

Delaware Valley College Information Security Policy

Delaware Valley College has developed an Information Security Policy to ensure that business objectives are accomplished in a secure and timely manner, while safeguarding college information assets. The policy has been developed to address security requirements for the current available technology and environment.

The purpose of this policy is to ensure that users of Delaware Valley College's information systems:

- Experience uninterrupted access to administrative data and systems
- Trust the integrity of administrative data and systems
- Trust that sensitive information is treated with care

The Information Security Policy is a work in progress, and as such, will be altered as needed to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.

The Information Security Group, comprised of the Director of Technology Services, Network Security Administrator, Network Administrator, and Server Administrator will review the Information Security Policy and make recommendations for change. These recommendations will then be presented to the Information Systems Planning Committee for review.

The Information Security Policy contains the following sections:

- Confidentiality Notice
- Physical Security
- General Security
 - General Policies
- System Security
 - General System Security
 - Password Security
 - Desktop Services Security
 - Server Security
 - Virus, Hostile, and Malicious Code Security
 - Internet Acceptable Use Policy
 - Configuration Management
- E-Mail Security
- Network Security
 - General Network Security
 - Intranet Security
 - Internet Access/Firewall Security
 - Remote Access Security

Confidentiality Notice

Any employee whose position requires interaction with the College's administrative information system may be provided with direct access to confidential and valuable data. In the interest of maintaining the integrity of this system and ensuring the security and proper use of College resources, employees must:

- Maintain the confidentiality of passwords.

- Maintain in strictest confidence the data to which they have access. Any confidential information must not be shared in any manner with others who are unauthorized to view such data.
- Use access to the College's systems for the sole purpose of conducting official business of the College. Understand that the use of these systems and their data for personal purposes is prohibited.
- Understand that any abuse of access to the College's systems and their data, any illegal use of copying of software, or any misuse of the College's equipment may result in disciplinary action and loss of access to the College's systems.

Physical Security

Technology Services is located in the basement of the Feldman Building, rooms 5 and 6. Feldman 6 houses the server room and central network equipment. The Feldman Building is typically locked between the hours of 10:00pm and 7:00am. All Technology Services staff members have access to the building by key. All Technology Services staff have access to Feldman rooms 5 and 6 by key and combination lock. Servers are housed in a secured server room which can only be accessed by authorized personnel. The server room has separate air conditioning units, and all servers and network equipment are protected by UPS units.

General Security

The General Security Policy forms the foundation of the College's Information Security Policy. This set of policies enables Technology Services to manage the security of information and maintain accountability. These policies provide the framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use Delaware Valley College information assets.

The General Security Policy applies to all employees, contractors, vendors, and anyone using Delaware Valley College assets. These policies are the organizational mechanism used to manage the confidentiality, integrity, and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by Delaware Valley College.

Violators of any policy are subject to disciplinary actions including loss of access to the College's computing systems, termination and/or civil and criminal legal action.

General Policies

1. All information systems within Delaware Valley College are the property of Delaware Valley College and will be used in compliance with Delaware Valley College policy statements.
2. Any personal information placed on Delaware Valley College information system resources becomes the property of Delaware Valley College.
3. Any attempt to circumvent Delaware Valley College security policy procedures (e.g. disconnecting or tunneling a protocol through a firewall) is strictly prohibited.
4. Unauthorized use, destruction, modification, and/or distribution of Delaware Valley College information or information systems is prohibited.
5. All users will report any suspicious activity found on Delaware Valley College information systems to the Technology Services department immediately upon detection.
6. Delaware Valley College information systems and information will be subject to monitoring at all times. Use of Delaware Valley College information systems constitutes acceptance of this monitoring policy.
7. All policy statements will be reviewed quarterly and updated as required.

