Information Technology Procedures Guide (Revision: May 2019)
Reference: Board of Trustees Policy 3.34

AUDIENCE AND SCOPE

Mohawk Valley Community College is committed to providing its employees, students and partners with current technology and computing resources and to protect them from illegal or damaging actions committed, either knowingly or unknowingly, by individuals who use these resources. Therefore, to protect themselves and others, all MVCC employees, students, alumni, contractors, consultants, temporary employees, tenants and guests of MVCC are required to adhere to the 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, that are owned and operated by MVCC, and any equipment directly attached to them (such as personally owned laptops, computers, tablets, smart phones, networking devices, etc.)

TERMS OF COMPUTING & NETWORK USAGE

- It is expected that primary use is restricted to any activity that supports the Mission, Vision and Purpose of the College. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their direct supervisor, the Executive Director of Human Resources, or the Executive Director of Information Technology. MVCC desires to provide reasonable levels of privacy; however, users should be aware that all material and data they create on the College's systems may be requested and possibly disclosed under the Freedom of Information Law (FOIL) or by government subpoena.
- MVCC aspires to provide, but cannot guarantee, a high expectation of electronic privacy in use of its computing and networking systems. All best practice and reasonable anti-intrusion systems and software will be maintained.
- All information stored, processed, or transmitted by electronic devices may be monitored or legally disclosed to appropriate personnel, or law enforcement agencies. Any such monitoring or disclosure shall be conducted for a stated purpose, and will expose confidential information as minimally as possible and only as needed for the stated purpose. The MVCC Executive Director of Human Resources must approve, in writing, the monitoring and/or dissemination of any individual's e-mail communications, web/internet activities or stored data.
- Any information that is considered Personally Identifiable Information (PII) that college procedure indicates is sensitive or confidential must be appropriately protected as described within this procedure.
- MVCC will implement anti-intrusion, anti-virus, anti-SPAM and other appropriate systems in order to provide a secure and private computing environment.
- MVCC reserves the right to block all Internet communications from sites, hosts or devices that are involved in disruptive or damaging practices, or that provide services that may expose the College to legal liability, or that are deemed to not meet the Mission, Vision or Purpose of the College.

- MVCC reserves the right to prioritize the allocation of network resources in times of peak resource demand.
- MVCC makes no warranties of any kind for the access being provided, and assumes no responsibility for the quality, availability, accuracy, nature, or reliability of the material accessed from the internet.
- MVCC will not be responsible for any damages suffered by a user resulting from the use of the Internet. MVCC will not be responsible for any unauthorized financial obligations resulting from the use of the Internet.
- Authorized users are responsible for the security of their passwords and accounts and are responsible for any violation that may originate from their computer or account.
- Personally Identifiable Information (PII) or other sensitive data must not be stored on local hard drives or removable media (including but not limited to floppy disks, PDAs, flash/thumb drives, writable CDs, DVDs, portable hard drives, smart phones, or MP3 players).
- All devices connected to MVCC networks, whether owned by the employee or MVCC, shall have current anti-virus and operating system security patches installed.
- It is the responsibility of employees to physically secure their mobile devices. Any instances of theft of MVCC equipment must be reported to the MVCC Director of Campus Safety and Security for on-campus incidents. For off-campus incidents, it is the responsibility of the employee to report the theft to the appropriate police agency, with a copy of the report filed with the MVCC Public Safety Office.
- MVCC reserves the right to audit networks and systems to ensure compliance with these procedures.

PROHIBITED PRACTICES

The following is expressly prohibited:

- 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.
- Effecting 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 college approval from college presidential cabinet level.
- 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.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- 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 TELECOMMUNICATONS NETWORK ACCESS

Open Usage Computers: Computers in are available for use in Open Labs by all current MVCC students, staff, Board of Trustees members, Emeritus and Retirees of Distinction. A valid MVCC ID Card may be requested for verification. Student, faculty and staff 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, Trustees, Emeritus and Distinguished Retirees are authorized to access MVCC Wireless Networks via their username and password. Using their own devices, guests of the college may request a temporary guest account at the Information Technology Help Desk.

Classroom Ports: Active network ports in classrooms 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 without the approval of the Information Technology Department.

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 / DegreeWorks / 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
- 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
- Advisement (DegreeWorks) – Asst. Dean of Student Enrollment and Advisement
- Banner General – Information Technology Database Administrator

Periodic 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 ("SIRS") - All MVCC employees, past and present, have access for current administrative functions and personal employment data. Former employees' access is limited to viewing historical tax-related forms (W-2, forms, etc.).

MVCC Telecommunication 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
- Emeritus
- Distinguished Retirees
- Retirees, for a period of three years from retirement (and beyond, contingent upon active use)
- Others as approved by the appropriate MVCC Presidential Cabinet Level or the Executive Director of Information Technology.

