WASHTENAW COMMUNITY COLLEGE (WCC)
ENTERPRISE INFORMATION SECURITY PLAN

PURPOSE

The purpose of this policy is to:

- Define procedures and processes to help protect College data generated, accessed, transmitted and stored by the College
- Educate the College community about the importance of protecting College data
- Ensure confidentiality, integrity, and availability of College data
- Promote compliance with local, federal and industry regulations regarding privacy, protection and confidentiality of information.

All members of the College community have a responsibility to protect College data from unauthorized generation, access, modification, disclosure, transmission, or destruction, and are expected to be familiar with and comply with this policy.

CONTENTS

1.0 DATA CLASSIFICATION

This Enterprise Information Security Policy defines for College employees the levels of security required to protect data they receive or use in the course of business and for which they are responsible. The information covered by this policy includes all information received or handled by College employees in the performance of their job duties, whether written, oral, or electronic ("College Information"). It includes, but is not limited to, information that is either stored or shared electronically.

All employees must familiarize themselves with these classifications and guidelines. All College Information must be classified into one of three categories: Restricted, Limited Access or Public. Based on the classification, employees must implement appropriate security measures to protect College data.

Questions about the proper classification of a specific piece of information are to be addressed to your supervisor. Questions about these guidelines are to be addressed to the Chief Information Officer (CIO) or designee, x3400.

General Rules:

1. With the exception of Public Information, access to College Information must be at all times limited to only those employees who have a business reason to know such information. For example, personal information, student records, accounts, balances, transactional information, credit cardholder information and ACH (electronic check) account numbers are to be accessible only to College employees with an appropriate business need for such information.

2. College Information shall only be used for College business purposes.

3. All third-party contractors who have access to the College's Restricted or Limited Access Information must sign nondisclosure agreements prior to being given access. Contractors must agree to use College information only for College business and to abide by this policy.

4. Employees must use their College e-mail address for all College business involving data covered by this policy. Because of security concerns, employees shall not have their e-mail forwarded from their college e-mail account to a private e-mail account.

5. Until data is classified under these guidelines, data shall be treated as Limited Access.

6. This document will be reviewed by the Security Analyst on an annual basis.

1.1 Restricted Information

Restricted Information is data about a person or entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or be damaging to the financial standing, employability, or reputation of the person or entity. The College is bound by law or by contract to protect some types of Restricted College Information. In addition, the College requires protection of some other kinds of information beyond legal or contractual requirements.

Restricted Information can only be shared as mandated by law or as required for administrative or educational functionality. Examples of Restricted Information are the following:

- Social Security Number
- Credit Cardholder Information
- Checking or Savings or other Bank Account Number(s)
- Debit Card Number
- Password(s)
- Disability Information
- Health and Medical Information
- Library Circulation Records

Access: Authorized College employees, and non-employees with signed nondisclosure agreements, who have a business need to know. Electronic access must be protected by a strong password, and users shall log out or secure the documents before leaving their stations. Departments shall promptly notify Information Technology Services regarding personnel changeovers.

Distribution within College: Interoffice mail stamped confidential, electronic mail and electronic distribution methods (see below). Library circulation records may not be distributed.

Distribution outside of College internal mail: Sent via U.S. mail or approved private carriers. Library circulation records may be distributed only as instructed by the Dean of Learning Resources in accordance with applicable law.

Electronic distribution: Must be encrypted if sent to approved recipients within College via e-mail system supported by the College. Must be encrypted, password protected, or faxed to approved recipients outside of College premises. Transmission of data must be via a secure method, such as secure file transfer protocol. Agreements with outside vendors must require encryption or password protection. Instant Messages and Cloud storage services are not to be used for electronic transmission without the prior approval of the CIO.

Storage: In paper form, must be stored in a locked drawer or other locked and secure location. May not be downloaded or stored on laptops, flash drives, and external removable media. May be downloaded on desktop personal computers temporarily for manipulation or processing. Backup files must be encrypted. Cloud storage services may not be used for storage without the prior approval of the CIO. A network drive/folder may be used if access is restricted to only those with a business need. Credit Cardholder Information shall be encrypted or not stored at all, per PCI guidelines.

