Kentucky Wesleyan College provides electronic resources to support its educational mission and administrative support of that mission. To ensure these resources are used appropriately, Kentucky Wesleyan has established the following policies and guidelines.

Table of Contents

Revised 11/19/16

Section 1

Policy Development Process

The KWC Software Review Policy defines the responsibilities of the CAMS Governance Committee to be an oversight agent for the College's primary data source: CAMS Enterprise. Since the vast majority of the College's data resources must interface with the CAMS system, the committee is also charged with the task of assigning priorities for technology use and developing plans to meet future technology needs. This committee provides input into budgetary decisions by establishing priorities for the purchase of hardware and software from general operating resources and the Student Technology Fee. The committee also evaluates the adequacy of technology services on a regular basis, seeking information from administrative offices, academic departments and students.

To facilitate fulfillment of its charge, the CAMS Governance Committee has developed or assisted development of the policies and guidelines contained in this handbook. The Handbook is intended to be a dynamic, "living" document. Consequently, the Committee will review the policies and guidelines regularly (See Appendix A: "Policy Review Schedule"). Assessment procedures include 1) collecting data relative to the use of information technology resources (network log files, web server statistics, etc.); 2) a student user survey taken every three years in conjunction with the library user survey; and 3) a faculty/staff user survey, also taken every three years.

Revised 11/19/16

Section 2

Definitions

2.1 Authorized Use

Authorized use of Kentucky Wesleyan College-owned or operated computer and network resources is used consistent with the mission of the college and these policies.

2.2 Authorized Users

Authorized users are defined as current faculty, staff and students of Kentucky Wesleyan College.

2.3 CAMS Governance Committee

The Kentucky Wesleyan College CAMS Governance Committee is charged with the oversight of the College's ERP system and is also charged with the task of assigning priorities for technology use and developing plans to meet future technology needs.

Membership

- Senior Director of Information Services and Resources
- Director of Information Technology Services
- Database Administrator
- Technology Support Director
- CETL Director
- Registrar
- Data Managers from the following units: Admissions, Athletics, Financial Aid, Development, Business Office, Student Success Center

2.4 Information Technology Services Staff

The Kentucky Wesleyan College Information Technology Services Staff consists of the Director of Information Technology Services, the Technology Support Director and the Database Administrator.

Revised 11/19/16

Section 3

INFORMATION TECHNOLOGY APPROPRIATE USE

This policy establishes guidelines for the appropriate use of computer equipment, software and networks owned or operated by Kentucky Wesleyan College. Access to the College's information systems is granted to KWC students, faculty and staff with the stipulation that they follow these guidelines and abide by local, state and federal laws.

> "Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

— *The EDUCOM Code*

3.1 Background and Purpose

This document constitutes a college-wide policy for the appropriate use of all Kentucky Wesleyan computing and network resources. It is intended to provide effective protection of individual users, equitable access, and proper management of those resources. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to those resources.

Access to Kentucky Wesleyan networks and computer systems is granted subject to College policies and local, state, and federal laws. Appropriate use should always be legal and ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy, freedom of speech, and freedom from intimidation, harassment, and unwarranted annoyance. The College is not responsible for unacceptable or unethical use of the information technology environment including computer and computer networks or electronic communication system.

3.2 Appropriate Use

Appropriate use of information technology resources includes instruction; independent study; authorized research; independent research; and official work of the offices, units, recognized student and campus organizations, and agencies of the College.

Authorized use of Kentucky Wesleyan-owned or operated computing and network resources is consistent with the mission of the College, and consistent with this policy.

Authorized users are: Kentucky Wesleyan faculty, staff, and students.

In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Acceptable conduct in and use of this environment must conform with: existing College policies, guidelines, and codes of conduct; Kentucky Wesleyan's Web, Email, Intellectual Property and Information Resource Policies; and existing local, state and federal laws.

It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to continuously verify the integrity and completeness of information that you compile or use. You are

responsible for the security and integrity of College information stored on your individual computing desktop system.

In making appropriate use of information resources you **MUST**:

1. Protect your userID from unauthorized use. You are responsible for all activities initiated under your userID.
2. Access only files and data that are your own, that are publicly available, or to which you have been given authorized access.
3. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting printer paper and other supplies.
4. Use the FACULTY, STAFF and/or STUDENT e-mail groups to communicate only college-related information, including notices about events, activities, sports competitions and general business/ academic information.

In making appropriate use of information resources you **MUST NOT**:

1. Use another person's files or data without permission.
2. Use computer programs to decode passwords or access control information.
3. Load software or data on the hard drive of any public access workstation.
4. Engage in any activity that might be harmful to systems or to any information stored therein, such as creating or propagating viruses, disrupting services, or damaging files.
5. Make or use illegal copies of copyrighted software or computer files (including music and video files), store such copies on College systems, or transmit them over College networks.
6. Use mail or message services to harass, intimidate, or otherwise annoy another person.
7. Use any e-mail group to distribute chain letters.
8. Use the FACULTY, STAFF and/or STUDENT e-mail groups for socializing, personal comments, etc. NOTE: Individual addresses should be used for personal messages and communications.
9. Use another person's userID and password.
10. Place on any College-owned or operated system information or software which
    a. infringes upon the rights of another person;
    b. is abusive, profane, or obscene; or
    c. promotes a commercial enterprise or product.

3.3 Confidentiality and Privacy

Authorized access to data or information entails both privilege and responsibility, not only for the user, but also for the system administrator. In general, the College will treat information stored on computers as confidential. However, there is no expectation of privacy or confidentiality for documents and messages stored on College-owned equipment. Additionally, email and data stored on Kentucky Wesleyan's network of computers may be accessed by the College for the following purposes:

- Troubleshooting hardware and software problems.
- Preventing unauthorized access and system misuse.
- Retrieving business related information.
- Investigating reports of violation of this policy or local, state or federal law.
- Complying with legal requests for information.

Rerouting or disposing of undeliverable mail.

To the greatest extent possible in a public setting, individuals' privacy should be preserved. However, privacy or confidentiality of documents and messages stored on College-owned equipment cannot be guaranteed. Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties.

3.4 Enforcement

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges without notification, disciplinary action, dismissal from the College, and legal action. Some violations may constitute criminal offenses, as outlined in Kentucky statutes and other local, state, and federal laws; the College will carry out its responsibility to report such violations to the appropriate authorities.

