# Mohawk Valley Community College Information Security Procedures

| | |
|---|---|
| **Policy Name:** | 5001 Information Security |
| **Issued:** | July 27, 2021 |
| **Revision Date:** | |
| **Responsible Office:** | Information Technology |

Mohawk Valley Community College (MVCC) is committed to providing its employees, students, and partners with current technology and computing resources while ensuring compliance with the General Data Protection Regulation (GDPR) and the Gramm-Leach-Bliley Act (GLBA). This commitment extends to protecting these resources from illegal or damaging actions carried out by individuals, whether knowingly or unknowingly. All MVCC employees, students, alumni, contractors, consultants, temporary employees, tenants, and guests (hereafter referred to as "end users") must adhere to established procedures related to all College Information Systems, including:

- MVCC-owned and supported desktop and laptop computers.
- Non-MVCC computers used to access MVCC network resources.
- Voice and data networks, wired and wireless, owned and operated by MVCC, and any equipment directly attached to them (e.g., personally owned laptops, computers, tablets, smartphones, networking devices, etc.).

## Terms of Computing and Network Usage

Primary use of computing and network resources is restricted to activities supporting the Mission, Vision, and Purpose of the College. End users are responsible for exercising good judgment regarding personal use. If uncertain, employees should consult their direct supervisor, the Executive Director of Human Resources, or the Executive Director of Information Technology.

MVCC endeavors to provide reasonable privacy levels; however, users should be aware that all material and data created on the College's systems may be requested and disclosed under the Freedom of Information Law (FOIL) or by government subpoena. Despite efforts to ensure electronic privacy, MVCC cannot guarantee this. The College will implement anti-intrusion, anti-virus, anti-SPAM, and other systems to provide a secure computing environment. Monitoring and disclosure of information stored, processed, or transmitted by electronic devices may occur for stated purposes, exposing confidential information only minimally and as needed. Monitoring and dissemination of an individual's email communications, web/internet activities, or stored data require written approval from the Executive Director of Human Resources.

## Protection of Personally Identifiable Information (PII)

Any information considered Personally Identifiable Information (PII) that college procedures deem sensitive or confidential must be appropriately protected as described in this procedure. MVCC will adhere to GDPR and GLBA requirements by:

- Ensuring that PII is only collected for specific, legitimate purposes and is not processed further in a manner incompatible with those purposes.
- Implementing adequate security measures to protect PII against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- Ensuring that end users have the right to access their personal data and correct any inaccuracies.
- Ensuring that PII is Collected and stored using software and accounts that has been approved by the Director of Compliance and the Executive Director of Information Technology to store PII. Employees seeking approval to use software and accounts that will store PII collection should send an email to the Executive Director of Information Technology and the Director of Compliance with a business justification.

## Network and Resource Management

MVCC reserves the right to block all Internet communications from sites, hosts, or devices involved in disruptive or damaging practices, potentially exposing the College to legal liability, or deemed not meeting the Mission, Vision, or Purpose of the College. MVCC may prioritize network resources during peak demand. No warranties are provided for access, and the College assumes no responsibility for the quality, availability, accuracy, nature, or reliability of material accessed from the Internet.

## Password and Account Security

End users must secure their passwords and accounts, remaining accountable for any violations originating from their computer or account. PII or sensitive data must not be stored on local hard drives or removable media. Devices connected to MVCC networks must have current anti-virus and operating system security patches installed.

## General Data Protection Regulations (GDPR) and Gramm-Leach-Bliley Act (GLBA) Compliance

Mohawk Valley Community College is dedicated to maintaining the privacy and security of all personal and financial information in compliance with the General Data Protection Regulation (GDPR) and the Gramm-Leach-Bliley Act (GLBA). As part of our commitment:

GDPR Compliance:

- MVCC ensures that any processing of personal data of individuals within the European Union (EU) adheres to the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality as outlined in the GDPR.
- Personal data collected and processed by MVCC will only be used for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Individuals have the right to access their personal data, request corrections or deletions, restrict processing, and object to processing. Requests can be made to the Director of Compliance. The Director of Compliance will review the request and inform the individual and the IT department of the appropriate action to take.
- MVCC implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the encryption of personal data and the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.