Disposal/Destruction: Shredded immediately after completion of task; electronic data must be expunged/cleared immediately after use. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Examples of How Data Can Be Lost or Compromised	**Impact of Restricted Data Loss**
• Laptop or other data storage system stolen from car. • Employee accesses system after leaving employment because passwords aren't changed. • Unauthorized person walks into unlocked office and steals equipment or files or accesses unsecured computer. • Unsecured application on a networked computer is hacked and data stolen. • Human error in programming changes. • Data transmitted over internet in unencrypted form.	• Long-term loss of funding from granting agencies. • Long-term loss of reputation. • Unauthorized tampering with enterprise data. • Increase in regulatory requirements. • Long-term loss of critical campus or departmental service. • Individuals put at risk for identity theft.

1.2 Limited Access Information

Limited Access Information is defined as not Restricted, but can be used as personally identifiable or private information. This information must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage, or other use.

This information is releasable in accordance with the Michigan Freedom of Information Act. Limited Access Information is generally restricted to members of the College community who have a legitimate purpose for accessing such data. Limited Access information must be appropriately protected to ensure a controlled and lawful release. One piece of Limited Access Information can't in and of itself be used to identify anyone. Two or more pieces of information is needed. For example, a WCC ID number itself is useless unless combined with a name and/or birth date. A list of salaries is useless unless combined with names and/or position titles.

Limited Access Information:

- Staff and student home address and phone number information
- Salaries
- FERPA directory information
- Class lists
- Student Records (Grades, test scores, attendance, enrollment and registration history, counselor's comments)
- Database access lists
- Payroll information
- Beneficiary/dependent info
- Benefit elections
- Campus Safety & Security Incident reports
- WCC ID#
- Drivers' license number
- DOB
- Ethnicity
- Purchasing information designated as proprietary or confidential

Access: College employees, and non-employees with signed non-disclosure agreements, who have a business need to know.

Distribution within College: Standard interoffice mail, electronic mail system supported by the College and electronic file transmission methods.

Distribution outside of College internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within College via e-mail system supported by the College. If this information is sent to the approved recipients outside of College e-mail systems, it must be encrypted, password-protected, or sent via a private link or faxed. Instant Messages and Cloud storage services are not to be used for electronic transmission of this data without the prior approval of the CIO.

Online Application for Admission: For the purpose of completing the WCC Online Application ONLY, the following use of the WCC Student ID and First Name or Preferred Name is allowed. The applicant will provide their personal email address, as they do not yet have a WCC email address. WCC will send only the applicant new Student ID along with First Name or Preferred Name, if given, to the applicant email provided.

Storage: Individual access controls shall be implemented at the network folder or directory level for electronic information. Cloud storage services may not be used for storage of this data without the prior approval of the CIO.

Disposal/Destruction: Shredded or placed in specially marked disposal bins for shredding on

College premises; electronic data must be expunged/cleared immediately after use. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Examples of How Data Can Be Lost or Compromised	Impact of Limited Data Loss
In addition to the above scenarios... • Staff member wanting to be helpful releases information they are not authorized to share.	• Short-term loss of reputation. • Short-term loss of research funding. • Short-term loss of critical departmental service. • Unauthorized tampering of research data. • Individuals put at risk for identity theft.

1.3 Public Information

Public Information is information that is open to the public and that can freely be given to anyone without any damage to the College or to individuals. Public Information, while subject to College posting or disclosure procedures, is available to all members of the College community and to all individuals and entities external to the College community.

Examples include the following:

- Publicly posted press releases
- Publicly posted schedules of classes
- Published College catalog
- Information authorized for posting on the College's public website
- On-line staff directory, interactive maps, newsletters, etc.
- High-level aggregate enrollment data
- Board of Trustees agenda and minutes.

Access: Public, external and internal

Distribution within College: No restrictions.

Distribution outside of College internal mail: No restrictions.

Electronic distribution: No restrictions.

Storage: No restrictions.

Disposal/Destruction: See WCC Retention and Disposal Guidelines.

Penalty for deliberate or inadvertent disclosure: Not applicable.