Unit heads have the authority to deny access, for unauthorized use, to Kentucky Wesleyan's computers and network systems under their control.

Revised 11/19/16

Section 4

Abuse of Information Technology Privileges

Users found in violation of Kentucky Wesleyan College's Information Technology Appropriate Use Policy are subject to a range of sanctions, including disciplinary action consistent with College policy and possible legal action.

4.1 Student violation of policy

The College considers any violation of the Appropriate Use Policy to be a serious offense and reserves the right to examine files allegedly related to inappropriate use. Violators are subject to immediate loss of e-mail and/or network access privileges and possible disciplinary action.

4.2 Faculty/Staff violation of policy

Violations by faculty and staff will be reported to the appropriate administrative officer who will document and take appropriate action to resolve the violation.

Revised 11/19/16

Section 5

Allocation of Resources

5.1 Fiscal Responsibility

5.1.1 Network Hardware/Software

Information Technology Services has planning/budgetary responsibility for the purchase and maintenance of network cabling, hardware (servers, hubs, switches, routers, etc.) and general use software. IT Services provides input into budgetary decisions by establishing priorities for requisition of this hardware and software.

5.1.2 Public Use Computers and Peripherals

Each semester students enrolled at Kentucky Wesleyan College are assessed a technology fee. The proceeds from this fee are restricted to the support of student and general instructional technology needs. IT Services has responsibility for establishing priorities for expending technology fee proceeds. Computers and peripherals in the student/instructional labs are acquired and maintained with these funds.

5.1.3 Departmental Hardware/Software

Each academic department and administrative unit has planning/budgetary responsibility for the purchase and maintenance of hardware and specialized software used exclusively in its area. Purchases must be made in accordance with the Section 5.2 of this policy (see below).

5.2 Hardware/Software Acquisition

Only equipment meeting system compliance requirements will be connected to the Kentucky Wesleyan College campus network.

5.2.1 Preferred Vendors

To ensure the system compatibility of hardware and software and to provide an optimum level of staff support, the College maintains purchasing and service agreements with selected computer vendors. Academic departments and administrative units purchasing computers with institutional funds must do so from these vendors through the Kentucky Wesleyan College Information Technology

Services Department. Departments and units must also consult Information Technology Services before purchasing specialized software if the software is to be networked. Faculty should consult Kentucky Wesleyan's Director of Information Technology and Software Information Coordinator for assistance in determining the best hardware and software solutions to meet their instructional needs. All computer hardware and software purchased with institutional funds will be inventoried according to College procedures.

5.2.2 Software Approval

To ensure the system compatibility of hardware and software and to provide an optimum level of staff support, any software acquisition or utilization, whether installed on college servers, computers, or accessed via the World Wide Web and whether purchased or free, must meet the requirements established in the College's Software Review Policy.

Revised 11/19/16

Section 6

Copyright and Licensure

6.1 Use of Copyrighted Information

The use of computers or network systems in no way exempts any member of the College community from the normal requirements of ethical or legal behavior. In particular, data, software, and computer capacity have value and must be treated accordingly. Copying, downloading, storing, displaying, or distributing copyrighted material using any College owned or operated system or network without the express permission of the copyright owner, except as otherwise allowed under the copyright law, is prohibited. Under the Federal Digital Millennium Copyright Act of 1998, repeat infringements of copyright by a user can result in termination of the user's access to College systems and networks, and further prosecution as is warranted by state and Federal Laws and the Federal Digital Millennium Copyright Act of 1998.

6.1.1 Procedures

The distribution of copyrighted materials over the Internet for which the distributor (any server — including your computer) does not have permission can be violation of federal criminal law, the Digital Millennium Copyright Act of 1998 ("DMCA"). All network traffic is subject to monitoring procedures conducted by Information Technology Services for purposes of determining compliance with College policies. Outside parties also actively monitor the internet to find incidents of illegal file sharing and may notify the College of such activity. When such a notification is provided by an outside source, the College may disable a person's network access until the situation is resolved.

6.1.2 Violations

Violations of these policies may result in the immediate suspension of computer account and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate College or outside authorities. Unauthorized use of Kentucky Wesleyan computing facilities can be a criminal offense.

6.2 Use of Licensed Software

6.2.1 Purpose

To ensure Kentucky Wesleyan College is in compliance with all applicable state and federal laws regarding the installation and use of computer software.
To ensure that Kentucky Wesleyan's computer users are aware that all proprietary computer software is protected by Federal copyright laws. If it is explicitly labeled as **Freeware**, **Free Software**, **Open Source**, **Public Domain** or **Free for Educational Use**, less stringent rules may apply.
To prevent the installation of illegal or unlicensed copies of software on any Kentucky Wesleyan owned or operated computer systems.

6.2.2 Policy

All software installed or run on Kentucky Wesleyan equipment must be licensed with a proof of purchase available for audit verification.

6.2.3 Background

The proper licensing of software is both a legal requirement and an ethical imperative. Industry watchdog organizations regularly survey organizations for software license compliance and can assess substantial penalties for noncompliance.
Kentucky Wesleyan purchases and licenses the use of computer software from a variety of outside companies and, unless authorized by the software developer, does not have the right to reproduce it except for backup purposes. Unless the College purchased a site license, a separate license must be purchased for each computer on which a software product is installed.
According to applicable copyright law, persons involved in the installation and operation of unlicensed software can be subject to civil damages and criminal penalties including fines and imprisonment. Kentucky Wesleyan College does not condone the illegal duplication, installation, or operation of software.

6.2.4 Definitions

Freeware: software for which a license is provided without charge. Distribution is permitted but it cannot be modified and the source code is not available. Frequently the license is provided to select groups (home users, educational users, etc.) although some freeware is available to anyone. Free software, as compared with "freeware", is a matter of the user's freedom to run, copy, distribute, study, change and improve and not necessarily tied to the cost of the software.
Free Software: refers to software distributed in source form, which can be freely modified and redistributed. It does not refer to zero-cost software.

Open source: refers to the fact that the source code of "Free software" is open to and for the world to take, modify and reuse. The distribution terms for "Open Source" are more stringent than for "Free Software".
Public Domain software: software that is not copyrighted.
Shareware: software for which a temporary license is provided without charge to use for evaluating the software. Virtually all such temporary licenses expire after a fixed period of time after which a standard license must be purchased.
Freeware, Free Software, and Public Domain Software should not be used above a department level application. Generally, this software does not provide for protection against developer participants coming back and suing for damages for the use of their software code without consent.

