# Encryption Policy

Version: 1.0
Issued: 4/12/2017

## PURPOSE

The purpose of this policy is to provide the information security requirements at ***Fitchburg State University (FSU)*** for the use of encryption algorithms to protect confidential and sensitive information. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

## SCOPE

This policy applies to the encryption algorithms used to protect confidential and sensitive information. A risk-based approach drives all ***FSU*** data encryption requirements. Considerations include legal or regulatory requirements, data inventory, classification, method(s) of access, storage or transmission mechanisms, and other contributing security controls in place.

## POLICY

***Fitchburg State University*** shall use approved encryption algorithms to protect sensitive and confidential information. ***Fitchburg State University*** must use only approved cryptographic techniques and follow Federal and State regulations and adhere to legal authority that is granted for the dissemination and use of encryption technologies outside of the United States.

## ENFORCEMENT

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

## ROLES AND RESPONSIBILITIES

| ROLE | RESPONSIBILITY |
|---|---|
| **Information Security Officer** | Ensure awareness and compliance with this policy.<br>Ensure that this policy and all component policies and procedures are maintained and implemented. |
| **IT Staff** | Ensure that confidential and restricted data is appropriately protected. |
| **Management Team** | Provide information to aid in the risk analysis to determine the necessity and applicability of encryption mechanisms. |
| **All Users** | Users who are unfamiliar with using approved encryption technologies should seek guidance from the ***FSU*** Information Security Officer. |

.

## REFERENCES

| Framework<br>COBIT 4.1 | Regulations and Requirements<br>PCI DSS - MA 201 | Supporting<br>Standards and Procedures |
|---|---|---|
| PO2.3 Data Classification Scheme<br>DS5.8 Cryptographic Management | PCI<br>Requirement 3: Protect Stored Cardholder Data<br>Requirement 4: Encrypt transmission of cardholder data across open, public networks. | |

# Encryption Policy

Version: 1.0
Issued: 4/12/2017

| Framework<br>COBIT 4.1 | Regulations and Requirements<br>PCI DSS - MA 201 | Supporting<br>Standards and Procedures |
|---|---|---|
| | MA 201 CMR 17:00<br>Section 17.15<br>Section 17.15 | |

## REVISION HISTORY

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

| Version Number | Issued Date | Approval | Description of Changes |
|---|---|---|---|
| 1.0 | 7/28/2015 | Compass ITC | Initial Draft |
| | | | |