Examples of How Data Can Be Lost or Compromised	Impact of Public Data Loss
See the above scenarios.	• Loss of use of personal workstation or laptop. • Loss of personal data with no impact to the College.

2.0 ADMINISTRATIVE PROCEDURES

2.1 Classification

Documents must be classified according to the type of information contained in the document. All documents must be classified and handled according to the procedures for the highest restricted level of any information contained in the document. For example, if a document contains both Restricted and Public Information, the document shall be treated according to the Restricted Information procedures.

Questions about the classification of particular information or documents are to be addressed to your supervisor. Questions about these guidelines may be addressed to the CIO or designee at x3400.

2.2 Training

2.2.1 Initial Training: All employees shall be trained on the procedures and guidelines of this policy and other issues pertaining to information security awareness. If significant changes are made to the definitions of information or the procedures required, all employees shall be informed via electronic or regular mail.

2.2.2 Periodic Refreshers: All employees shall complete a review course on information security awareness at least annually.

2.3 Definitions and Guidelines

Appropriate measures: Appropriate measures are defined under the individual data type definitions.

Approved Electronic File Transmission Methods: Includes supported Secure File Transfer Protocol (SFTP) and Secure Sockets Layer (SSL) clients and Web browsers as defined or approved by Information Technology Services (ITS)

Approved Electronic Mail: Includes all mail systems supported by ITS.

Approved Encrypted email and files: Information must be encrypted in accordance with ITS guidelines. Contact User Support for assistance.

Configuration of College-to-outside-party connections: Connections shall be set up to allow other entities to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Credit Cardholder Information: banking information, credit card information, credit card track (magnetic stripe) information, security codes, other data obtained as part of a payment transaction or other confidential information as described in the Payment Card Industry Data Security Standard (PCI-DSS). The PCI-DSS standards can be found at https://www.pcisecuritystandards.org/.

Expunge: To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data supplied by ITS User Support. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.

Individual Access Controls: Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac's and PC's, this includes using boot-up/login and screen saver passwords. Employees must always sign out of controlled access systems before leaving their desk or station. Desktop systems must be locked or turned off before leaving the workstation.

2.4 Violations

Violations of the security guidelines contained in this policy shall be reported immediately to your supervisor. The supervisor shall immediately contact the CIO or designee, x3400, to determine if further action is needed to secure College information. The CIO or designee will work with the affected areas and personnel to determine the appropriate actions to be taken.

3.0 SYSTEM SECURITY

3.1 Physical Security

3.1.1 Computer Room Access: Doors to the computer room are closed and locked at all times. A limited number of ITS and maintenance staff have access, and access is only via use of the electronic fob/key card system so that access can be tracked. The computer room is monitored by closed circuit television and Campus Security staff performs security checks 24 hours a day. Access logs are reviewed bi-weekly by ITS staff.

3.1.2 Remote Access: Remote access must use secure connection protocols. Remote access to the servers is limited to staff members with a legitimate business reason and must be done through the approved Virtual Private Network (VPN).

3.1.3 Video Surveillance: The ITS department is monitored via closed circuit television at all times.

3.1.4 Personnel Verification: All staff members shall present a picture ID to Campus Security staff if requested.

3.2 Network Security

3.2.1 Firewalls: All network traffic to and from the primary application/database servers must pass through at least one firewall, which monitors and blocks unauthorized traffic. All servers behind the firewall use Network Address Translation (NAT) addresses. Private addresses will not be disclosed to external entities. All new connections behind the firewall are scanned by the firewall upon connection. Firewall and router rule sets will be reviewed at least every 6 months.

3.2.2 E-Mail Filter: A robust e-mail filter system shall be used to significantly reduce the amount of e-mail spam. All incoming e-mail shall be scanned for malicious software

3.2.3 Packet Shaping: Packet shaping technology shall be utilized to monitor network traffic. A packet shaping appliance throttles down unwanted protocols and allocates bandwidth where it is most needed.

3.2.4 Wireless Environment: Wireless connections at the College are unable to access the College administrative network.

3.3 Server Security

3.3.1 Login Accounts

3.3.1.1 Administrator Accounts: Administrator privileges are granted after review of the need for such privileges. Only personnel in charge of systems have access to administrator accounts.

