencies.
5. The Program will establish an operational incident handling capability and process to identify, detect, respond, and recover from information security incidents.
6. The Program will regularly test the college's operational incident handling capabilities and processes to verify the college's ability to identify, detect, respond, and recover from information security incidents.
7. The Program will establish, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery for the college's technology resources to ensure the availability of those technology resources and data critical to the continuity of college operations.
8. The Program will regularly test the college's technology resources emergency response plans to verify the college's ability to ensure the availability of technology resources and data critical to the continuity of college operations.

Responsibilities
The roles and responsibilities for college information security includc:

Trinity College Board of Trustees
The Board of Trustees of the college is responsible for governing the affairs of Trinity College. The Board of Trustees and its committees, including the Audit & Risk Committee, oversee institutional information security risk at the governance level. The Board of Trustees ensures that information security is evaluated and assessed in the annual audit plan, and directs the college administration to conduct and report on risk assessments where necessary.

President
The President of the college has general responsibility and control of all of the business and affairs of the college. The President and President's Cabinet are accountable for providing executive oversight and support of the college information security program and for compliance with this policy.

Vice President for Library and Information Technology Services
The Vice President for Library and Information Technology Services is responsible for:

- reporting in writing to the Board of Trustees, regularly, and at least annually, regarding the overall status of the college's information security program and material matters related to the program;

- advising the Board of Trustees Audit & Risk Committee on college information security needs and resource investments;
- advising the President and President's Cabinet regarding college information security needs and resource allocation; and
- overseeing the implementation and enforcement of the college's information security program.

Associate Vice President & Chief Technology Officer
The Associate Vice President for IT is responsible for administering this policy and monitoring the effectiveness of the college information security program.

Lead Security Analyst
The Lead Security Analyst is responsible for leading the execution, maintenance, and enforcement of this policy and the college information security program.

Vice Presidents, Deans, Department Heads, and Supervisors
Vice Presidents, Deans, Department Heads, and Supervisors are responsible for ensuring that units, staff, and end-users receive appropriate information security training and adhere to college information security policies and standards.

Privileged Technology Administrators and Data Stewards
Privileged technology administrators and data stewards occupy unique positions of trust and responsibility that grants them enhanced access to college technology resources and college data. These individuals must take special care to:

- follow applicable college policies and procedures, including college information security policies, in exercising their privileged responsibilities;
- ensure that their privileged access is reserved for tasks that require the use of privileged access; and
- grant access to college technology resources and data only in response to legitimate business needs.

End-Users
All end-users of college technology resources, including students, faculty, and staff, are responsible for:

- following college information security policies;
- completing college-mandated information security training; and
- reporting promptly potential information security incidents.

Compliance
Violations of this policy or any law related to the use of college technology resources or college data, including, but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Gramm Leach Bliley Act (GLBA), may result in disciplinary action in accordance with the Student Handbook, Faculty Handbook, Employee Handbook, as appropriate, and/or any other applicable rules governing employment at Trinity College.

Responsible Officer
Vice President for Library and Information Technology Services or a designee appointed by the President

Key Offices to Contact Regarding the Policy and Its Implementation
Questions or clarifications regarding this policy should be reported to: security@trincoll.edu.

Actual or suspected information security incidents should be reported to security@trincoll.edu

Links to Procedures or Forms
Information technology policies and procedures can be found at:
https://www.trincoll.edu/lits/help-support/tech-support/security/information-technology-policies-procedures/

Date of Initial Policy
This policy was issued on February 1, 2022.