# Computer Disk Encryption Policy

## Policy/Procedure

**1. Introduction**
The ever-increasing threat to financial liability and institutional and/or personal reputation in the event of data theft underscores that the security of College-owned technology must be the highest priority.

This policy outlines Dickinson's approach to data encryption on College-owned computers. Awareness and compliance with this policy will ensure that consistent computer security levels are maintained campus-wide to keep data, and users, safe and minimize exposure to security breach.

Library and Information Services reserves the right to apply security measures and updates, and modify operating system settings and functions on College-owned computers in the interests of protecting College data and the College community as a whole.

**2. Background**
The primary focus of data encryption is to prevent the theft of personally identifiable information (PII) due to lost or stolen College-owned computers by encrypting all data on a computer's hard drive. The definition of PII is collectively defined by the Financial Services Modernization Act of 1999, also known as the Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA - Public Law 104-191), the Family Educational Rights and Privacy Act (FERPA – 34 CFR Part 99), and the European Union's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Illicitly obtained PII can be used to commit identity theft as defined in the Federal Trade Commission's Red Flags Rule based on sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). While Pennsylvania state law defines a data breach (ie. the unauthorized access and acquisition of personal computerized data) in terms of specific PII (ie. data containing name and Social Security Number, name and driver's license number, or name and credit card number), institutional or personal damage can result from the theft of many other types of data other than PII. Disk encryption helps to prevent data breaches, the disclosure of which could expose Dickinson to possible substantial liability, by rendering all data on a computer's hard drive unreadable without authorized login credentials.

**3. Disk Encryption**
As it is not always known, even to the user, what information may be stored on the computers they use (ie. caching, inadvertent saved attachments, etc.), encryption is required for all College-owned laptops or mobile computers. For clarity, when denoting 'College-owned' computers, it should be noted that all computers, regardless of how the devices were originally funded (departmental funds, User Services funds, endowed funds, etc.) remain the property of Dickinson College.

User Services will deploy appropriate cryptographic security controls in conjunction with procedures that manage the associated encryption keys on College-owned computers. Cryptographic security controls will adhere to government Advanced Encryption System 256 algorithm standards.

It may be required to unlock a protected computer by obtaining a 48-digit Recovery Key. It is not permissible to write down or otherwise store the Recovery Key as it may be used to provide subsequent illicit access to the drive should the device fall into unauthorized hands. It is also not permissible for employees to disable cryptographic security controls in place on College-owned computers.

## Related Information

## History/Revision Information

**Responsible Division/Office:** Library and Information Services/User Services

**Effective Date:** 3/9/18

**Last Amended Date**: 3/7/18

**Next Review Date:** 6/5/22

**Also Found In:**