6.2.5 Compliance

Each KWC department head is responsible for assuring that the software running on all computers operated or managed by department employees is appropriately licensed. College employees must not install, upload, download, or use any unlicensed software. Properly obtained and licensed demo and personal software may be installed by the employee at the discretion of the department head with the understanding that Information Technology will only support standard College academic and administrative software. Kentucky Wesleyan employees who make, acquire, or use unlicensed copies of computer software are subject to disciplinary action. Upgrades, service packs and or hot fixes will be coordinated through Information Technology.

6.2.6 Procedures

Each Kentucky Wesleyan employee who believes that unlicensed software is installed on equipment that they use is responsible for advising their department head of that circumstance. Each department head that has reason to believe that unlicensed software is installed on any equipment operated or managed by their department employees should either immediately purchase appropriate licenses, remove the software immediately, or consult with Information Technology to resolve the problem. Information Technology's Help Desk (ext. 3268) can provide assistance in removing unlicensed software from desktop computers or servers. Information Technology can only perform software inventories on computers that are regularly connected to the network and meet university standards. Departments that choose to use non-standard equipment or below-standard windows computers, will need to inventory their own equipment and provide separate assurance of compliance. Departments will also need to inventory software on all computers not regularly connected to the network including standalone PCs, laptops and notebooks, handheld computers (PDAs), and College equipment installed at off-site locations including homes.

Users must not install, copy, or use software subject to licensing until that software is properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) have been met.

Revised 11/19/16

Section 7

Security

The availability of information technology resources brings with it the responsibility to protect those resources from unauthorized access and use. Kentucky Wesleyan College has instituted security measures designed to protect the integrity of its systems and data. Any attempt to circumvent these procedures will be considered a violation of College policies and/or state and federal statutes.

7.1 Gramm-Leach-Bliley Act Compliance Plan

7.1.1 Purpose

This compliance plan ("Plan") describes Kentucky Wesleyan College's safeguards to protect non-public, financial-related personal information ("covered information") in accordance with the requirements of the Gramm-Leach-Bliley Act of 1999 (GLBA). The Safeguards Rule of the GLBA, as defined by the Federal Trade Commission (FTC), requires financial institutions, which the FTC explicitly indicates includes higher education institutions, to have an information security program to protect the confidentiality and integrity of personal information.

These safeguards are provided to:

a. Ensure the security and confidentiality of covered information.
b. Protect against anticipated threats or hazards to the security or integrity of such information.
c. Protect against unauthorized access to or use of covered information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

a. Designate an employee or employees to coordinate the information security program.
b. Identify and assess the internal and external risks that may threaten covered information maintained by Kentucky Wesleyan.
c. Design and implement safeguards to control the identified risks.
d. Oversee service providers, including third party contractors, to ensure appropriate safeguards for covered information are maintained.
e. Periodically evaluate and adjust the information security program as circumstances change.

7.1.2 Scope

This policy applies to all Kentucky Wesleyan departments, administrative units, affiliated organizations and third party contractors that create, access, store or manage covered information.

7.1.3 Policy

The College will develop, implement and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards to protect covered information.

7.1.4 Definitions

Covered Information: Information that Kentucky Wesleyan has obtained from a customer (e.g., a student) in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Information Security Program: The administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered information.

Service Providers: Any person or organization that receives, maintains, processes, or otherwise is permitted access to covered information through its direct provision of services to the College.

7.1.5 Roles and Responsibilities

Chief Information Officer (CIO): The CIO is responsible for coordinating and overseeing all elements of Kentucky Wesleyan's information security program. The CIO will work with appropriate personnel from other offices as needed (such as the Registrar's Office, Internal Audit, and Financial Aid) to ensure protection of covered information.

7.1.6 Information Security Program Elements

A. **Risk Assessment**

Under the oversight of the CIO, risk and privacy assessments are performed for all information systems that house or access covered information. These risk and privacy assessments shall address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

Internal and external risks at Kentucky Wesleyan include, but are not limited to:

1. Unauthorized access of covered information by persons within or outside the College
2. Compromised system security as a result of human error, vulnerabilities, infection by malicious software, or unauthorized system access
3. Interception of data during transmission
4. Loss of data integrity
5. Physical loss of data in a disaster
6. Errors introduced into the system
7. Corruption of data or systems
8. Unauthorized access through hardcopy files or reports
9. Unauthorized disclosure of covered information through third parties

Risk and privacy assessments are used to determine the likelihood and magnitude of harm that could come to an information system, the affected individual(s), and ultimately the College itself in the event of a security breach. By determining the amount of risk that exists, the College shall determine how much of the risk should be mitigated and what controls should be used to achieve that mitigation.

Both risk and privacy assessments shall be performed prior to, or if not practical, immediately after acquisition of an information system (in the event that the information system is owned/operated by the College) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of the College). Further, the risk and privacy assessments shall be reviewed and, where required, updated after three years or whenever a significant change is made to the information system, whichever comes first.

Risk assessment should include consideration of risks in each of the following operational areas, in accordance with the requirements of the GLBA:

Employee training and management

Prior to being granted access to covered information, new employees in positions that require access to covered information (e.g., the Business Office, Admissions,

Development, Registrar, and Financial Aid) will receive training on the importance of confidentiality of student records, student financial information, and other types of covered information, and the risks of not providing appropriate protection. Furthermore, all employees receive annual training in general information technology security. Training also covers controls and procedures to prevent employees from providing confidential information to an unauthorized individual through social engineering or improper disposal of documents that contain covered information. All training will be reviewed and, where needed, updated at least annually.