8. Use of any Delaware Valley College information systems or dissemination of any information in a manner bringing disrepute, damage, or ill will against Delaware Valley College is not authorized.
9. Release of Delaware Valley College information will be in accordance with Delaware Valley College policy statements.
10. Users will not attach their own computer or test equipment to Delaware Valley College computers or networks without prior approval of the Technology Services department.

System Security

The System Security Policy applies to all Delaware Valley College employees, contractors, vendors, and any other person using or accessing Delaware Valley College information or information systems. Exceptions to this policy must be approved by the Security Administrator.

Authorized users must comply with the following policies:

General System Security

General system security covers the set of procedures appropriate for controlling changes to a system's hardware and software structure to ensure that changes will not lead to violations of the Delaware Valley College systems security policy.

1. All College systems will be configured in accordance with the appropriate security implementation standards.
2. Stringent access controls will be used to secure information systems (e.g. log on, password security, screen saver).
3. Passwords must conform to the Delaware Valley College Password Security Policy.
4. Information systems will not be used for personal gain.
5. Copyright and licensing agreements will not be violated.

Password Security

Poorly selected, reusable passwords represent one of the more vulnerable aspects of information security. Delaware Valley College authorized users must comply with creation, usage, and storage policies to minimize risk to college information.

1. All system accounts must be assigned a unique user ID and password that are protected in accordance with college password policy statements.
2. All initial system accounts will be set up by the Technology Services department.
3. If group accounts and passwords are utilized, they will only be provided to individuals that require access to shared data.
4. Passwords will be a minimum of 12 characters and must contain 3 of these 4 items – uppercase letter, lowercase letter, number, or symbol.
5. Sharing of passwords is prohibited.
6. Users are prohibited from logging into systems for other users.
7. Users will disclose the passwords to authorized personnel only after positive identification has been made of the requesting person.
8. Any suspicious queries regarding passwords will be reported to the Technology Services department.
9. Passwords will be protected as Delaware Valley College proprietary information. Posting passwords or storing them in an unsecured area (e.g.. in desk drawers, under keyboards) is prohibited.
10. Using programs or scripts that include system passwords is prohibited. For example, if a user has automated the login process so that typing in password and user ID is avoided, an intruder may steal that program and impersonate the user. The user will then be held responsible for any damage or theft that may occur.

11. Users must change passwords every 60 days and may reuse passwords only after 14 different passwords have been used. After changing their password, users must wait at least 1 day before they will be allowed to change it again.
12. Accounts will be locked out after 5 failed password attempts in a 30 minute time period. Accounts can be reset by contacting the Technology Services department.
13. Network Administrators will enforce required password changes out of cycle for certain security events that have the potential for security compromises (i.e. employee relocation, intrusion attempt, or employee termination).
14. Passwords will be changed within 24 hours after a possible compromise.
15. When users leave the organization, their accounts will be immediately disabled or deleted.
16. If a user leaving the organization was a privileged user, system passwords will be changed within 1 day.

Desktop Services Security

The Delaware Valley College Desktop Services Security Policy addresses the authorized and legitimate use of hardware, operating systems, software, networks, file servers, and other peripherals used to access any Delaware Valley College information system.

1. Access controls:
 - a. Systems that support automatic log-off or screen lock will use these tools with an activation time not more than 20 minutes.
2. System configuration:
 - a. A baseline copy of operating systems and initial software loads for desktop computers will be maintained by the Technology Services department.
 - b. Prior approval of the Technology Services department will be obtained for communication configuration changes (e.g. network addresses or names).
 - c. Before connecting to any system or network, the desktop system will have a 'least privilege' access control configuration.
3. Security monitoring:
 - a. All Delaware Valley College systems and network activities will be subject to security monitoring. Use of Delaware Valley College systems and networks constitutes consent to this monitoring.
 - b. Disabling or interfering with virus protection software is prohibited.
 - c. Disabling or interfering with logging, auditing, or monitoring software is prohibited.
 - d. All Delaware Valley College desktop services will be subject to inventory and inspection.
 - e. Security irregularities, incidents, emergencies, and disasters related to Delaware Valley College information or systems will be reported to the Technology Services department immediately.
4. System usage:
 - a. Sabotage, destruction, misuse, or unauthorized repairs are prohibited on Delaware Valley College information systems.
 - b. The Technology Services department will authorize all repairs.
 - c. Desktop resources will not be used to compromise, harm, destroy, or modify any other services or resources (internal or external).
 - d. Desktop resources will not be used in the presence of environmental threats such as the presence of water, excessive static electricity, or fire.
 - e. All data on information systems at Delaware Valley College is classified as college proprietary information.
 - f. Storage, development, or the unauthorized use of tools that compromise security (i.e. password crackers and network sniffers) is prohibited.
5. No software will be installed on a computer without the approval of the Technology Services department.