GLBA Compliance:

- MVCC complies with the GLBA by protecting the privacy of consumer financial information and implementing an information security program that includes administrative, technical, and physical safeguards.
- The College identifies and assesses the risks to customer information, designs and implements information safeguards to control these risks, and regularly monitors and tests the effectiveness of these safeguards.
- Employees, students, and partners handling sensitive financial information receive training on their responsibilities to protect this information and the procedures to follow to ensure compliance with the GLBA.

MVCC is committed to ongoing compliance with GDPR and GLBA requirements and regularly reviews and updates its policies and procedures to reflect any changes in regulations and best practices. Any questions or concerns regarding data privacy and security can be directed to the Information Technology Office or the Executive Director of Information Technology.

## Reporting and Auditing

Any instances of theft of MVCC equipment must be immediately reported to the Executive Director of Information Technology and Public Safety for on-campus incidents. For off-campus incidents, it is the responsibility of the employee to immediately report the theft to the Executive Director of Information Technology and appropriate police agency. A copy of the police report must be filed with the Executive Director of Information Technology.

## Prohibited Practices

The following activities are expressly prohibited:

- Collecting and storing Personally Identifiable Information (PII) using software or account that has not been approved by the Director of Compliance and the Executive Director of Information Technology.
- Activity that is illegal under local, state, federal or international law while utilizing MVCC-owned computers or networks.
- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property.
- The installation or distribution of "pirated" software products that are not appropriately licensed for use by MVCC.
- The installation of “Bootable Devices” on any PC or Laptop.
- Unauthorized copying of copyrighted material including, but not limited to, digitized and distributed photographs from magazines, books or other copyrighted sources, copyrighted music or videos, and any copyrighted software for which MVCC or the end user does not have an active license.
- Misrepresenting one's identity or relationship to the College when obtaining or using College computers or networks.
- Exporting software, technical information, encryption software or technology that violates local, regional, international or export control laws.
- Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, phishing, etc.).
- Using an MVCC computing asset to actively engage in procuring or transmitting material that is in violation of anti-pornography, sexual harassment, libel, slander, or hostile workplace laws in the user's local jurisdiction.
- Using an MVCC computing asset for private commercial purposes or making fraudulent offers of products, items, or services originating from any MVCC account.
- Carrying out security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning.
- Executing any form of network monitoring which will intercept data not intended for the employee's host device unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any device, network, or account.
- Interfering with or denying service to any user (for example, denial of service attack).
- Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session, via any means, locally or via the network.
- Providing information about, or lists of, MVCC employees to parties outside MVCC, unless within the formal approved scope of one’s job, or without approval from Cabinet.

- Using the College's email system (outside of MVCC Today) to solicit or advertise personal products, productions or other items or events not related to the College's stated mission, vision, and purpose unless the user has obtained prior approval from his or her direct supervisor.
- Any form of harassment via email, telephone, instant messaging, or other electronic means, whether through content, frequency, or size of messages.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of College equipment and communication systems by employees or other authorized users to attempt to influence legislation or in any other way lobby elected officials, except on behalf of SUNY or the College.
- Blogging that does not fall within the Mission, Vision or Purpose of the College.

## MVCC Network Access

**Open Usage Computers:** Computers are available for use in Open Labs by all current MVCC students, staff, and Board of Trustees members. A valid MVCC ID Card may be requested for verification. Computer access is gained by one's username and password.

**Teaching Lab Computers:** Teaching Lab Computers are accessible to all MVCC students and faculty during a formal class period. Special hours of Open Lab time specific to the software / course being taught in the lab may be provided.

**Office computers:** Only active MVCC employees (excluding students), who hold a Network Account for access to the MVCC Domain are authorized to access faculty and administrative office computers, unless otherwise authorized by the area Dean/Supervisor or the Executive Director of Information Technology.