Each department responsible for maintaining covered information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

B. **Designing and Implementing Safeguards**

Safeguards are necessary to mitigate and control the risks identified through risk assessment. Furthermore, the effectiveness of safeguards' key controls, systems, and procedures should be regularly tested to ensure continued protection of covered information. The policy framework for Kentucky Wesleyan's information security program that governs the design, implementation, and maintenance of these safeguards is provided in sections 7.2 through 7.6

C. **Overseeing Service Providers**

In the process of choosing a service provider that will maintain or regularly access covered information, the selection and retention processes shall ensure the ability of the service provider to implement and maintain appropriate safeguards for covered information. Contracts with service providers may include the following provisions:

1. An explicit acknowledgment that the contract allows the contract partner access to covered information.
2. A specific definition or description of the covered information being provided.
3. A stipulation that the covered information will be held in strict confidence and accessed only for the explicit business purpose of the contract.
4. An assurance that the contract partner will protect the covered information it receives according to commercially acceptable standards and no less rigorously than it protects its own covered information.
5. A provision providing for the return or destruction of all covered information received by the contract provider upon completion or termination of the contract.
6. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles Kentucky Wesleyan College the right to terminate the contract without penalty.
7. A provision ensuring that the contract's confidentiality requirements shall survive any termination of the agreement.

D. **Program Evaluation and Adjustment**

The CIO will periodically review and adjust the information security program as it relates to the GLBA requirements, with input from the Campus Technology Committee and relevant stakeholders. Program evaluation should be based on results of testing and monitoring of security safeguard effectiveness and reflect changes in technology and/or operations, evolving internal and external threats, and any other circumstances that have a material impact on the information security program.

7.2 Operations and Management Security

7.2.1 Purpose

The purpose of this policy is to help ensure the secure operation of Kentucky Wesleyan information systems and proper management of Kentucky Wesleyan's IT security program and technologies.

7.2.2 Scope

This policy applies to all departments, administrative units, and affiliated organizations that use College information technology resources to create, access, store or manage College data to perform their business functions.

7.2.3 Policy

Business continuity plan – Kentucky Wesleyan must have a business continuity plan to guide recovery from disasters or other major disruptions to service in a manner that maintains the security of the College's information systems and ensures timely restoration of services.

Configuration management - the configuration of servers, workstations, network devices, firewalls and other enterprise security technologies should be managed in a way that provides consistent setup, documents changes, and ensures security requirements are maintained when the configuration is changed.

Data backups - College data must be backed up regularly and backup media stored securely, commensurate with the classification of the data.

Firewalls - All connections to networks outside the Kentucky Wesleyan campus, such as the Internet, must be protected with a firewall that filters both incoming and outgoing network traffic against common threats. All enterprise information systems and any Kentucky Wesleyan system hosting confidential data must be protected by a network firewall and a host-based software firewall, both configured in "default deny" mode for incoming traffic and enforcing documented trust

relationships for those systems. All College computers connected to the College network must have a host-based firewall configured appropriately for the security requirements of the system and the classification of data stored therein. Logging should be enabled for all firewalls and periodically reviewed for anomalous events. Configuration of network firewalls and host-based firewalls on enterprise information systems should be audited periodically to ensure consistency with the security requirements of the system(s) they protect.

7.2.4 Definitions

Authentication: Process of verifying one's digital identity.

Confidential data: Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

Default Deny: A firewall ruleset that begins with blocking all network traffic, both incoming and outgoing, then only allowing specific network traffic required for the effective and secure operation of the system(s) protected by the firewall.

Enterprise information system: An information system and/or server providing services commonly needed by the College community and typically provided by ITS.

Firewall: A specialized device or software program that controls the flow of network traffic between networks or hosts to enforce security policies and provide protection for the resources on those networks or hosts. For the purposes of this policy, a router with Access Control Lists (ACLs) is not considered a firewall.

Trust relationships: A specification of the level of access granted to computer systems and/or applications that are trusted to access resources on a server and its associated data and applications. This applies to access controls between systems, not access rights for individual users or roles.

College Computer: Any computer considered to be the property of Kentucky Wesleyan College.

College Data: Any data related to Kentucky Wesleyan College ("College") functions that are:

a. Stored on College information technology systems.
b. Maintained by Kentucky Wesleyan faculty staff, or students.
c. Related to institutional processes on or off campus.

This applies to any format or media.

College Network

Any part of Kentucky Wesleyan's data network physically located on campus.

7.3 System Development and Maintenance Security

7.3.1 Purpose

The purpose of this policy is to define requirements for system security planning and management to improve protection of Kentucky Wesleyan's information system resources. Security has to be considered at all stages of the life cycle of an information system (i.e., feasibility, planning, development, implementation, maintenance, and retirement) in order to:

a. ensure conformance with all appropriate security requirements
b. protect sensitive information throughout its life cycle
c. facilitate efficient implementation of security controls
d. prevent the introduction of new risks when the system is modified
e. ensure proper removal of data when the system is retired

This policy provides guidance to ensure that systems security is considered during the development and maintenance stages of an information system's life cycle.

7.3.2 Scope

This policy applies to all departments, administrative units, and affiliated organizations that use College information technology resources to create, access, store or manage College data to perform their business functions. The requirements apply to enterprise information systems or systems that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein.

7.3.3 Policy

Appropriate security controls should be considered at all stages of an information system life cycle, including the development and maintenance stages.

System security plans and documentation - System security plans and documentation must be prepared for all enterprise information systems or other systems under development that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein. Such plans should provide an overview of the security requirements of the system and describe the controls in place, or planned, for meeting those requirements through all stages of the system's life cycle. When

the system is modified in a manner that affects security, system documentation must be updated accordingly.

Separate development, testing, and production environments - System development, testing, and production should be performed in separate environments.

Test data - Testing of enterprise information systems should be conducted with fabricated data that mimics the characteristics of the real data, or on copies of real data with any confidential data appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or confidential data must have appropriate security controls employed.

Vulnerability management - An assessment of the system's security controls and a vulnerability assessment that seeks to identify weaknesses that may be exploited must be performed on all new enterprise information systems or ones undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production enterprise information systems and appropriate measures taken to address the risk associated with identified vulnerabilities. Vulnerability notifications from vendors and other appropriate sources should be monitored and assessed for all systems and applications associated with enterprise information system.

Vendor acquisitions - If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system.

7.3.4 Definitions

Confidential data: Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

Enterprise information system: An information system and/or server providing services commonly needed by the College community and typically provided by ITS.

Live data: Data accessible to users through systems that are in production (i.e., live).

College Data: Any data related to Kentucky Wesleyan College ("College") functions that are:

a. stored on College information technology systems
b. maintained by Kentucky Wesleyan faculty staff, or students
c. related to institutional processes on or off campus

This applies to any format or media.