6. Unauthorized copying or distributing of copyrighted software is a violation of federal copyright law and will not be permitted.
7. Personal software will not be installed on any Delaware Valley College machine.
8. Users will not allow non-employees to use any Delaware Valley College machine or device.

Server Security

Delaware Valley College recognizes that a secure server safeguards the Delaware Valley College information systems by requiring authentication for server access, encrypting private information, and protecting the integrity of data.

1. Server access controls:
 - a. Each user will have a unique, non-anonymous user ID.
 - b. In order to achieve a consistent and unique username representation, the college standard for account names is Last Name+First Initial.
 - c. Systems that support automatic log-off or screen lock will use these tools with an activation time not more than 20 minutes.
 - d. Only members of the Technology Services department who have appropriate training or experience will have administrative rights to college servers.
 - e. Guest accounts will not be enabled on any college server.
2. Server configuration:
 - a. A baseline copy of operating systems and initial software loads for server resources will be maintained by the Technology Services department.
 - b. Users shall only be given access to those services and files on the server that they need access to in order to perform their job functions.
 - c. Users will be given access to servers through groups to ease administration and to help enforce security.
 - d. Virus protection software will be installed on all systems in accordance with the Virus, Hostile, and Malicious Code Security Policy.
 - e. Only services necessary on the server shall be installed to minimize risk.
3. Server security monitoring:
 - a. All Delaware Valley College server services will be subject to inventory and inspection.
 - b. The Information Security Group will monitor available news sources for information about availability of new releases of, or patches for, server software.
 - c. The Information Security Group will monitor available news sources for information about vulnerabilities in server software and how to patch or work around those vulnerabilities.
 - d. New releases or patches for server software will be evaluated by the Information Security Group before implementation.
 - e. New releases or patches for server software will only be obtained from the vendor or another trusted source.
4. Server usage:
 - a. All data on information systems at Delaware Valley College is classified as college proprietary information.
 - b. Old user files, such as archived e-mail, will be reviewed quarterly and may be destroyed. Only files and e-mail identified as critical will be stored indefinitely.
 - c. Network and system servers will not be used as end user workstations.
5. All data stored on college servers shall be backed up according to the backup policy.

Virus, Hostile, and Malicious Code Security

The intent of this policy is to better protect Delaware Valley College against attack from destructive or malicious programs.

1. Any public domain, freeware, or shareware software will be evaluated by the Information Security Group prior to being installed on any college resource.
2. System users will not execute programs of unknown origin because they may contain malicious logic.
3. Only licensed and approved software will be used on college computing resources.
4. All licensed software will be write-protected and stored by the Information Security Group.
5. Delaware Valley College users will scan all files introduced into its environment for virus, hostile, and malicious code before they are used.
6. The Technology Services department will ensure that Delaware Valley College obtains and deploys the latest in virus protection and detection tools.
7. Delaware Valley College users will not disable or circumvent Delaware Valley College antivirus protection.
8. All information systems media (disks and CD-ROMs), e-mail, and Internet file transfers will be scanned for virus, hostile, and malicious code.
9. All users will report any suspicious occurrences to their supervisors or the Technology Services department immediately.
10. Permissions of directories containing executable files will be set to read and execute (not write) whenever possible.
11. All college systems will be protected by a standard virus protection system.
12. Virus protection engines and/or data files will be updated on a weekly basis.
13. Viruses that are detected on a user's workstation will be reported to the Technology Services department immediately for action and resolution.
14. Anomalous behavior of any software program will be reported to the Technology Services department immediately.