**Wireless Network Access:** Active Employees, active students, and Trustees are authorized to access MVCC Wireless Networks via their username and password. Using their own devices, guests of the college may request the guest account login at the Information Technology Help Desk.

**Physical Ports:** Active network ports may only be used by faculty or staff if arrangements are made in advance with the Information Technology Department. Under no conditions should a preexisting network connection be unplugged or plugged in without the approval of the Information Technology Department. Any non-domain device will be prompted for a network username and password.

**Operating Systems and Anti-Virus Updates:** MVCC owned computers, upon connection to one of the network domains, will have patches and updates automatically downloaded and installed.

## Access to Administrative Data

Banner / Degree Works / Argos / OnBase Accounts (Administrative Data)

Employees with an MS-Windows Network Account (on the MVCC Domain), with "Administrative Data Supervisor" approval (or appointed designee), are authorized to access administrative data in which they have a legitimate business interest.

Administrative Data Supervisors are defined as follows:

- Student – Registrar
- Advisement (Degree Works) – Registrar
- Admissions – Director of Admissions
- Finance – Controller
- Payroll – Controller
- Student Accounts Receivable – Controller
- Human Resources – Director of Human Resources
- Advancement – Executive Director of Institutional Advancement
- Financial Aid – Director of Financial Aid
- Banner General – Information Technology Database Administrator

**Access Review –** On a yearly basis a report of all individuals who have access to MVCC Administrative Systems and Data will be provided to the Administrative Data Supervisors for their review. Any irregularities in access rights must be reported to Information Technology Database Administrator for corrective actions.

**Self-Service Banner ("MyMV") - -** Upon departure from the college, employee access to MyMV will be disabled.

## MVCC Network and Email Accounts

The following individuals are authorized to hold active Network and Email Accounts:

- Current employees and students of MVCC
- Members of the MVCC Board of Trustees
- Others as approved by the appropriate MVCC Presidential Cabinet Level or the Executive Director of Information Technology.

### End-User Accounts – Storage Quotas

Active employees and students are allocated 50GB of email storage and 1TB of file storage on OneDrive.

### Employee Email Address Format(s)

The standard email address format is: firstname.lastname@mvcc.edu (john.doe@mvcc.edu) or firstinitialandlastname@mvcc.edu (jdoe@mvcc.edu) as determined by the employee's name on

file for HR/Payroll purposes. Employees may request that a "preferred first name" be used in the email format in lieu of first name via application in the Human Resources Department.

## Employee Network Accounts

Employee network accounts, including email, accounts shall be disabled upon departure from the college. At the supervisor's request, incoming emails to the employee's account will be forwarded to a designee specified by the employee's supervisor.

Disabled accounts will be removed from the active directory.

## Student Email Address Format

The standard student email address format is: firstinitial.lastname"birthday day of month"@student.mvcc.edu (jdoe02@student.mvcc.edu). Students may request that a "preferred first name" be used in the email format in lieu of first name via application in the Office of Records and Retention.

## Student Network Accounts

Student network accounts, including email, accounts shall be automatically disabled one year after the end date of the last attended semester, if the student is not scheduled. Disabled accounts will be removed from the active directory.

## Student MyMV Accounts

Student MYMV account access shall be disabled one year after the end date of the last semester the student attended.

Password Protocol

All passwords must meet the following standards to be considered a valid and "strong password":

- A minimum of 8 characters
- May not contain User/Login Name
- Must contain the following two characteristics:
- At least one upper case character.
- At least one numeric

## Password Expiration

Existing passwords will automatically expire after 180 days of creation. End-Users will be required to specify new passwords and may not repeat previously used passwords.

## Account Security

A user has three opportunities to enter a correct password. If s/he does not enter the correct password after three tries the account will be locked and s/he will be prompted to contact the Information Technology Helpdesk for a reset. All users are required to use Multifactor Authentication (MFA).

### Sharing Account Information

A user should not share his/her account password with others or allow use of his/her account by others, except for the Information Technology Department for the purpose of software troubleshooting or installation.

### Generic Accounts

Creation of generic accounts shall be considered an exception to security best practices and will only be done with the approval of the Executive Director of Information Technology. Generic accounts require a designated employee that will be responsible for the account.

