PL03 – Disk Encryption Policy

Version: 1.0
Issued: 1/12/2017

Purpose

This document provides the Trinity community with the requirements and guidelines necessary to effectively protect the confidentiality of restricted Information (sensitive data) of College owned data (DATA CLASSIFICAION POLICY). This policy will be effective immediately for all new computer hardware and applies to all Trinity-owned or Trinity-managed desktops and portable computing devices storing Confidential data. Existing computer hardware will be required to adhere to this policy effective one year from the official posting date.

Scope

The scope provides the policy and guidelines of approved encryption technologies for supported devices that are deployed at the College that store, transmit or process data classified as Confidential (DATA CLASSIFICAION POLICY). Whole Disk Encryption provides an additional level of protection for Confidential Data, (Data encrypted at rest). It prevents unauthorized parties from viewing any data stored on the device in the event of accidental loss or theft.

Policy Details

1. All portable computing devices that store, transmit or process data classified as Confidential are required to use whole disk encryption.

2. All desktops that store data classified as level 4 (Confidential) require whole disk encryption.

3. Encryption requirements

   a. ITS will centrally manage copies of encryption keys.

   b. Trinity College reserves the right to decrypt data using the centrally maintained key as required by law enforcement and or through approval of the Office of General Counsel.

4. Users will not attempt to disable, alter or remove the ITS deployed encryption software.

Encryption

Full Disk encryption in addition to file level encryption is currently considered to be the most secure solution to protect confidential data (at rest) in case of accidental loss or theft. This method does not protect the data from being viewed by unauthorized users in case of compromised credentials (username/password, loss of encryption key) or data in transit. While this policy recommends the use of whole disk and file level encryption, it only requires the compliance with the mandatory Full Disk encryption requirement at this time.

Guidelines:

Step 1 - Data Classification

Data classification will be determined by the level of sensitivity of the data and assigned by the data owner with support of ITS. The degree to which any data needs to be secured should be determined by the Data Classification Policy. Any data held at Trinity College should be classified between Level 1 (Public/Unclassified) and Level 4 (Confidential) as determined by the (DATA CLASSIFICAION POLICY)..

Step 2 - Encryption Technologies

Any encryption technology deployed should be native and supported by the operating system vendor. Devices with Microsoft Windows based operating systems are required to use BitLocker to comply with this policy, while devices using Apple OSX/iOS operating systems will use FileVault. Operating systems that do not support native encryption, or use an encryption technology that does not support the management of encryption keys by ITS, will require an alternative encryption technology that must be evaluated and approved for use by ITS.

Step 3 - Encryption Key Creation

The creation of the encryption/decryption keys will be completed with the assistance of Distributed Computing Support staff.

Step 4 - Encryption Key Management

Encryption keys will be securely stored with ITS. ITS will secure the encryption keys using standard security practices.

Step 5 - Encryption Key Recovery

Information Services will determine the technical and procedural processes for key retention, access and recovery.

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.

PL03 – Disk Encryption Policy

Version: 1.0

Issued: 1/12/2017

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

Frameworks	**Name**	**Reference**
	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
Supporting Standards and Procedures		

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

Version Number	Issued Date	Approval	Description of Changes
1.0	1/4/2017	Suzanne Aber	Original Document