

Eastern Shore Community College

Information Technology Security Policy

Table of Contents

Introduction.....	1
Objectives	1
Roles and Responsibilities	2
Review Cycle	2
Policies and Procedures	
System Accounts.....	3
Physical Security of Equipment.....	5
Software / Data Security	6
Personnel Security	10
Penalties for Non-Compliance	10
Exception Handling	11
Glossary of Terms.....	12
Contact Information	13

Introduction

Every user of information technology resources at Eastern Shore Community College (ESCC) is entrusted with the protection of those assets. From the president of the college to the casual visitor to our campus, every user must be held accountable for those resources to which he has been granted access.

In order for the protection of ESCC's information technology resources to be most effective, faculty, staff, and students must have specific written guidelines to follow. This document contains the policies and procedures established at ESCC in order to safeguard the college's sensitive and critical information technology resources.

Objectives

The Eastern Shore Community College Information Technology Security Policy and Procedures document is intended to

- provide clear, written guidelines to members of the ESCC community that define acceptable and unacceptable local security practices.
- protect sensitive data from unauthorized access.
- protect critical systems from damage or compromise.
- ensure that no illegal or unethical use of local or state systems occurs.
- establish guidelines for handling intentional and unintentional violations of security policy.
- demonstrate the commitment of ESCC's upper management to effective information technology security practices.

Roles and Responsibilities

Ultimate authority over and responsibility for ESCC information technology security reside with the college president. The designated Information Technology Security Officer bears responsibility for recommending and implementing the policies and procedures to monitor and protect ESCC's information technology resources. In addition, the Security Officer is responsible for sharing up-to-date security information with the ESCC community. Currently, the Information Security Officer is the IT Coordinator.

Access to information technology is a privilege that must be taken seriously and guarded responsibly by all users at ESCC. Members of the Information Technology Department staff are expected to be especially diligent in the enforcement of the college's information technology security procedures. Users, including students, faculty, staff, and guests, are expected to adhere to ESCC's information technology security policy in order to protect those resources to which they have access.

Review Cycle

In order to keep ESCC's Information Technology Security Policy most effective, the policy and procedures will be reviewed and updated as necessary annually. The document should be reviewed by the appropriate college committees, college personnel, and the president. The review should be completed prior to June 1 of each year.

Policies and Procedures

1. System Accounts

Policy

- 1.1 Users must be granted the lowest level of access required to perform their roles at ESCC.

Procedures

- 1.1.1 Students are granted a local network account with the permissions and privileges required by the classes or programs in which they are enrolled.
- 1.1.2 Student local network access will be revoked upon withdrawal from all classes or completion of personal objectives, such as graduation or an extended period of time without enrollment.
- 1.1.3 Visitors and guests are allowed access to generic accounts with appropriately restricted user access only on public kiosks or other workstations approved by the IT Security Officer.
- 1.1.4 Employees are granted local and state network accounts as appropriate for their job responsibilities.
- 1.1.5 All account owners are provided with training or information regarding acceptable and unacceptable security practices.
- 1.1.6 All account owners are subject to the ESCC/VCCS Ethics Agreement, which is summarily displayed on all workstations upon login, published in the ESCC Catalog and Student Handbook, and posted in public access areas throughout the college.
- 1.1.7 Administrative access is restricted to designated IT staff.
- 1.1.8 IT staff use administrative access only as required to perform system setup and maintenance.

Policy

- 1.2 The IT Security Officer must conduct a regular review of all account access rights.

Procedures

- 1.2.1 At a minimum, the IT Security Officer will conduct a thorough review of local and state account access annually.
- 1.2.2 Auditable records of account reviews must be maintained for a three-year review cycle.
- 1.2.3 Accounts that have not been used within a twelve-month period are disabled unless specifically authorized to remain by the IT Security Officer or appropriate supervisor, if the account belongs to an employee.

Policy

- 1.3 Account creation and maintenance must be authorized by the appropriate personnel or local event.

