PL01 - Acceptable Use

Version: 2.0
Issued: 1/12/2017

PURPOSE

The purpose of this policy is to define the acceptable use of Trinity College applications, hardware, and other systems by Trinity College employees, contractors, and third parties.

SCOPE

This policy applies to all Trinity College employees, contractors, and third parties who access Trinity College systems.

POLICY

General Use

Access to information technology resources is a key component to facilitating the expansion of productivity and creativity of our users. As such, users are encouraged to use Trinity College information technology resources to the fullest extent in pursuit of the organization's goals and objectives.

Unacceptable Use

Trinity College electronic communications systems, including intranet, Internet, telephony, email, and messaging services, are to be used primarily for work-related purposes. Examples of inappropriate use of the Trinity College electronic communications systems include, but are not limited to: excessive use of Trinity Resources for non-Trinity related business, unreasonable or unauthorized personal use; storing, sending or forwarding e-mails that contain libelous, defamatory, racist, obscene, inappropriate, or harassing remarks; visiting or sending information to or receiving / downloading information from Internet sites involving inappropriate topics for non-academic use.

Trinity members shall not attempt to circumvent or disable protection mechanisms (e.g. Internet content filtering) that have been put in place by Trinity College.

Use of Technology

I. Access

Users of Trinity College (Nonpublic) information systems are authorized to access only systems, including hardware and software, where access has been previously approved.

II. Media

Employees using removable media, such as flash drives, are required to ensure their devices are clean of all malware and viruses prior to using them on Trinity resources.

Encryption

Occasionally users may have a business need to transfer or store, in a secure manner, information classified as confidential or restricted. In these instances, information must be protected using encryption methods that have been approved and are listed in the Trinity College encryption standards. (Encryption Policy) Users who may be unfamiliar with using encryption technologies should seek guidance from IT Staff. (Data Classification Policy)

III. Cloud Computing and Storage

Advances in cloud computing and storage offer a low-cost, convenient solutions to technology-based problems such as data storage and connectivity. Trinity College Users may not store Trinity data classified as Private, Restricted, Sensitive or Confidential, on any non-Trinity approved

storage sites. Cloud based tools include, but are not limited to, Box, Dropbox, iCloud, and Google Drive. (Data Classification Policy)

Computer Virus and Malware Protection

It is important that users take particular care to avoid compromising the security of the network. Users shall exercise reasonable precautions in order to prevent the introduction of a computer virus or other malware into the Trinity College network. Virus scanning software is installed on all Trinity College systems and is used to check any software downloaded from the Internet or obtained from any questionable source. Users are prohibited from disabling, or attempting to disable, virus scanning software. Users must scan portable media devices for viruses and malware before using them to see if they have been infected. If staff members are unsure of how to utilize virus and malware scanning tools it is recommended that they contact Trinity College IT Staff for additional information.

Messaging Technologies

Use of e-mail and other messaging technologies shall never be used to transmit confidential or restricted information in an unencrypted format (PII). Users must pay additional attention to e-mail content and senders and must not open e-mail attachments from unrecognized or suspicious senders. If there are questions about the security of an e-mail, e-mail attachment, or messaging technology users should contact the Trinity College IT Helpdesk, (http://www.trincoll.edu/Litc/its/help/Pages/default.aspx)

Information Protection

In the course of performing their jobs, users may have access to confidential or proprietary information. Information is classified in the Trinity College Data Classification Policy (Data Classification Policy). It is not permissible for users to acquire, or attempt to acquire, access to confidential data unless required by their jobs. Under no circumstances may users disseminate any confidential information, unless such dissemination is required by their jobs.

Incident Response (Incident Response Policy)

The Trinity College IT staff is tasked with responding to all IT security related incidents, such as computer virus infections, but in order to effectively respond to these events the IT staff relies on timely information and reporting from users. Subsequently, users are required to contact the IT Help Desk or another Trinity College IT staff member.

- They observe suspicious activity
- They know or suspect that a security incident has or is going to occur.

Password Use

Many of the Trinity College systems and applications require the use of a unique user identification and password. Users must never share their passwords with anyone else and must promptly notify IT personnel if they suspect their passwords have been compromised. Trinity College IT Staff should never ask for your password. Passwords should not be a single word or common phrase. All passwords must be at least eight characters in length and contain uppercase characters, lowercase characters, and at least one number and symbol.

Physical and Environmental Security

Assistance from users is required to facilitate a physically and environmentally secure working environment. Protection of Confidential and Restricted Data extends beyond the electronic format. Users are required to be aware of locking and access restriction mechanisms. Additionally, to aid in the physical security of workstations and information technology resources, users who will be leaving their devices unattended for extended periods must secure the space and log off or lock the system before leaving.

Problem Management

Users are required to report problems or issues discovered with Trinity College systems to the Trinity College Helpdesk (http://www.trincoll.edu/Litc/its/help/Pages/default.aspx) immediately following discovery.

ENFORCEMENT

Any employee found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including termination of employment.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Management Team	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented. Review this policy periodically and update as needed in response to environmental and/or operational changes.
All Users	Understand and adhere to this policy. Use Trinity College resources in only those methods, which have been identified as acceptable by this policy. Immediately report suspicious activities or violations of this policy to their manager or the IT Manager.

REFERENCES

	Name	Reference
Frameworks	**CoBiT 4.1**	DS5 DS8
	NIST	AC-8 System Use Notification IR-6 Incident Reporting PL-4 Rules of Behavior PS-6 Access Agreements PS-8 Personnel Sanctions

Regulations and Requirements	**Name**	**Reference**
	PCI DSS 3.1	Requirement 4 Requirement 5 Requirement 8 Requirement 12
	HIPAA/HITECH	§ 164.308(a)(1)(i): Security Management Process § 164.308(a)(1)(ii)(C): Sanction Policy § 164.308(a)(3)(i): Workforce Security § 164.308(a)(6)(i): Security Incident Procedures § 164.310(a)(1): Facility Access Controls § 164.310(a)(2)(ii): Facility Security Plan § 164.310(b): Workstation Use

This section contains revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
2.0	1/12/2017	Suzanne Aber	Revision Document