7.4 Physical and Environmental Security

7.4.1 Purpose

This policy defines the requirements for protecting College information and technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference with Kentucky Wesleyan operations.

7.4.2 Scope

This policy applies to all departments, administrative units, and affiliated organizations that use College information technology resources to create, access, store or manage College data to perform their business functions.

7.4.3 Policy

All College information and technology resources should have appropriate physical and environmental security controls applied commensurate with identified risks.

7.4.4 Definitions

Core network facilities: The cabling, equipment, and network/telecommunications rooms associated with the high speed backbone of Kentucky Wesleyan's campus network that carries aggregated network traffic for all the buildings and external network connections.

Mobile storage devices: Any easily movable device that stores College data, including but not limited to laptop computers, smartphones, external hard drives, and USB flash drives.

Uninterruptable Power Supply (UPS): A device designed to provide power, without delay, during any period when the normal power supply is incapable of performing acceptably.

College Data: Any data related to Kentucky Wesleyan College ("College") functions that are a) stored on College information technology systems, b) maintained by Kentucky Wesleyan faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media and is not limited to electronic data.

7.4.5 Roles and Responsibilities

Responsibility for physical and environmental security of Kentucky Wesleyan information and technology resources is shared by the individuals using these systems, units that own them, and system administrators responsible for managing the systems.

7.4.6 Implementing Procedures

Physical Security

a. **Network wiring and equipment** – Network wiring and equipment rooms and cabinets must be locked when unattended with access limited to authorized personnel (typically network support staff) and visitors escorted by said authorized personnel. Other network cabling and devices should likewise be physically secured where feasible.
b. **Office doors** – All office doors should remain locked after hours or when offices are unattended for a prolonged period of time.
c. **Mobile storage devices** – Mobile storage devices should be stored securely when unattended. Appropriate secure storage methods include a locking security cable attached directly to the device, storage in a locked cabinet or closet, storage in a locked private office, or the like. Encrypting data stored on mobile devices, such as whole disk encryption on laptop computers, likewise reduces the risk of a breach of College data resulting from theft, loss, or unauthorized access. When traveling with mobile storage devices or using them in public places, appropriate security precautions should be taken to prevent loss, theft, damage, or unauthorized access. Use of tracking and recovery software on laptop computers is encouraged.

Environmental Security

a. **Electrical power** – Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Each UPS should have sufficient capacity to provide at least 30 minutes of uptime to the systems connected to it. Systems hosting confidential data should also be protected with a standby power generator where feasible.

7.5 Access Controls Security

7.5.1 Purpose

Access controls are the rules that an organization applies in order to control access to its information assets. The risks of using inadequate access controls range from inconvenience to critical loss or corruption of data. This policy defines

access control standards for system use notices, remote access, and definition and documentation of trust relationships for Kentucky Wesleyan information systems.

7.5.2 Scope

This policy applies to all departments, administrative units, and affiliated organizations that use College information technology resources to create, access, store or manage College data to perform their business functions.

7.5.3 Policy

Access control standards for Kentucky Wesleyan information systems are to be established in a manner that carefully balances restrictions that prevent unauthorized access to information and services against the need for unhindered access for authorized users.

System use notice - Before a user gains access to a Kentucky Wesleyan computer, a general system use notice must be displayed that welcomes users and identifies it as a Kentucky Wesleyan system, warns against unauthorized use of the computer, and indicates that use of the system implies consent to all relevant Kentucky Wesleyan policies. The general system use notice should also be displayed before a user gains access to a Kentucky Wesleyan information system, where practical. The system use notice must state the following:

Welcome to Kentucky Wesleyan College's information technology resources. Access to this system and all other electronic resources at Kentucky Wesleyan is restricted to employees, students, or individuals authorized by the College or its affiliates. Use of this system constitutes agreement to abide by all relevant Kentucky Wesleyan policies. Unauthorized or inappropriate use may result in limitation or revocation of use privileges and/or administrative, civil, or criminal penalties.

Remote access - Remote access control procedures must provide appropriate safeguards through appropriate identification, authentication, and encryption techniques. Direct log-on to campus computers from off-campus locations is not allowed. A remote user must first authenticate to an authorized campus remote access service with strong encryption, such as Kentucky Wesleyan's Virtual Private Network (VPN) service or a departmental Windows Terminal Services (i.e. Remote Desktop Services) before logging into a campus computer. This restriction does not apply to authenticated user access to web applications like Brightspace, CAMS Portals, Webmail, or to systems designed for public access.

Trust relationships - Trust relationships for centrally-managed College information systems or any system with confidential data must be defined and documented, approved by an appropriate authority, and periodically reviewed and revised as needed. Security controls, such as firewall rulesets, must be configured to enforce the trust relationships.

7.5.4 Definitions

Authentication: Process of verifying one's digital identity.

Confidential Data: Highly sensitive College data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

Kentucky Wesleyan Computer: Any computer considered to be the property of Kentucky Wesleyan College.

Local Network: Any segment of Kentucky Wesleyan's data network physically located on campus.

Remote Access: Accessing a Kentucky Wesleyan local network from any physical location outside the campus. This includes access from off campus using Kentucky Wesleyan's Virtual Private Network (VPN) service.

Trust relationships: A specification of the level of access granted to computer systems and/or applications that are trusted to access resources on a server and its associated data and applications. This applies to access controls between systems, not access rights for individual users or roles.

College Data: Any data related to Kentucky Wesleyan College ("College") functions that are:

a. Stored on College information technology systems.
b. Maintained by Kentucky Wesleyan faculty, staff, or students.
c. Related to institutional processes on or off campus.

This applies to any format or media.

Virtual Private Network (VPN): Provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

7.5.5 Implementation Procedures

The System Use Notice should be passively displayed such that no user action is required to view it before logging into the Kentucky Wesleyan computer or information system.

7.6 Security for Information, Computing and Network Resources

7.6.1 Purpose

To establish and maintain security requirements necessary to protect College information, computing and network resources, and minimize susceptibility to

attacks on Kentucky Wesleyan resources or from Kentucky Wesleyan locations against other sites.

7.6.2 Scope

This procedure and accompanying requirements apply to all College locations and all system users at any location, including those faculty, students and staff using privately owned computers or systems to access College information, computing and network resources.