Procedures

- 1.3.1 For students, enrollment in classes constitutes appropriate authorization.
- 1.3.2 Written requests for the creation of accounts for new employees must be submitted by the employee's supervisor to the IT Coordinator.
- 1.3.3 Supervisors are required to provide immediate written notification to the Human Resources Officer who notifies the IT Coordinator in writing immediately upon notification that an employee will be terminating employment at the college.
- 1.3.4 Upon notification of termination of employment, all local and state-level employee access is disabled by the close of business on the last day of employment, and notification of the action is sent to the employee's former supervisor.
- 1.3.5 Written requests for the creation of generic or special-use accounts are submitted by the requestor to the IT Coordinator.
- 1.3.6 Supervisors must inform the IT Coordinator in writing immediately upon notification that an employee's IT access requirements should be modified as a result of changes in his job description or duties.
- 1.3.7 Upon notification that an employee's IT access requirements at the college will change, all local and state-level employee access must be modified as appropriate by the close of business on the date of change indicated by the employee's supervisor.

Policy

- 1.4 All computer accounts will be protected by an effective authorization method.

Procedures

- 1.4.1. All computer accounts are protected by a username and password combination.
- 1.4.2. A strong password policy is enforced for all local network accounts.
- 1.4.3. Users are forced to change local passwords every 90 days.
- 1.4.4. Users are prohibited from sharing access to accounts unless specifically authorized by the IT Security Officer for exceptional circumstances.
- 1.4.5. Passwords must contain a combination of at least three out of four of the following: lowercase alphabetic characters, uppercase alphabetic characters, digit characters, and special characters (e.g., ~@#\$\$%^&*()_+).
- 1.4.6. Password cracking software is used on an established schedule. Accounts with weak passwords are disabled, and the account owner must contact the IT Department in order to unlock his account access.

- 1.4.7. Hard copies of usernames and passwords for accounts with extraordinary user access, such as administrative accounts, or accounts used for mission-critical activities and equipment, are kept in a locked drawer, and the location is shared with the backup network administrator and the Vice President of Financial and Administrative Services.
- 1.4.8. Storage of passwords on computer media is forbidden, unless the file(s) containing them is (are) encrypted.
- 1.4.9. Proof of identity is required before any username or password is divulged to a user.
- 1.4.10. Account information pertaining to a user is never divulged to anyone other than the owner of the account.
- 1.4.11. Writing down user passwords and account names in any area that is easily accessible or in plain view of others is forbidden.

2. Physical security of equipment

Policy

- 2.1. All access to sensitive or critical equipment will be strictly controlled.

Procedures

- 2.1.1. Servers are stored in a locked room, unless attended by an authorized member of the IT staff.
- 2.1.2. When in areas where sensitive or critical equipment is stored, unauthorized personnel or visitors must be accompanied by an authorized member of the ESCC staff at all times.
- 2.1.3. Laptop computers must be in one of the following states at all times: stored in a locked room or cabinet, attended by an ESCC employee, or anchored securely to a desk or other sturdy furniture by an approved antitheft device.
- 2.1.4. Employee workstations other than laptops should be secured in a locked room when unattended.
- 2.1.5. Students and guests are prohibited from using employee workstations without supervision.
- 2.1.6. Student or guest use of employee workstations is strongly discouraged.
- 2.1.7. Employee workstations must be in a locked state whenever they are in use, but unattended.
- 2.1.8. IP telephones are not installed in public access areas.
- 2.1.9. Keys belonging to servers, cabinets, and other equipment are kept in a secure location.
- 2.1.10. Unauthorized individuals are forbidden from disconnecting computing equipment from or connecting computing equipment to the college's network infrastructure.
- 2.1.11. Changes to network configuration including servers, switches, edge devices, wiring, or other devices supporting sensitive and critical systems must be approved by the IT Coordinator.

- 2.1.12. Changes to network configuration including servers, switches, edge devices, wiring, or other devices supporting sensitive and critical systems should be scheduled during a time when the users of those systems are least disrupted.
- 2.1.13. When disruption of sensitive and critical systems will occur due to changes in network configuration including servers, switches, edge devices, wiring, or other infrastructure, the users of those systems should be notified in advance whenever possible.
- 2.1.14. Changes to network configuration including servers, switches, edge devices, wiring, or other devices supporting sensitive and critical systems must be documented in the Network Administrator's Handbook.

Policy

- 2.2. Sensitive and critical equipment must be protected from environmental and physical damage.