3.3.1.3 User Accounts: User accounts are created for each new employee with minimal access privileges (e-mail, MyWCC, intranet, etc.). Additional access privileges are granted on an as-needed basis.

3.3.1.4 Vendor Accounts: Vendor accounts will only be enabled during the time period needed and monitored while in use.

3.3.1.5 Password Policy: All passwords shall be changed at least every 90 days for the cardholder and payment applications. Unique passwords are required. Users shall not share passwords.

Any vendor supplied password will be changed before any implementation of hardware or software.

Individual accounts created on websites that are not hosted by WCC ITS staff must use a different password from that used for the user's WCC netID.

The WCC password guidelines can be viewed from any WCC website page (www.wccnet.edu) by selecting the "Quick Links" menu, then "netID management" and then "Help"

3.3.2 File/Directory Access: Permissions on system files shall be as restrictive as possible while still allowing users to be effective.

3.3.2.1 Database Files: Database files are accessible only to the system and database administrators.

3.3.2.2 Source Code: Access to source code is restricted to ITS staff.

3.3.2.3 Output/Report Files: Read only access to reports is restricted to employees who have the business need to see the report information and who are properly authorized.

3.3.3 Data Backup

3.3.3.1 Backup Media: Servers are backed up every day in accordance with established backup policies. Backup media is stored in a limited access, monitored room and off site with a third party recognized in the business of storing such media. A limited number of staff are authorized with this vendor to deposit and retrieve this media.

3.3.3.2 Personal Data Files: It is the responsibility of each department and employee to assure that the confidentiality, preservation, and integrity of sensitive data (restricted or limited) within the College's policies. This includes the secure distribution, storage, and destruction of sensitive data on personal media.

3.3.4 OS Enabled and Disabled Services: Where applicable, servers are logically and/or physically separated from one another for security. Installed servers run only the services necessary to perform their duties in an effective manner. Configuration changes are made to harden the machine against potential security threats. Monitoring and logging is set up both locally and centrally for each server.

3.3.5 OS Patches: Operating systems are patched on a regular basis, or specifically when there are major security/stability issues. Other installed software is likewise patched either on a regular basis or when a specific security/stability bug report is released.

3.3.6 Server Functions and Disclosure: Servers shall be created based on industry best practices and business requirements. Best practice is for one primary function per server to prevent functions that require different security levels.

Disclosure of private internal IP addresses of cardholder, payment, business computers or other college computer hardware is prohibited, unless required for an approved business purpose.

3.4 Database Security

Database Security applies to the access of data stored in a database management system (DBMS) such as Oracle, MySQL, and Microsoft SQL Server.

3.4.1 User Accounts: User accounts can be managed either in the application or by the DBMS. In the first case, the user security is built into the application and requires the administrator to employ application utilities to manage user accounts. In the second case, the users log directly into the database and the database administrator (DBA) uses database features to maintain database security.

3.4.1.1 Account Creation and Termination: User accounts are either created by the database administrators or automatically through business application logic. Banner account creation requires a request from a validated supervisor and must be preceded by appropriate training. Banner accounts are created by DBAs while Blackboard accounts are typically generated through the enrollment logic for students and by the Blackboard administrator for faculty. Likewise MyWCC accounts are generated automatically either by the student enrollment or the employment processes. Similarly, account termination is either by direct DBA action or automatically through application logic or external processes that attach to the database.

3.4.1.2 Password Complexity and Expiration: All accounts must have an ID and a login password. Passwords are stored encrypted in system tables. Automatic password expiration rules and password retry attempt limits are in accordance with WCC standards. Reset requests require identity verification.

3.4.1.3 Timeouts: Idle connection timeouts are another aspect of electronic security, especially in situations of public computer use. Idle timeout for Banner is typically one hour for the WCC staff. MyWCC has idle timeouts varying from fifteen minutes (students) to two hours (advisors) depending on the user's functional role. Timeout rules vary depending on user status and the nature of the application.