Security requirements shall be in place for the protection of the privacy of information, protection against unauthorized modification of information, protection of systems against the denial of service, and protection of systems against unauthorized access.

7.6.3 General Policy

College information, computing and network resources may be accessed or used only by individuals authorized by the College. The College encourages the use of computing and network resources and respects the privacy of users. However, the College may access information stored on the College's network of computers for the following purposes:

a. Troubleshooting hardware and software problems.
b. Preventing unauthorized access and system misuse.
c. Retrieving College business related information.
d. Investigating reports of violation of College policy or local, state or federal law.
e. Complying with legal requests for information.
f. Rerouting or disposing of undeliverable mail.
g. Addressing safety or security issues.

To the greatest extent possible in a public setting, individuals' privacy should be preserved. However, there is no expectation of privacy or confidentiality for documents and messages stored on College-owned equipment. College information technology staff access to information stored on the College’s network will be limited to what is reasonably necessary to acquire the information and/or resolve the issue.

7.6.4 Consequences for Noncompliance to Requirements

Systems that are found to pose a threat to the integrity of the information, computing and network resources may have their access to these resources suspended. The suspension of services will continue until the problem has been remedied and the system validated by Information Technology Services for operation within the Kentucky Wesleyan information, computing and network resources environment. The College reserves the right to invoke emergency

suspension of services without prior notification if the situation poses a serious threat to the information technology environment.

7.6.5 Requirements for Information, Computing and Network Security

The following system requirements represent the minimum standard that must be in place in order to establish and maintain security for College information, computing and network resources.

Initial Network Hook-up

Each system must be capable of passing a test for vulnerabilities to hacker attacks and relaying of unsolicited email prior to being attached to Kentucky Wesleyan's information, computing and network resources. System testing will be the responsibility of the Director of Information Technology.

Password Specification

a. **Password Policy:** All passwords on any system, whether owned by Kentucky Wesleyan or by an individual, directly connected to Kentucky Wesleyan's network must adhere to the following standards when technically possible. This includes devices connected to the campus network with a direct wired connection, wireless, remote access software (e.g., Windows Remote Desktop), use of a Virtual Private Network (VPN), and the like. This policy applies to all passwords – KWC UserID, system, user, database, application, etc. Any user that does not comply may have their network access blocked without prior notification. The password standards are maintained by the CIO or designee.

b. **Password Standards**

1. Passwords must have a minimum of 7 characters.
2. Passwords must contain characters from 3 of the 4 following categories:
   - Uppercase letters
   - Lowercase letters
   - Numbers
   - Special characters (e.g.: !,@,#,$,%,^,&,*, etc.) Be aware that if traveling outside the U.S. that some symbols, like the U.S. dollar sign, may not be available on international keyboards.
3. Passwords cannot be the same as the Kentucky Wesleyan KWC UserID and not easily guessed (e.g.: no variants of the Kentucky Wesleyan KWC UserID, dictionary words, family names, pet names, birthdates, etc.).
4. Most passwords must be changed every 180 days. Others may need to change more often, depending on access to secure information.

5. Passwords must be changed significantly and cannot repeat more frequently than every two years.
6. Passwords that are written down or stored electronically must not be accessible to anyone other than the owner and/or issuing authority.
7. The same password used to access Kentucky Wesleyan Systems (e.g., your KWC UserID password) must not be used for accounts or other forms of access to non-Kentucky Wesleyan systems or applications such as online shopping, banking, etc.
8. Passwords must not be shared unless explicitly permitted by the issuing authority. KWC UserID passwords must not be shared under any circumstances.
9. Anyone who believes their password has been compromised must immediately notify their department head, College IT support, or the IT Help Desk to evaluate possible risks.
10. Default passwords in vendor-supplied hardware or software must be changed during initial installation or setup.
11. The KWC UserID password must never be transmitted over the network in clear text (e.g., it must always be encrypted in transit). It is also strongly recommended that other types of passwords be encrypted in transit.

Unattended Computers

To protect against unauthorized access to data on computers left unattended, the following precautions are required:

a. Enable password protection on the screen saver for all College computers with the exception of special-purpose computers designed for public access, such as public computers in the library, or computer labs where locking is undesirable due to the risk of a user monopolizing a shared computer. The length of time before the password-protected screen saver comes on should be set to 5 minutes or less. For lab situations, it is recommended that computers be set to automatically logout after a maximum of 30 minutes of idle time.
b. Never leave your computer unattended and unprotected. Before leaving your computer, lock the display or log out in a manner that requires a password to gain access. If you leave your work area, ensure that egress doors are locked.

Protection from Malicious Software and Intrusions

Malicious software, or malware, comes in many forms - viruses, worms, Trojan horses, denial of service attacks, botnets, spyware, adware, spam relays, etc. All pose a security risk, some of which are a very serious threat to the confidentiality, integrity, or availability of Kentucky Wesleyan's information and technology resources. Appropriate precautions must be taken to protect Kentucky Wesleyan systems and information from compromise by malware. To that end, Kentucky Wesleyan may require the installation of essential security software on computers connected to the Kentucky Wesleyan campus network or accessing Kentucky Wesleyan information and technology resources. The following sections define specific requirements for antivirus, spyware/adware, personal firewalls, and email. Assuring the validity of malware protection software is the responsibility of each user, the department representative, and the CIO.

Virus Protection

a. Computers listed below must use College-approved antivirus software configured in a managed mode (managed mode allows a server to monitor and configure the antivirus protection on the client computer and push updates to the client on demand). If a College owned or managed computer is compromised and is not running an antivirus program, the computer will remain blocked until the system is rebuilt and an antivirus program is installed.

    1. Any College-owned computer.
    2. Student-owned computers in Kentucky Wesleyan residence halls.
    3. Users of Kentucky Wesleyan's Virtual Private Network (VPN).
    4. Users of Kentucky Wesleyan's wireless or wired network if it is a College-owned computer or one that belongs to a current Kentucky Wesleyan faculty, staff, or student.

b. All other computers accessing the Kentucky Wesleyan campus network or information technology resources must be running active, up-to-date virus protection software.
c. Virus definition files (e.g., the database in the antivirus software that identifies known malware) must be up-to-date with the most current version available from the vendor.
d. Comprehensive virus scans of all local hard drives must be performed at least weekly.