Internet Acceptable Use Policy

The personnel policy for administrators, faculty and staff concerning E-Mail and Internet Use is below.

Because of the unique nature of e-mail/internet, and because of the College's desire to protect its interests with regard to its electronic records, the following rules have been established to apply to all agents of the College, including but not limited to administrators, faculty, staff, student employees, non-paid volunteers, adjunct faculty and independent contractors. Faculty policy regarding the use of Delaware Valley College 's e-mail and internet systems is as agreed upon in the Collective Bargaining Agreement.

Definitions

Electronic mail ("e-mail") is defined as an office communications tool whereby electronic messages are prepared, sent and retrieved on personal computers.

On-line services (i.e., the internet, the web) are defined as a communications tool whereby business information, reference material and messages are sent and retrieved electronically on personal computers.

Policy and Procedures

1. Delaware Valley College 's e-mail and internet system is intended to be used for business purposes, including dial-in access from off-campus.
2. Delaware Valley College 's e-mail and internet system is the property of the College, and the employees of the College have no personal privacy rights with respect to messages created, received or sent from the College's e-mail and Internet system. The College reserves the right to monitor all stored e-mail and internet files without notice. Further, the College must have access to the entire system for emergencies and maintenance.
3. All e-mail/internet records are considered College records and should be transmitted only to individuals who have a business need to receive them. Additionally, as College records, e-

mail/internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other legal process. Consequently, employees should always ensure that the business information contained in e-mail/internet messages is accurate, appropriate and lawful. Delaware Valley College reserves the right to disclose employee e-mail messages and internet records to law enforcement or government officials or to other third parties, without notification to or permission from the employees sending or receiving the messages.

4. No e-mail messages/internet records should be created or sent which may constitute intimidating, hostile or offensive material on the basis of sex, gender, race, color, religion, national origin or disability. The College's policy against sexual or other harassment applies fully to the e-mail/internet system.

5. Abuse of the e-mail or internet systems, through excessive personal use, or use in violation of law or College policies, will result in disciplinary action, up to and including termination of employment. All persons to whom these rules are applicable, as stated above, are responsible for adhering to these rules. Discipline for violation of the law or the policy by members of the faculty bargaining unit will be administered pursuant to the Collective Bargaining Agreement. All supervisory personnel are responsible for ensuring that these rules are adhered to within their respective areas of responsibility.

Configuration Management

This policy provides for the identification, control, accounting for, and auditing of all changes to system hardware, software, firmware, documentation, test plans, test results, communications interfaces, operating procedures, and installation structures throughout the development and operation of the system.

1. Installation of new software, especially operation system upgrades and/or patches, will be reviewed prior to installation.
2. Relocation of information systems will be approved by the Technology Services department.
3. As-installed/implemented documentation will be developed and maintained for all college systems by the Information Security Group.
4. All system users will promptly report any identified/discovered vulnerabilities to the Information Security Group.
5. All system maintenance will be performed by authorized personnel.
6. If off-site maintenance is required for a system or system component(s), all non-public information will be removed prior to sending the device off-site.
7. If a remote diagnostic capability is required, access should be physically disconnected (if possible) until needed.
8. All maintenance activity requiring system access (log-in) will be audited.
9. All maintenance personnel will be identified to ensure they are authorized to gain access to any college system.

E-Mail Security

The Delaware Valley College E-mail Security Policy specifies mechanisms for the protection of information sent or retrieved through e-mail. In addition, the policy guides representatives of Delaware Valley College in the acceptable use of e-mail. For this policy, e-mail is described as any computer-based messaging, including notes, memos, letters, and data files that may be sent as attachments.