3.4.1.4 Auditor and Contractor Accounts: On occasion, the need arises for auditors or private outside contractors to have access to databases. WCC's policy is to create such accounts with the access required, but to either lock them or drop them after the work is performed. All outside auditors and contractors sign confidentiality and nondisclosure agreements before access is granted.

3.4.1.5 Restricted Access Accounts: Certain database accounts are used for data ownership. These accounts contain tables or stored procedures used by the application. Only data base administrators or application developers log into these accounts. Since they are permanent accounts, their login access is carefully restricted by the database administrators.

3.4.2 MyWCC Accounts: MyWCC is the web-based information system self-service product. The web application gives an individual access to his/her personal data stored in the Banner ERP. It is also the primary vehicle for student registration, faculty grade entry, and advisor overrides and reports. Access into MyWCC requires a user account with a unique user name and password and requires the user to agree to confidentiality and access conditions.

3.4.3 Database Object Access: Database objects include tables with data, views on those tables, and stored procedures. Access to database objects is normally via the application and depends on the user's application security privileges. However, direct access is authorized and granted to a small number of users for reporting purposes.

3.4.4 Database Auditing: Database auditing consists of the automated collection of database events and changes and the manual review of that information by the database administrators. There are also audit trails on the web servers and application servers. The UNIX administrators and database administrators have also developed in-house auditing programs. Data collected is used to detect security breaches and assess damage. Third party software packages are also used for auditing purposes.

3.4.5 Data Encryption: Data encryption refers to the encoding of clear text into a binary form that requires proper authorization and decryption keys to decode. The College employs encryption for secure websites that use the https (or http over SSL) protocol. In this case, encrypted data is sent and received over the internet. Encryption is also used for some sensitive data stored in College database tables.

3.5 Application Security

Applications often serve as the delivery mechanism through which personal data and other sensitive information is transferred online. Unsecured or poorly written applications can be exploited to bypass security measures or used to transfer information that is easily intercepted.

WCC applications are developed following industry best practices. SSL and SFTP protocols are used for access and transmission of Restricted and Limited Access Data.

3.6 Desktop Security

3.6.1 Standard Windows Image: Standard images have been created that are deployed on all new computers and are used to refresh existing computers. The use of standard images prevents the installation of unneeded services.

3.6.2 Virus Protection: Antivirus software is utilized to protect systems from viruses. The software is automatically updated frequently. On-access scanning is always running, and full scans are automatically performed twice per week. Users can also configure and run a local scan.

3.6.3 Automatic Updates: Windows updates are controlled via an internal server. Updates are reviewed and approved by User Support staff. Updates are set to install at shutdown or they may be installed manually via a system tray icon.

3.6.4 Remote Desktop Access: Windows Remote Desktop functionality shall be disabled on all college-owned computers by outside addresses. If there is a need for remote access to college-owned machines, it will only be allowed using the WCC approved VPN and permission of the Chief Information Officer. Two-factor authentication for remote access is required.

3.6.5 Cardholder Data Desktop Access: **Access to credit card and payment applications requires secure connections (https).**

3.6.6 Machine Reuse: When a computer is being retired, User Support shall wipe and overwrite all data from the hard drive using standard practices such as the DOD wipe.

3.6.7 Cashier Office Workstations: When a machine used for credit card and payment applications is retired or repurposed the hard drive will be DOD wiped and physically destroyed so there is no chance of retrieving data from the drive.

3.6.8 Firewall: All computers on the administrative network shall have a firewall installed that is administered by ITS.

3.7 Detection and Auditing Procedures

The ITS department maintains and routinely updates its internal audit procedures and damage assessment and control procedures.

3.8 Business Continuity and Disaster Recovery Procedures

The College maintains, and updates as needed, a Business Continuity and Disaster Recovery Plan. This plan would be implemented in the event of destruction or disruption of the College's information systems. The plan outlines a protocol of responses based on the type and severity of the event.

4.0 PAYMENT PROCESSING

4.1 PCI Compliance

All credit card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted in accordance with the WCC security and PCI-DSS standards and procedures. No activity may be conducted or any technology employed that might obstruct compliance with any portion of the PCI-DSS, WCC security procedures or the WCC Enterprise Information Security Plan.

All credit card and payment processing technologies and software applications must be approved by ITS and Finance prior to any implementation or use within WCC or any application associated with the college.