Spyware/Adware Protection

a. All computers connected to the campus network must run active spyware/adware protection software.

b. Spyware/adware definition/detection rules must be up-to-date with the most current version available from the vendor.
c. Scans of all local hard drives for spyware/adware must be performed at least weekly.

Personal Firewall Protection

a. All computers using College-approved security software (which includes virus, spyware, intrusion, and firewall protection) must have the firewall enabled.
b. Any other computer connected to the campus network must run a personal firewall. Microsoft Windows Firewall is an acceptable personal firewall.

Email Protection

a. The campus email server must provide antivirus protection that detects and mitigates infected email messages.
b. Infected messages must be discarded or quarantined, not returned to the sender.

Security Patches

All systems connected to the campus network and the applications and databases running on those systems must have the latest security patches available from the respective vendors applied. Any system or application with known vulnerabilities for which a patch is not available must take appropriate measures to mitigate the risk, such as placing the system behind a firewall. Kentucky Wesleyan may block access to the network for systems that have not been patched.

7.6.6 Enforcement

Enforcement of these policies and associated standards is the responsibility of the CIO or designee. Any system that does not comply with security policies and standards, is susceptible to a known vulnerability, or is compromised may have its network access blocked immediately and without prior notification to protect the integrity of other systems and data.

Revised 11/19/16

Section 8

Privately-Owned Computer Equipment

Any Kentucky Wesleyan College student, faculty or staff member with a valid network user account may request that his or her personal (privately-owned) computer be connected to the campus network, provided he or she agrees to the following:

1. Users of privately-owned computers attached to the network are subject to the same responsibilities and regulations as users of College-owned equipment. (See Section 3 and Section 4 of this handbook)
2. The purchase, maintenance and service of privately-owned computer equipment attached to the campus network is the responsibility of the owner of the equipment.
3. The College maintains no responsibility or liability for loss or corruption of data on privately owned computers.
4. Should the Information Technology Services staff have reason to believe that an individual is using a privately-owned computer to abuse his or her network privileges, they reserve the right to monitor network traffic to and from the computer, and if justified, disconnect the computer from the network and take appropriate punitive action.

4/27/06

Section 9

Web Publishing

9.1 Introduction

Kentucky Wesleyan College maintains a presence on the World Wide Web to provide information about its programs and services; support its educational mission and the continuing academic excellence of its faculty; and provide access to informational resources for study and research. This policy is intended to promote appropriate use of the World Wide Web as a publishing medium by clarifying the responsibilities of authors and providing guidelines for the production of accurate, useful and attractive publications that enhance KWC's mission and image.

9.2 Scope

This policy applies to information:
- published on servers owned by Kentucky Wesleyan College;
- published within the KWC Internet domain (kwc.edu); and
- published elsewhere under direction or control of a KWC department, a KWC organization, or an individual, and identified as official KWC information*.

*****Any department, organization or individual wishing to publish official Kentucky Wesleyan College information on a server not owned by the college must receive approval to do so from the KWC Director of Marketing and Communications, and the KWC CAMS Governance Committee. Without this approval, such information will not be considered official and will not be linked from any Kentucky Wesleyan College Web site.

The Web sites maintained by Kentucky Wesleyan College are official publications of the College. Unless otherwise indicated all text and images appearing on official pages (see "Definitions" below) are copyrighted and should not be reproduced without permission from the KWC director of marketing and communications.

9.3 Access

Access to the Internet and the World Wide Web from Kentucky Wesleyan computers and networks is restricted to authorized registered users for academic, research, learning and administrative purposes. Public access to Kentucky Wesleyan computers and networks may be available from the Internet and World Wide Web or from within specially designated public facilities, such as the Winchester Center Smith Lounge or the Greenwell Library and Learning Center.

9.4 Responsibilities

It is the responsibility of all students, faculty and staff who use information technology resources at KWC to be familiar with and abide by the provisions of the Kentucky Wesleyan College Information Technology Appropriate Use Policy. Publishers of information on KWC Web sites are subject to all provisions of this policy. Contents and usage of all Web pages must be consistent with current KWC operational policies and local, state, and federal laws.

Web pages posted on KWC servers MUST NOT contain:

- copyrighted or trademarked materials in any form without the consent of the copyright or trademark owner;
- information that violates any licensing or contractual agreement;
- images, audio, videos or movies of people without their consent;
- information promoting personal gain or commercial activities not related to the mission of the College;
- information, confidential or otherwise, pertaining to individuals who do not want the information included; or
- images or data that are discriminatory, abusive, profane, harassing or otherwise offensive.

9.4 Definitions

9.41 Official pages

Official pages include the following:

The Kentucky Wesleyan College home page (www.kwc.edu) and pages linked directly from that page. Together, these pages comprise the index level of KWC's publicly accessible Web site. Informational pages linked directly from the index pages comprise the detail level. Generally, index and detail level pages are designed for college-wide or external audiences. As KWC's "front door," these pages are subject to College publication policies pertaining to external communications, graphic identity and public information.

Departmental/unit pages. These are pages produced and maintained by the director of marketing and communications, departments, units, and other officially sanctioned groups (including student organizations) within the College. These pages are usually devoted to items of interest to a particular department, unit or group and its specific audience.

Project/special interest pages. These pages provide information about special College-sponsored activities, and are produced and maintained by individuals, departments, units or groups associated with those activities.

Information published in the above pages is deemed "official" College information and is subject to review by the Director of Marketing and Communications and Campus Technology Committee for accuracy and conformance with appropriate College policies.

9.42 Personal pages

With the approval from the Director of Marketing and Communications, individual faculty and staff may create personal Web pages to be included on the publicly accessible KWC Web site. Students may create Web pages to be included on internal sites in conjunction with course assignments and under the direction of an instructor. Such individual pages are intended for **professional and instructional purposes only** and must comply with College policies, local, state and federal laws, and any relevant licensing agreements relating to intellectual property. The College assumes no responsibility for the contents of personal Web pages or for any links from these pages. The College does, however, reserve the right to monitor personal Web pages, to investigate complaints, and to remove or limit access to Web pages that are deemed unacceptable.

The following disclaimer (or a link to this disclaimer statement) must appear on all personal Web pages included on the publicly accessible KWC Web site: "*The views and opinions expressed in this page are strictly those of the page author. The contents of this page have not been reviewed or approved by Kentucky Wesleyan College.*"

Use of official Kentucky Wesleyan College graphic elements such as logos, seals and other identifying marks is prohibited on personal pages.