The E-Mail Security Policy applies to all Delaware Valley College employees, contractors, vendors, and any other person using or accessing Delaware Valley College information or information systems. Exceptions to this policy must be approved by the Technology Services department.

Policy

1. Access controls:
 - a. Access to e-mail will be password protected and all Delaware Valley College Password Security Policy line items apply.
 - b. All e-mail on the Delaware Valley College information systems, including personal e-mail, is the property of Delaware Valley College.
 - c. Users terminated for cause will have all e-mail access blocked, including forwarding to new addresses.
 - d. No user is authorized to open or read the e-mail of another without written permission of the account holder.
 - e. Remote users of e-mail will employ encryption if they access across non-Delaware Valley College networks (i.e. the Internet).
 - f. E-mail is provided to the users and contractors of Delaware Valley College to enhance their ability to conduct Delaware Valley College business.
 - g. Items in users' Deleted Items folders will be automatically deleted after 30 days.
 - h. Items in users' Junk Mail folders will be automatically deleted after 10 days.
2. Content:
 - a. Use of profanity, inappropriate language, pornography, or slanderous, misleading content in e-mail is prohibited.
 - b. Use of e-mail to spam (e.g. global send, mail barrage) is prohibited. This includes the forwarding of chain letters.
 - c. Use of e-mail to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin, or any other category.
 - d. Use of e-mail to send unprofessional or derogatory messages is prohibited.
 - e. Forging of e-mail content (e.g. identification, addresses, etc.) is prohibited.
3. Usage:
 - a. Any e-mail activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
 - b. When a user receives e-mail error messages that appear to be abnormal, they will be saved and reported to the Technology Services department.
 - c. When sending e-mail, users should verify all recipients to whom they are sending e-mail messages.
 - d. Users should understand that e-mail could be altered during transmission from the sender to the receiver, and the identities of the sender or receiver could be falsified. Users should apply common sense when assessing whether e-mail is legitimate.
 - e. Deleting an e-mail message does not necessarily mean it has been deleted from the system.
 - f. Users should apply common sense when writing and sending e-mail messages.

Network Security

The purpose of this policy is to establish a comprehensive set of network security standards for Delaware Valley College. Network security is crucial for maintaining the integrity of the data that Delaware Valley College relies on for everyday operations. Delaware Valley College network administrators have the primary responsibility for implementing and ensuring adherence to this policy; however, all employees have a responsibility to protect the integrity of the Delaware Valley College computing network.

The Network Security Policy applies to all Delaware Valley College employees, contractors, vendors, and any other person using or accessing Delaware Valley College information or information systems. Exceptions to this policy must be approved by the Technology Services department.

General Network Security

General network security covers the protection of networks and their services from unauthorized modification, destruction, or disclosure. This provides assurance that the network performs its critical functions correctly and there are no harmful side effects. It also provides for information accuracy.

1. Accounts will be considered inactive after 30 days without a valid login. Inactive accounts are subject to deletion. All files will be deleted after an additional 90 days. The manager of a former employee must review all files belonging to that user and notify the Technology Services department of any files that will be retained.
2. No staff or full-time faculty account will be created without written notice from Human Resources.
3. All other accounts (i.e. adjunct faculty, workstudy) require supervisor approval.
4. Users who do not need access to their accounts for a period of 13 weeks or more will have their accounts disabled.
5. No unauthorized user login scripts will be used on the network. Only group, container, and profile login scripts will be used.
6. Network restrictions will apply in special cases to restrict an account to a specific workstation. Normal users will not have workstation restrictions. No time-of-day restrictions will be used.
7. Normal accounts will not have expiration dates. Expiration dates will be used in special cases (e.g. when a consultant has a time-dependent contract).
8. The administrator account will not be for general use. Network administrators will use their own login accounts whenever possible.
9. Account rights and privileges will be limited to what is necessary for a user to perform his or her function. Written permission may be required from the user's supervisor.
10. All files stored in common directories will be subject to deletion at any time. The responsible supervisor should review files stored in common directories monthly. Supervisors should delete any unnecessary files.
11. Files stored in a user's home directory cannot be accessed or viewed by another user without the originating user's written permission.
12. Rights to the file system should be assigned on an as-needed basis. Only the minimum rights necessary to accomplish a task should be issued.