End-User Accounts – Storage Quotas
Employee / Ex-Employees are allocated 10GB of email storage and 25GB of file storage. Active and Past Students are allocated 2.0 GB of email storage and 15GB of file storage.

Employee Email Address Format(s)
The standard email address format is: *firstname.lastname@mvcc.edu or firstinitial.lastname@mvcc.edu (all lower case)* as determined by the employee 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.

Student Email Address Format
The standard student email address format is: *firstinitial.lastname"birthday day of month"@student.mvcc.edu (all lower case*). 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 Accounts shall be automatically deleted after three consecutive semesters of non-usage.

End-User Account Deletion
Upon notification to the Information Technology Department by a Presidential Cabinet level member or the Executive Director of Human Resources (or designee), an individual employee's Systems / Data access will disabled.

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 five opportunities to enter a correct password. . If s/he does not enter the correct password after five tries the account will be locked and s/he will be prompted to contact the Information Technology Help Desk for a reset.

Sharing account information
A user should not share his/her account password with others or allow use of his/her account by others, with the exception of 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.

Locking machines
For security of data, end-users should "lock" their computers when leaving their work stations.

Connecting personal equipment to the network
Personal equipment is not allowed to be connected to the MVCC network with the following exceptions:

Virtual Private Network (VPN) - Computers that connect to the MVCC networks from offsite using a Virtual Private Network must have virus protection installed and be current with all patches or updates for the operating system. By using a VPN, users agree that their computers may be remotely inspected to verify the presence of virus protection and patches or updates. Computers may be denied access via a VPN should the virus protection be deemed to be inadequate or it is discovered that patches or updates are missing.

Change of Job Duties
In the event that an employee changes jobs within the College, access to computer network resources related to their old job will be discontinued. If access from their former job is still required, 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 MS-Windows 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.

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 10
- MS-Office 2018
- MS-Outlook 2018
- Internet Explorer11

Employees should contact the Information Technology Help Desk 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.

Installation Technology makes to 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-Windows10
- OSX (Mac)
- MS-Office 2018
- MS-Outlook 2018
- Internet Explorer11

Customized software installations in Academic Labs will be configured over summer and holiday breaks to meet the particular 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 MANANGEMENT – 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 shutdown 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.

TELECOMMUTING

Telecommuting is defined as the "ability to work at home (or other remote location) using a computer or mobile device connected to the MVCC Data Network, servers and its software". All special telecommuting requests must be approved by the appropriate supervisor and the Executive Director of Information Technology. All reasonable software, hardware, security and support considerations will be provided upon approval of such requests; under the assumption that telecommuting is considered a courtesy and not a mandated employee right.

COLLEGE ISSUED LAPTOPS

Fulltime faculty members may choose to be issued either a desktop computer or a laptop. Part time employees may request a loaner laptop from the MVCC Media Center (pending availability).

Fulltime non-teaching staff may request a laptop in lieu of a desktop with a justification that their job requires mobility of their computer.

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 Help Desk.

MOBILE DEVICES CONNECTING TO MVCC EMAIL SYSTEMS

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 and configuration of personal cell phones are the responsibility of the end-user. End-users should be aware that optimal configurations will occur if the phone is compatible with MS-Exchange Server 2018. 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

Full-time active employees may request a licensed version of MS-Office for working at home. Software installation and all potential risk to personally owned systems is the responsibility of the requesting employee. Before the software is issued, the requesting employee must sign an affidavit that the issued software (to be installed on non-MVCC equipment) will be used for MVCC-related business needs; this form must also be signed by the appropriate supervisor, indicating approval.

Retiree Email Accounts

Upon retirement from the college, in agreement with their supervisor, retirees may opt for one of the following email account configurations to be in place for a period of three years from date of retirement. At the conclusion of year three, the retiree's email account shall be closed.

OPTION #1:

The retiree's email account will remain active and the retiree will monitor incoming emails.

Upon receipt of email applicable to college business, the retiree will forward the email to their supervisor.

OPTION #2:

Incoming emails to the retiree's account will be auto-forwarded to a designee specified by the retiree's supervisor. The retiree will continue to have access to the email account and the incoming emails.

OPTION #3:

Incoming emails to the retiree's account will be auto-forwarded to a designee specified by the retiree's supervisor. The retiree will no longer have access to the email account and the incoming emails.

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.
- IT will evaluate all equipment to see if it can be used for another College application.
- IT will arrange for the removal of any and 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 decal 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 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 Computer Assets will be submitted to the Vice President for Administrative Services for insurance purposes.

DATA PRIVACY AND SOFTWARE USE

Anyone 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 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/ 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 Affairs on a yearly basis.