9.5 Use of College Name

Use of Kentucky Wesleyan College's names (i.e. Kentucky Wesleyan College, Kentucky Wesleyan, KWC), trademarks, official logos, or other intellectual property and creative works is governed by Kentucky Wesleyan intellectual property and creative works policies.

Unauthorized presentation of any web page or file as an Official Kentucky Wesleyan Web Page or Official Kentucky Wesleyan File or any unauthorized or illegal use of Kentucky Wesleyan computers and networks is prohibited.

9.6 Administration and Management

Page managers. Departments, units and groups creating official pages must appoint a page manager for each page published. Page managers for student organizations must attend a web training session and sign a server access agreement form. Page managers are responsible for ensuring that the content of their pages is accurate, current and appropriate for online publication.

Portal/Intranet Administrator. The Portal/Intranet Administrator works with page managers and other information providers to maintain KWC's internal Web sites.

CAMS Governance Committee. The KWC CAMS Governance Committee in conjunction with the Director of Marketing and Communications is responsible for developing, interpreting and reviewing policies pertaining to KWC Web sites. (somehow include me in this language).

9.7 Publication Guidelines

1. Pages published on KWC web sites should be accessible and useful from all generally used Web browsers.
2. All graphic elements on pages should employ the <alt> tag to provide a textual replacement for the image.
3. The words Kentucky Wesleyan College should be prominently displayed on all official pages included on the publicly accessible KWC Web site.
4. All departmental/unit pages should include the name of the department near the top of the page or in an otherwise prominent location on the page.
5. Navigation between pages should be obvious, simple, and consistent.
6. The purpose of the page and audience for whom it is intended should be clear.
7. Text on all pages should be grammatically correct and free of spelling errors.

9.8 Reservation of Rights

The College reserves the right to disable and/or remove, without notice, any Web page or file (official or unofficial) from any computer which is owned or operated by Kentucky Wesleyan and, after appropriate review and warning, the publishing capability on any computer which is owned or operated by Kentucky Wesleyan of anyone who violates this policy (See Section 4: Abuse of Information Technology Privileges).
Revised 11/19/16

Section 10

Data Backup and Disaster Recovery

10.1 Data Backup

10.1.1 Purpose

All electronic information which is a Kentucky Wesleyan College record must be copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

10.1.2 Scope

IT Services is responsible for providing adequate backups to ensure the recovery of electronic information (includes KWC records and software) in the event of failure. These backup provisions will allow College business processes, including the academic enterprise to be resumed in a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple generations of backups should be maintained.
Federal and state regulations pertaining to the long-term retention of information (e.g., financial records) will be met using separate archive policy and procedures, as determined by the Business Owner of the information. Long-term archive requirements are beyond the scope of this policy.

10.1.3 Policy Statement

- Backups of all KWC records and software must be retained such that computer operating systems and applications are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
- At least three versions of College records must be maintained.
- At a minimum, one fully recoverable version of all College records must be stored in a secure, off-site location. An off-site location may be in a secure space in a separate College building, and with an off-site storage vendor approved by the CIO.

- The practice of taking backup media to the personal residence of staff persons is not acceptable.
- Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
- All College record information accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. KWC record information located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives. Alternatively, College record information located directly on workstations, laptops, or other portable devices may be backed up using a 3rd party vendor approved by the CIO. Convenience records and non-records, or other information which does not constitute a KWC record does not carry this requirement.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested on an annual basis.

10.2 Disaster Recovery

10.2.1 Purpose

The purpose of this policy is to ensure the development and maintenance of IT Disaster Recovery for IT System Assets that support critical functions of the College. The policy ensures the College is able to continue to deliver services in the event of a serious disaster or incident by defining a framework that enables:

- Risk reduction in the event of a disaster or serious incident;
- Availability of IT systems required to support critical College processes to agreed levels;
- Compliance with regulatory requirements;
- Integration with College Business Continuity polices and processes; and
- A responsible approach to protect the interests of KWC stakeholders, policyholders, business partners, and suppliers.

10.2.2 Scope

The policy is applicable to all software applications and IT System Assets that support the College across all faculties, academic divisions, and business units hosted internally by the College or externally.

10.2.3 Definition

> **IT System Assets** includes information, the computer systems that support business and control functions, networks and communication links, business applications and programs, and all forms of electronic storage media.

10.2.4 Policy

Information Technology Services is accountable and responsible for the development of an IT Disaster Recovery Plan that ensures the recovery of critical systems and services in a timely manner.

IT Disaster Recovery plans must be:

- Integrated and aligned with the Emergency Management Plan to reflect the College's needs;
- Developed following an approved Disaster Recovery Planning process;
- Periodically tested (at minimum on a semi-annual basis);
- Properly maintained and audited;
- Communicated to all relevant stakeholders;
- Aligned to business/operational needs; and
- Have an owner formally appointed.

IT Disaster Recovery should be developed and maintained in line with a defined IT Disaster Recovery Framework, which will inherently achieve the above requirements.

10.2.5 Administration and Management

The college's CIO is responsible for:

- Overseeing the maintenance and development of the IT Disaster Recovery function;
- Ensuring that IT Disaster Recovery procedural and technical controls are adequately specified and resourced;
- Monitoring the effectiveness of IT Disaster Recovery provisions.

Appendix A

Policy Review Schedule

The Campus Technology Committee will review the policies in this Handbook at least once every three years.

Policy	Adopted	Reviewed	Revised	Next Review
Appropriate Use	12-13-16	12-01-16	11-19-16	Fall 2019
Abuse of Information Technology Privileges	12-13-16	12-01-16	11-19-16	Fall 2019
Allocation of Resources	12-13-16	12-01-16	11-19-16	Fall 2019
Copyright and Licensure	12-13-16	12-01-16	11-19-16	Fall 2019
Security	12-13-16	12-01-16	11-19-16	Fall 2019
Privately-Owned Computer Equipment	12-13-16	12-01-16	4-27-06	Fall 2019
World Wide Web	12-13-16	12-01-16	11-19-16	Fall 2019
Data Backup and Disaster Recovery	12-13-16	12-01-16	11-19-16	Fall 2019