Intranet Security

The Intranet contains sensitive company information for Delaware Valley College. This information is critical to the business needs of the college and needs to be protected from external access. The following policies are to be adhered to by all authorized users:

1. All Intranet servers must comply with the Internet Access/Firewall Security Policy.
2. Only authorized personnel may access information stored on Intranet servers.
3. Intranet servers store college proprietary data and must be secured accordingly.
4. Information stored on and used from Intranet servers is for business use only.
5. Remote access to college Intranet servers is prohibited.
6. Only authorized browsers may be used to access any Intranet site.
7. Software used to create or modify the Intranet site must be approved by the Technology Services department.

Internet Access/Firewall Security

The Delaware Valley College firewall is a gateway that limits access between networks in accordance with Delaware Valley College Internet Access/Firewall Security Policy. This system, or combination of systems, enforces a boundary between two or more networks. All traffic from

the inside-out and outside-in must pass through it, and only authorized traffic is allowed to communicate.

1. All Internet users will immediately notify the Technology Services department of any suspicious activity.
2. Unless the Technology Services department waives firewall use to support Delaware Valley College operational needs, all Internet access will be accomplished through approved firewalls and security processes.
3. Firewalls will be placed between the Delaware Valley College network and the Internet to prevent unauthorized access to the Delaware Valley College network.
4. All users requiring Internet access from the Delaware Valley College network will only be provided that access through Delaware Valley College firewalls.
5. If the firewall fails, it will fall back to a configuration that denies all connections.
6. Failed firewalls will be returned to service by authorized personnel only.
7. Firewalls will be configured to transparently pass outbound connections.
8. Appropriate firewall documentation will be maintained offline at all times.
9. New releases of patches for firewall software will be evaluated by the Network Security Administrator before implementation.
10. New releases of patches for firewall software will only be obtained from the vendor or another trusted source.
11. The Network Security Administrator will monitor available news sources for information about vulnerabilities in firewall software and how to patch or work around those vulnerabilities.
12. The Network Security Administrator will monitor available news sources for information about availability of new releases, or patches for firewall software.
13. Remote administration access to all firewalls over untrusted networks will use strong authentication.
14. Any connections to trusted external networks (e.g. VPN connections) that pass through Delaware Valley College firewalls will comply with all other policy statements applicable to external network connections.
15. Strong authentication will be required for access through the firewall to any internal systems.
16. Firewall configuration changes will be approved by the Information Security Group before being implemented.
17. Details of the Delaware Valley College internal network should not be visible from outside the firewall.
18. Firewalls will run on dedicated systems; only software or services essential to firewall operation will be installed or run.
19. Systems that provide public network services (e.g. web servers, mail servers, name servers, etc.) will be placed on an intermediate network (Demilitarized Zone – DMZ). All access to the intermediate network, whether originating from an internal or external network, will pass through a firewall.
20. Physical access to firewalls will be limited to members of the Technology Services department.
21. Firewalls will perform Intrusion Detection Service functions.

Mobile Device Security

Technology Services defines a mobile device as any portable system that can store data. This includes but is not limited to the following devices.

