Messiah College Data Security Policy

I. Purpose

This policy identifies data security, retention requirements and responsibilities for proper management of College data and compliance with retention requirements, and defines penalties for violations.

II. Definitions

The following are definitions for terms used within the context of this policy:

1. Data – any records or files in either electronic or printed format.
2. Email – any transmission utilizing a College mail server or server that is provided by an external entity to the College for the purpose of electronic correspondence.
3. User – any individual who utilizes any of the College's computer devices, computer networks or data in paper format.

III. Data Classifications

Data should be classified in the following categories:

1. **Public**
   Defined as data, paper or electronic, that may or must be open to the general public. The disclosure, use or destruction of public data will have no adverse effects on the College nor carry any liability.

   Some examples of public data:
   a. College maps
   b. College newsletters
   c. College news

2. **Private**
   Defined as data that is not required to be publicly disclosed. It includes information that the College is under legal or contractual obligation to protect. Private data may only be copied and distributed by authorized users within the College to authorized users. Distribution to external users may require a signed Confidential Information Addendum (found on the ITS Channel in MCSquare).

   Some examples of private data:
   a. Employment candidate and search information
   b. Prospective student information
   c. Donors to the College

3. **Confidential**
   Defined as data that by law is not to be publicly disclosed. The recipients of confidential data have an obligation not to reveal the contents to any individual unless that person has authorized permission from the appropriate authority to access the data, and the person revealing such confidential data has specific authority to do so.

   Some examples of confidential data:
   a. Social security numbers
   b. Personally identifiable student/employee information
   c. Data of students who have requested privacy under FERPA

IV. Scope

This policy applies to all data, regardless of whether they are maintained in hard (paper) copy, electronically, or in some other fashion (including, but not limited to campus voicemail). All employees should be knowledgeable of the applicable Records Retention and Data Destruction Schedule. Employees who acquire data outside of their own office/department should make a reasonable effort to be knowledgeable of the retention and destruction procedure for that data. The Records Retention and Data Destruction Schedule will be required to be updated annually (Fiscal Year).

V. Policy

A. Background

The College is committed to the retention of its data in order to meet legal requirements, optimize use of space, minimize cost, and preserve the history of the College. The College is subject to a range of federal, state and local regulations regarding data retention and is required to maintain records accordingly. Each department should develop a data management plan appropriate for the particular data it maintains in cooperation with Human Resources (employee data), the Registrar's Office (student educational data), Student Affairs (student non-education data) and the Business Office (all financial and transactional data).

B. Retention and Maintenance of Data

The College requires that its data be maintained in a consistent and logical manner and be managed so that the College:

1. Meets legal standards for protection, storage and retrieval;
2. Protects the privacy of all Messiah entities as required by law;
3. Optimizes the use of storage space (physical or virtual);
4. Minimizes the cost of data retention; and
5. Destroys data as outlined in the Record Retention and Data Destruction (RRDD) schedule in an appropriate manner.

C. Ownership

All College data are the property of Messiah College regardless of their physical location, and as such, may not be permanently removed from the College nor destroyed except in accordance with the College's Records Retention and Data Destruction Schedule. All College data shall be maintained in a medium owned or controlled by the College. Offices/Departments that maintain College data are responsible for establishing appropriate data management procedures and practices. Each Provost/VP must do the following or delegate these tasks to an appropriate designee:

1. Be familiar with, and reference, the College's Records Retention and Data Destruction Schedule to determine:
   a. the length of time a particular class of data must be maintained.
   b. the final disposition of a data.
2. Be familiar with, and reference, specific office/department data management procedures and practices.
3. Educate employees within the specific office/department in understanding sound data management practices.

4. Control access to data to ensure its integrity.
5. Coordinate the destruction of data as provided in the Records Retention and Data Destruction Schedule.

D. Confidentiality Requirement

All confidential and private data are subject to the Records Retention and Data Destruction Schedule. Such data are protected by federal, state and local statutes, including the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley (GLB) Act, and the Health Insurance Portability and Accountability Act (HIPAA) and other regulations as applicable. In addition to statutory requirements, any data that contain anything confidential should be treated in accordance with the College's privacy and security policies.