### Locking Machines

For security of data, end-users must "lock" their computers when leaving their workstations to prevent unauthorized access.

### Connecting Personal Equipment to the Network

The network will be configured to only allow personal equipment that is up-to-date, including virus protection to connect to the WiFi.

### VPN

VPN is available for active employees who are approved to work remotely. VPN will only be installed on MVCC owned devices. VPN utilizes multi factor authentication, this requires a separate device for the app.

All remote work requests must be approved through the remote work policy. Remote workers will be assigned a laptop as their device for both remote and on campus work. Monitors, printers, and other devices will be at the employee's expense. The remote policy should be reviewed for further details.

### Change of Job Duties

If an employee changes jobs within the College, access to computer network resources related to their old job will be removed. If access from their former job is still needed, written authorization must be obtained from the supervisor for the former job.

If an employee changes jobs, and the new job requires access to new Administrative Systems/Data, changes in access must be approved by the appropriate Administrative Data Supervisor(s).

## Data Access Privileges

### Shared Folders

Individuals will be granted access to shared folders upon approval from the folder's owner.

### Domain Top Administrator Account Privileges

MS-Windows Domain Administrator level access to computer and network systems shall be granted only to specific Information Technology Department personnel as authorized by the Executive Director of Information Technology.

### Sensitive Data/Privacy

Sensitive/Private data is defined as any data that could provide access to personal information of an individual or institution. Such data includes, but is not limited to, documents and files that may contain Personally Identifiable Information such as financial, human resources, payroll and student information documents and files.

Personally Identifiable Information ("PII") is defined as any of the following:

- First, Middle, Last Names
- Social Security Number
- Passport Number
- Employee or Student Identification Number (M#)
- State or Federally Issued ID numbers (e.g., driver's licenses).
- Date of Birth
- Maiden Name
- Mother's Maiden Name
- Credit Card or Financial Account Information
- Results of background or criminal history checks
- Payroll and salary information
- Medical Information
- Accommodation requests and related information
- Biometric data (such as fingerprint, voice print, retina, or iris images)
- Digital or other electronic signature files.
- PII data should never be stored on local hard drives or external storage media or by using any using software or account that has not been approved by the Director of Compliance and the Executive Director of Information Technology.

## SMS Communications

SMS communications are subject to the same privacy, security, and data protection requirements that apply to other College information systems. The following requirements govern the collection, use, retention, and protection of mobile phone numbers and SMS consent records used in College-sponsored text messaging communications.

### SMS Privacy Disclosure

Mobile phone numbers and SMS opt-in consent are collected solely for the purpose of delivering the text messages described at the time of opt-in. SMS opt-in data and consent will not be sold, rented, shared, transferred, or disclosed to any third parties or affiliates for marketing or promotional purposes.

We do not share text messaging originator opt-in data or consent with any third parties, except with trusted service providers that assist us in delivering SMS communications (such as messaging platform providers), and only for the purpose of facilitating message delivery and related support services.

### SMS Terms and Conditions

Mohawk Valley Community College may send text messages using an SMS messaging service to communicate with students regarding admissions, enrollment, registration, student services, event notifications, reminders, and other College-related communications

### Opt-In

Individuals may opt in to receive SMS messages by completing an information request form. Consent to receive SMS messages is optional and not a condition of applying, enrolling, receiving services, or participating in College programs. Message frequency may vary.

### Opt-Out

Text STOP to stop receiving text messages. Text HELP for help.

## External Transmission of Sensitive data

Sensitive data must never be transmitted outside of the College system via insecure means, including email and File Transfer Protocol (FTP). The Information Technology Department shall provide secure email and file encryption resources to employees and/or departments for strict compliance of HIPAA and FERPA Privacy Regulations.

## Faculty/Staff Standard Software

- MS-Windows
- MS-Office
- MS-Outlook
- Anti-Virus/Anti-Malware

Employees should contact the Information Technology Helpdesk to arrange for custom software installations. Installation of specialized software is at the discretion of the appropriate supervisor and the Executive Director of Information Technology. Employees are not permitted to perform their own installations without the authorization of the Information Technology Department.