- Laptop Computers
- Blackberry's
- PDAs (Palm Pilots, etc...)
- Some mobile phones (Text Messaging, email and memory cards)
- USB/Flash/Thumb drives, Memory Cards

Mobile devices provide important functionality, allowing Delaware Valley College faculty and staff to have their computing resources at hand in meetings/classes, those who travel on College business to be maximally functional and productive while away, and those who occasionally work at home to eliminate duplication of resources, files, etc. Unfortunately, mobile devices that are lost as a result of theft or accident can leave the College at risk. The possible loss to the College could be substantial and includes losses in dollars, productivity and reputation. This policy addresses the actions that must be taken in order to minimize the risk of the theft of College-owned mobile devices and the associated data that belongs to the College.

This policy applies to all faculty and staff who use a College owned mobile device. These individuals are hereinafter referred to as "caretakers." Each caretaker of a College-owned mobile device is responsible for the security of the device, regardless of whether the device is used in the office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport.

Physical Security

Mobile Devices in Campus Offices

A caretaker of College-owned mobile device will secure the room in which the device is being used if it becomes necessary to leave the device unattended. If the caretaker is unable to secure the room a security cable should be used to attach a device, like a laptop, to an immovable object, typically a desk. Technology Services will provide placement advice and installation as well as help you purchase the appropriate cable.

Mobile Devices Out of Campus Offices

When a caretaker takes a mobile device out of his/her office, s/he is expected to keep the laptop in hand, in sight or in a secure and locked location at all times.

- Mobile devices should not be left in an unattended vehicle, even for a short period of time.
- Special care should be taken in particularly vulnerable locations like airports, conference centers, hotels and coffee shops.

If it is inappropriate or impractical to secure a mobile device in a given situation, it is the caretaker's responsibility to take all reasonable steps to minimize the risk of loss of the device.

Password-protect your mobile device

Physical security is a major concern for mobile devices. If your mobile device is lost or stolen, a device password may be all that stands in the way of someone reading your email and other sensitive data. Most devices have some type of password protection. For example, a laptop would require a logon password and a Blackberry can be set with a lockout password.

When selecting a password, please choose a strong password. The security of your system is only as strong as the password you select to protect it. You should have a complex password. This would include some combination of letters, numbers and symbols. It should also be reasonably long and be changed every couple of months.

Sensitive Data

Sensitive data includes, but is not limited to, financial information, the personal information of the faculty, staff and students, information that could compromise a business partner, medical data and intellectual property that belongs to the College. If the caretaker believes that the data that is on his/her mobile device falls into this category, the College's Network Security Administrator should be contacted to discuss options that are available. These options may include data encryption schemes or just a change in a procedure.

Software

All College laptops are delivered to the caretaker with certain software that the College has a license to use. This software includes but is not limited to Microsoft Office and virus protection.

The caretaker is not permitted to install or change any of this software. Putting unlicensed software on College-owned computers may make a system unstable or even create legal issues for the College if the software is deemed illegal. Uninstalling security software or virus protection is not acceptable for any reason. If you have questions or concerns regarding this software, please contact the College's Network Security Administrator.

PDA's are also potentially at risk for viruses. While the risk is minimal at the current time, it is only a matter of time until this threat becomes more prevalent. In an effort to prevent security issues, these devices should have up to date virus protection installed. Antivirus software is available for various mobile platforms. Please contact Technology Services if you have any questions or need any software recommendations regarding these devices.

Wireless Security

When connecting to wireless networks, at home or at other remote locations, it is the caretaker's responsibility to ensure that encryption is being used to protect the data that is being transmitted. Wi-Fi Protected Access (WPA or WPA2) is the most secure method of securing wireless data. Wired Equivalent Privacy (WEP) is an older and much less secure method of securing wireless data. WEP is still better than no encryption but it should be avoided if possible. If you have questions regarding wireless security, please contact Technology Services.

Laptop Tracking and Recovery

All laptops must be purchased through Technology Services. Effective April 2007 all new laptops will have College approved asset tracking and recovery software installed on them. Some laptops purchased previously are eligible for this software. Technology Services will contact you your laptop qualifies.