Procedures

- 2.2.1. Areas where servers and other critical equipment are stored contain fire extinguishers approved for use on electronic equipment.
- 2.2.2. Temperature and humidity are monitored in rooms where servers and other critical equipment are stored.
- 2.2.3. UPS and surge protection devices are used for all critical equipment.
- 2.2.4. System logs are monitored regularly for indications of equipment failure.
- 2.2.5. No food or drinks are allowed in any areas containing critical equipment.
- 2.2.6. The use of food and drink near any computer equipment is strongly discouraged for all employee workstations; it is prohibited in public access areas, such as computer labs or kiosks.
- 2.2.7. To the extent feasible, replacement devices are in storage locally in order to replace critical equipment as quickly as possible.
- 2.2.8. Critical equipment that it is not feasible to buy as backup devices are covered by extended warranty contracts with next business day replacement coverage to minimize outage of key systems.

3. Software / Data Security

Policy

- 3.1. Reasonable measures will be taken to protect sensitive or critical data from unauthorized disclosure.

Procedures

- 3.1.1. User account access applies the principle of least privilege.
- 3.1.2. System account access rules as described in Section 1 above, apply.

- 3.1.3. Storage of unencrypted sensitive data on mobile storage media, including laptops and flash drives is strictly prohibited.
- 3.1.4. Encryption is required whenever sensitive or critical data will be communicated over a non-secured transmission medium.
- 3.1.5. Before any magnetic media is recycled or transferred to another user, the media are erased using software approved by DOD standards for the permanent destruction of data.
- 3.1.6. Any media that cannot be erased, such as optical media, or any hard drive that cannot be accessed due to hardware fault, are physically destroyed.
- 3.1.7. Media that should remain intact and transfer to an authorized user are exempt from permanent destruction.
- 3.1.8. Printed materials containing sensitive or critical data must not be left in plain view on desktops or otherwise unattended.
- 3.1.9. Sensitive or critical data must be printed on a printer that is either attended by authorized personnel or located in a secure area.
- 3.1.10. Sensitive or critical data must be removed from the printer output bin as soon as possible by the owner of the printout or other authorized employee.
- 3.1.11. Printing sensitive data on publicly accessible output devices is discouraged.
- 3.1.12. With the exception of instructional workstations located in labs and classrooms, only college-owned data storage devices may be physically connected to college-owned IT systems.
- 3.1.13. Storage of sensitive data on other than college-owned storage devices is forbidden.

Policy

- 3.2. Reasonable measures will be taken to protect sensitive or critical data from accidental loss or destruction.

Procedures

- 3.2.1. Both incremental and full backup of sensitive and critical data are performed on a regular schedule.
- 3.2.2. Backups are tested on a regular schedule in order to ensure they can be used to replace lost data.
- 3.2.3. Backup media are stored in a locked, fire-proof safe in a locked area on campus.
- 3.2.4. A secure off-site location is used to store a second copy of the most recent full backup media.

Policy

- 3.3. Reasonable measures will be taken to protect software from unauthorized distribution or use.

Procedures

- 3.3.1. College-owned software is stored in a locked room or cabinet.
- 3.3.2. Whenever possible, backups are made of original software media.
- 3.3.3. To prevent illegal copies of software from being distributed on recycled media, before any magnetic media are recycled or transferred to another user, the media are erased using software approved by DOD standards for the permanent destruction of data.
- 3.3.4. Any media that cannot be erased, such as optical media, or any hard drive that cannot be accessed due to hardware fault, are physically destroyed to prevent the copying of software.
- 3.3.5. Media that should remain intact and transfer to an authorized user are exempt from permanent destruction.
- 3.3.6. Employees are prohibited from sharing college software installation keys or codes except as allowed by the licensing agreement for the software.
- 3.3.7. All software must be formally reviewed and approved before being installed on college-owned systems. The review process must include the college ISO.
- 3.3.8. Copies of all software for distribution to employees is catalogued and stored in a secure area.
- 3.3.9. Records of software distributed to employees covered by licensing agreements are kept for the duration of the software licensing agreements.
- 3.3.10. Employees are prohibited from making copies of software either for personal use or for redistribution, except as allowed by licensing agreements.
- 3.3.11. Illegal copying or redistribution of software or data using college computers is prohibited.
- 3.3.12. Wherever possible, account access is set such that installation of software by users other than IT staff members is disabled.
- 3.3.13. Proof of software licensing must be provided to the IT Department prior to installation of software on any college computers.
- 3.3.14. Infringement of copyright law is strictly prohibited; no user shall download or distribute any software, files, or other data except as permitted by copyright laws governing use in education.
- 3.3.15. All college equipment is subject to examination by the IT Security Officer in order to determine whether illegal software is being used or illegal activities have taken place.
- 3.3.16. The IT Department reserves the right to monitor all workstations in order to ensure compliance with software licensing agreements.