E. Preservation of Data Relevant to Legal Matters

Any data that is relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation or enforcement action shall be retained at least until final resolution of the matter. In these circumstances, Human Resources will notify relevant departments and work with employees to identify and preserve any data that could be relevant to the matter. This will include a directive that the relevant unit's normal record retention policies or protocols temporarily be suspended. Employees who become aware that an investigation or legal proceeding has commenced against their department or unit must promptly notify Human Resources so that all data with potential relevance to the investigation or legal proceeding can be preserved as necessary.

F. Data Protection

The College expects all employees and all vendors to use the following methods to protect the College's data assets.

1. Paper Data
   a. Lock the door where the confidential or private data are located (if available), whenever room is unoccupied.
   b. Do not leave printed copies of confidential/private data in plain sight on desks or shelves.
   c. Close and lock filing cabinets containing confidential/private data when not in use.
   d. Lock doors in rooms that contain filing cabinets or document storage areas whenever room is unoccupied.
2. Electronic Data
   a. Lock or log off the Computer workstation whenever leaving a workstation or if individuals who do not have authorized access to confidential information can see your screen.
   b. ITS will identify mechanisms that can be used to encrypt data. All employees who handle confidential/private data are required to use prescribed encryption methods to protect the College's data. Areas of concern include:
   c. Any private or confidential data downloaded or exported to a College-owned computer from College systems must be encrypted.
   d. Any private or confidential data transported off campus (e.g., Flash Drive, CD, External Hard Drive, etc.) must be encrypted.
   e. Confidential or private College data can only be stored on a College-owned system or a system contracted by ITS.
3. Data Access
   All wireless data communication devices (e.g., personal computers, cellular phones, PDA's, etc.)

connected to any of Messiah College's internal networks, including any form of wireless communication device capable of transmitting packet data, must conform to the following:

a. Approved Technology
All wireless LAN access must use ITS-approved vendor products and security configurations. Non-ITS approved access points are not allowed to be installed unless an exception is granted by ITS.

b. Encryption and Authentication
ITS requires authentication to all campus wireless networks and strongly suggests encryption. Only limited network resources are granted to devices that are not encrypted.

4. Account Lockout
There are two primary ways a user account will be locked:

a. If a user enters an incorrect password five (5) consecutive times when attempting to log on to the Messiah network.

b. If a user has not changed their password in six (6) months. This lockout will stay active until the user changes their password.

5. Session Timeout
After a specified duration of inactivity the computer will automatically timeout to a login screen; the user can either login with their password proceeding to where they left off, or logout of the computer entirely.

G. Email Retention

1. Background
This section highlights specific security and retention matters that are directly applicable to email. The College maintains the right to monitor, delete, archive, move and/or access all email on the College's email system for legitimate business reasons, including monitoring employee performance, compliance with any applicable laws and industry regulations, and where there is reasonable suspicion of activities that may violate this or other College policies.

2. Retention Length
All items originated or received by or through the use of College email systems will be automatically deleted from the email system and the central email archive 3 years after the creation date.

3. Email Archiving
For both legal and resource reasons the College strongly recommends users do not maintain any items originated or received by, or through the use of, the College email system on any medium other than the campus email system. Any user maintaining email data external to a campus email system will personally be held liable if it is maintained beyond the Record Retention and Data Destruction Schedule and is required to provide the contents if requested by the College or an outside entity in a legal proceeding (e.g., in a discovery procedure).

VI. Enforcement

The College may take such action as may be necessary in its discretion to address any violation(s) under this policy, including suspension or termination of a user's network account, and up to and including termination of employment or dismissal from the College. ITS may temporarily suspend or block access to an account when determined necessary to protect the integrity, security, or privacy of data, or to protect the College from liability. In addition, Messiah College reserves the right to limit or restrict the use of its computing and electronic communication resources when there is evidence of a violation of applicable College policies, contractual agreements, or federal, state or local laws. The College may refer suspected violations of applicable laws to the appropriate law enforcement agencies.