This software also gives the College the ability to delete all data on your lost or stolen laptop. This will be done after a laptop is reported stolen.

Reporting a Theft or Loss

If a College-owned mobile device is stolen or lost, its caretaker is expected to immediately file an Incident Report with the Office of Public Safety and Security. The Director of Technology Services should also be notified of the loss. Along with reporting the loss of the equipment, the caretaker should report the loss of any data that puts the College at risk. This data includes, but is not limited to, financial information, the personal information of the faculty, staff and students, information that could compromise a business partner, medical data and intellectual property that belongs to the College.

All of the above requirements can help mitigate the risks to the College but they are not a panacea. Due diligence and common sense are still the best tools to use when it comes to preventing data loss. If you have questions, comments or suggestions regarding mobile device security, please contact Technology Services.

Remote Access Security

Delaware Valley College provides remote access to employees with a valid requirement for telecommuting. Additionally, vendors and contractors may be granted remote access to further Delaware Valley College business if they comply with access requirements and any additional restrictions deemed necessary by Delaware Valley College. This service is a shared resource. Employees are asked to use good judgment and be considerate of the needs of others when using this service.

1. The following statements are for the Trusted User Community:

- a. Virtual Private Network (VPN) and dial-up remote access is only authorized through equipment and methodologies approved by the Technology Services department.
 - b. Any sensitive data (see **Sensitive Data Security** below) will be secured through the use of approved encryption methods.
 - c. All data that is downloaded to a remote computer should be removed after it is no longer needed. The downloaded files should also be cleared from the Recycle Bin or whatever disposal method is used by the operating system on the computer.
 - d. Passwords used for remote access will comply with the Password Security Policy. These passwords will be changed semi-annually.
 - e. When possible, passwords for remote access will be different than those used for desktop services.
 - f. Remote access usernames and passwords will be unique to individuals and will not be shared.
 - g. The Technology Services department will ensure only valid remote access points exist.
 - h. Positive identification of authorized users will be obtained before resetting passwords and access controls.
 - i. The Technology Services department will review and revalidate a user's requirement for remote access periodically.
 - j. It is prohibited to remotely dial into Delaware Valley College from a system simultaneously attached to any other network without authorization from the Technology Services department.
2. The following statements are for the Untrusted User Community:
- a. All users will comply with all the trusted access requirements, unless otherwise approved by the Network Security Administrator.
 - b. All users will be responsible for ensuring that any computers that are connected to the Delaware Valley College networks are free of viruses or any other damaging software.
 - c. When remote access is no longer required, the user or supervisor will notify the Technology Services department within one business day in order to discontinue access.
 - d. Remotely accessible services will be limited to the minimum set required to support the business objectives of Delaware Valley College.

Wireless Security

When connecting to wireless networks, at home or at other remote locations, it is the caretaker's responsibility to ensure that encryption is being used to protect the data that is being transmitted. Wi-Fi Protected Access (WPA or WPA2) is the most secure method of securing wireless data. Wired Equivalent Privacy (WEP) is an older and much less secure method of securing wireless data. WEP is still better than no encryption but it should be avoided if possible.

Sensitive Data Security

The loss of sensitive data to the College could be substantial and includes losses in dollars, productivity and reputation.

Sensitive data includes, but is not limited to:

- Financial information
- The personal information of the faculty, staff and students
- Information that could compromise a business partner
- Medical data and intellectual property that belongs to the College

No sensitive data should be stored on non-College-owned computers. This includes data transferred by disk, USB key or remote access/VPN solution. Please refer to the College's Sensitive Data Protection Policy for much more information.

If a data owner believes that the data that is on his/her laptop/computer falls into this category, the College's Network Security Administrator should be contacted to discuss options that are available. These options may include data encryption schemes or just a change in a procedure.

Revision Changes:

February 13, 2007-Adjusted for all mobile devices-Mike Davis

November 14, 2006-Information Security Policy created-Mike Davis