- Personal software shall not be installed on college owned devices.
- Information Technology makes no warranties for the recovery of data stored on local storage devices.
- Employee data should be stored on the allocated network storage (M-Drive or H-Drive).

## Academic Labs Software

- MS-Windows

- OSX (Mac)
- MS-Office
- MS-Outlook
- Anti-Virus/Anti-Malware

Customized software installations in Academic Labs will be configured over summer and holiday breaks to meet the specific curriculum needs. Modifications to customized software in Academic Labs will not be performed after the start of each semester's classes unless authorized by the Executive Director of Information Technology.

## Computer Energy Management - Best Practices

- All employee computers should be "shutdown" at the end of the workday.
- When two (2) hours or more of inactivity is expected, the computer should be shut down or placed into hibernation or standby mode.
- Hard drives should be configured to turn off after 30 minutes of inactivity.
- Computer monitors should be configured to enter power-saving mode after 20 minutes of inactivity.
  Screen savers should not be configured.

## College Issued Laptops

Fulltime faculty members may choose to be issued either a desktop computer or a laptop. Part time employees must provide their own device unless using a desktop on campus.

Fulltime non-teaching staff may request a laptop in lieu of a desktop with a justification that their job requires mobility of their computer. Remote workers will be required to use a laptop which they will transport between locations.

Upon termination of employment from the College, College-issued laptops must be returned to the Information Technology Help Desk as part of the overall College checkout procedure.

If a fulltime faculty member (with a previously issued laptop) moves to part-time employment status, that employee shall relinquish the laptop to the Information Technology Helpdesk.

## College Issued Cell Phones

College-issued cell phones and related mobile devices (e.g., smartphones, tablets, hotspots) are provided to employees who demonstrate an ongoing and legitimate business need for mobile communication. Devices are approved through the appropriate supervisory chain and Office Services, which manages acquisition, configuration, and service plans.

Employees must use College-issued cell phones primarily for official College business. Limited personal use may be permitted when incidental and does not interfere with job responsibilities or incur unnecessary costs to the College.

Employees are expected to:

- Safeguard the device against loss, theft, or damage and report incidents immediately to Office Services.
- Refrain from using devices for illegal, inappropriate, or personal business activities.
- Avoid storing or transmitting confidential College data through unsecured applications or public networks.
- Follow all applicable safety laws, including the use of hands-free options when operating a vehicle.

Office Services may monitor usage, disable or retrieve devices as needed, and will terminate service when the device is no longer required or upon the employee's separation from the College. All College-issued devices and data remain the property of the College and must be returned upon request.

## Mobile Devices Connecting to MVCC email System

Up-to-date personal cell phones and/or other employee-owned mobile devices may connect to the MVCC Email System(s). The Information Technology Department will provide the needed credentials for the connection. The selection, purchase, updating, and configuration of personal cell phones are the responsibility of the end-user. The Information Technology Department will provide reasonable levels of assistance for mobile devices but assumes no liability for their ability to connect and function with MVCC Systems in cases of non-compliant software and hardware.

## Damaged Equipment

Damage to College-issued equipment (laptops, desktop computers, etc.) must be reported to the Information Technology Department Helpdesk. Attempts will be made to repair the equipment; and as required, equipment will be replaced. In the case of damage due to negligence, replacement will not occur until the Executive Director of Information Technology has documented the damage with the appropriate supervisor. Any repayment of replacement costs or other corrective action is at the discretion of the supervisor and the Executive Director of Human Resources.

## Microsoft Office Software for Home Usage

With an MS365 account, active employees can login from any location.

## Disposal and Inventory of Computer Equipment

- At periodic intervals or due to computer obsolescence, campus computers (in offices and academic labs) will be removed and/or replaced by the Information Technology Department.