4.2 Mobile Device Security

Any College owned mobile device, that has direct connectivity to the Internet, will have a firewall installed.

5.0 INCIDENT RESPONSE

5.1 Data Security Incident Response Plan

In the event of a breach of security involving unauthorized access to College electronic information, the President, Chief Information Officer or their designee shall immediately convene a Response Team to manage the College's response.

The Information Technology Services department will respond to reports of incidents, compromises and breaches of WCC computers, data, and network resources. The purpose of the Incident Response Plan is to establish procedures in accordance with applicable legal and regulatory requirements to address instances of unauthorized access to or disclosure of College information. The Incident Response Plan defines the steps, roles and responsibilities for the involved personnel when reacting to an information security threat.

The primary emphasis of this plan is to return the WCC computing environment to a secure state as quickly as possible, while minimizing the adverse impact to the College. Depending on the circumstances, the Response Team may decide to modify or bypass one or more of the procedures outlined in this plan in response to a particular security incident, with the understanding that all reasonable steps will be taken to investigate and resolve any security issues.

The college shall provide timely and appropriate notice to affected individuals and departments when there has been a security incident, a compromise or a breach involving WCC data, computers or networks. The Chief Information Officer, Chief Financial Officer, and the College Legal Counsel shall be responsible for reviewing breaches to determine whether notification is required, and directing responsible departments in complying with the notification obligation. All known or suspected security incidents must be reported to the CIO or designee.

5.2 General Incident Response Procedures

This plan outlines the steps to follow in the event secure electronic data is compromised or any intrusion of the computing environment is detected. The same steps can be followed for a suspected data compromise or breach. This plan is focused on Credit Card data and confidential and restricted access electronic information. The WCC security incident response plan is as follows:

- Each department must report an incident or perceived incident to the CIO or designee.
- The CIO or designee will begin the formation of the Response Team.
- The Response Team will investigate the incident and determine if a breach has occurred. The Response Team will, if necessary, assist the compromised department in limiting the exposure of Restricted Data.
- The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, cardholders, etc.) as necessary.
- The Response Team will document the incident and determine if policies and processes need to be updated to avoid a similar incident in the future.

5.3 Incident Response Team

An Incident Response Team (Response Team or IRT) will be established to quickly and effectively address an incident. The IRT is headed by the CIO or designee. The IRT is authorized to take the appropriate steps deemed necessary to contain, mitigate or resolve the incident to protect College data and computing environment.

The IRT will consist of the following members and/or their designated staff:

- Chief Information Officer or designee
- College Legal Counsel
- Chief Financial Officer or designee
- Other staff as required

5.4 ITS Security Incident Response Procedures

Any department with a suspected or actual system compromise must contact the CIO. After being notified of a compromise, the Response Team, along with other designated staff will implement the incident response plan and other steps needed to resolve the incident.

In response to a systems compromise, the Response Team will:

- Ensure compromised system(s) is/are isolated on/from the network. Do not immediately shut down the machine, as you may lose important information. If the machine is being used to attack others, or if the attacker is actively using or damaging the machine, you may need to disconnect it from the network. Other actions may include disabling user accounts, changing passwords, stopping services, stopping backups to preserve good backup files.
- Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system and application logs. This may also include database logs and local PC event logs.
- Assist department in analysis of locally maintained system and other logs, as needed.
- Conduct appropriate forensic analysis of compromised system(s).
- Define and/or implement changes needed to the WCC computing environment or applications to resolve the incident.
- The Chief Information Officer and/or Chief Financial Officer will notify the necessary college staff or outside organizations as appropriate.
- Make forensic and log analysis available to appropriate law enforcement or card industry security personnel as necessary.
- Assist law enforcement and card industry security personnel as necessary.
- Notify card holders as appropriate per legal requirements.
- The CIO shall document the determinations made by the Response Team and the implementation of the College's response.

6.0 RELATED POLICIES

- **WCC Website Privacy Policy**
  https://www.wccnet.edu/services/account/terms-service/

- **WCC Schedule for the Retention and Disposal of Records**
  Available upon request from WCC Records Management.