- The Information Technology will evaluate all equipment to see if it can be used for another College application.
- Information Technology will arrange for the removal of all data from the machine using a hard drive wiping application or degaussing prior to final disposition.
- If appropriate, the Business Office will coordinate the sale or public auction of surplus computers/equipment.
- If old computers are deemed no longer usable, operational, or not fit for public sale or auction (by the Information Technology Department), the Environmental Health and Safety Officer will coordinate with a NYSDEC authorized recycling vendor for removal from the College physical inventory and proper disposal.
- Items to be disposed will be recorded with item description, College asset tag number and item serial number.
- A summary list of equipment to be disposed will be approved by the Executive Director of Information Technology and the Vice President for Administrative Services prior to disposal. Appropriate updates to the Fixed Assets Module in Banner will also be maintained.
- Per requirements of the New York State Office of the State Comptroller, the Environmental Health and Safety Officer will retain all certificates and detailed disposal invoices.
- Equipment will be stored in a secure area prior to its disposal.
- A yearly report of computing assets will be submitted to the Vice President for Administrative Services for insurance purposes.
- All grant purchased equipment sales or disposals must be approved by the Campus Compliance Officer.

## Data Privacy and Software Use

Any person having data representation in a college database has the right to data privacy. There are specific federal and state legal rights involving personal data access, manipulation and dissemination that are afforded to everyone. They address:

- Right of access - "legitimate interest" required in the normal conduct of business
- Manipulation - being accomplished with full knowledge and consent of the file or account owner
- Dissemination of data - only to persons or agencies having a "need to know"

In addition, students have specific rights under the Family Educational Rights and Privacy Act of 1974 including access to their data by themselves and their families. College procedure governing the implementation of the provisions of this Act is detailed in the Student Handbook (“Release of Student Information"). In general, student educational records should be accessible to college faculty and staff when they have a "legitimate educational interest in the data". Personally identifiable information can only be released to other persons or agencies within the limitations described in the procedure.

Data privacy restrictions also apply to the creation and release of student data in response to special external requests outside normal college operations.

They specify that:

- Release of student data must conform to the provisions of the Family Educational Rights and Privacy Act. If there is doubt regarding this, please contact the Registrar.
- Use of the data must have a legitimate educational basis. If in doubt, please contact the Vice President for Learning and Academic Affairs.
- Creation of special lists or reports must not unduly interfere with college operations.

Data requests are handled by the Information Officer, the Vice President for Administrative Services.

There may be a charge for the creation of special lists and reports. The current College charge is $50 per hour for computer personnel and computer time to produce the material plus 10 cents per page for the printout. The rates may be changed by the Vice President for Administrative Services.

## Violation and Enforcement

Individual users are responsible for any violation of any of these procedures that may originate from their computer(s) or account(s). Violations of these procedures may result in disciplinary action, including suspension of privileges, termination of employment, and civil liability. Violations of some portions of this policy may constitute a criminal offense and may result in the engagement of appropriate law enforcement authorities.

## Periodic Review

These procedures shall be reviewed by the Executive Director of Information Technology and the Vice President for Administrative Services on a yearly basis.

In addition to the Mohawk Valley Community College Information Technology Policy and Procedure the College is required to follow the SUNY Information Security Policy.

The Mohawk Valley Community College Incident Response Policy and Information Technology Incident Response Plan have been developed under the SUNY Incident Response Policy.

### Revision History

| Date | Revision Description | Revisions Made by: |
|---|---|---|
| 8.23.24 | Added language to comply with General Data Protection Regulations (GDPR) and the Gramm-Leach Bliley Act (GLBA). | Anne Nolan, Director of Compliance; Mary Jane Parry, Executive Director of Information Technology |

| | | |
|---|---|---|
| 9.16.24<br><br>10.21.24 | Policy appeared as a first reading before the Board of Trustees<br><br>Adopted by the Board of Trustees | |
| 11.13.25 | Added language to cover MVCC issued cellphones | Anne Nolan, Director of Compliance; Mary Jane Parry, Executive Director of Information Technology |
| 9.17.26 | Added section about SMS communication | Suada Ikeljic, Director of Compliance; Anne Nolan, Dean of Institutional Research and Organizational Performance |