Policy

- 3.4. Reasonable measures will be taken to protect systems from malware, including worms, viruses, and spyware.

Procedures

- 3.4.1. Antivirus software is installed on all machines, unless the IT Security Officer has granted an exception for compelling reasons.
- 3.4.2. Memory-resident antivirus software is installed on all machines.

- 3.4.3. Antivirus scanners are programmed to update automatically at least once per week.
- 3.4.4. Antivirus scanners are programmed to scan for viruses at least once per week; more frequent scans are recommended.
- 3.4.5. All computers must be patched with all critical operating system updates; exceptions may be granted by the IT Security Officer.
- 3.4.6. Every effort is made to locate a substitute vendor patch in those cases where an OS patch will interfere with normal operation of the equipment.
- 3.4.7. Public access computers are scanned regularly for the existence of spyware.
- 3.4.8. Employees are encouraged to scan their workstations regularly for spyware.
- 3.4.9. Whenever possible, pop-up blocker software is installed.
- 3.4.10. Network messenger broadcast service is disabled on all machines.
- 3.4.11. Edge devices are monitored regularly to detect worm or virus activity.
- 3.4.12. Accessing pornographic, hacking, and illegal music and software distribution web sites is expressly forbidden.
- 3.4.13. The IT Department communicates information regarding serious threats to college resources to the college community in order to prepare users to avoid infection or compromise.
- 3.4.14. The IT Security Officer subscribes to industry accepted distribution lists and other notification services that warn of impending threats or newly discovered vulnerabilities affecting critical and sensitive IT resources.

Policy

- 3.5. Reasonable measures will be taken to detect intrusion events or system compromise.

Procedures

- 3.5.1. System logs are examined on a regular basis, and any notable events are recorded.
- 3.5.2. Intrusion detection technology is used to monitor intrusion attempts.
- 3.5.3. Intrusion events are handled as specified in the ESCC Contingency Management and Business Recovery Plan.
- 3.5.4. All workstations, servers, or other networked equipment, are patched off-line and hardened against break-in attempts using industry-accepted best practices prior to production use, except where a documented exception permitted by the IT Security Officer exists.
- 3.5.5. Perimeter and host-based firewall technology is implemented in order to prevent intrusion.
- 3.5.6. Penetration testing by an approved partner should be performed regularly.
- 3.5.7. Approved intrusion testing must avoid damage or compromise to sensitive or critical systems.
- 3.5.8. The results of the security test procedures performed in 3.5.6 above will be reviewed by the IT Security Officer, and the results, along with a plan to eliminate

- or reduce any system vulnerabilities will be submitted to the president within three months following the testing event.
- 3.5.9. Implementation of any improvements or changes documented in 3.5.8 above will be completed before the next intrusion testing event.
 - 3.5.10. Any modification to system servers is noted in the server activity log.

4. Personnel Security

Policy

- 4.1. Reasonable measures will be taken to ensure that college personnel practice acceptable security behaviors.

Procedures

- 4.1.1. All new employees are required to complete the ESCC Security Awareness Training Program within 30 days of employment at the college.
- 4.1.2. All employees receive employee security awareness refresher training annually.
- 4.1.3. Personnel are provided with timely information regarding service disruption and security issues.
- 4.1.4. IT Personnel responsible for security receive appropriate annual training.
- 4.1.5. The most recent version of this policy must be provided to all ESCC employees and students on the college's website.

5. Penalties for Non-Compliance

Policy

- 5.1. Users who violate ESCC information systems security policy are subject to appropriate disciplinary action.

Procedures

- 5.1.1. Faculty, staff, and students at the college or VCCS should immediately report violations of information security policies to the IT Security Officer, who will research the information about the case and identify the offender, if possible.
- 5.1.2. If state or federal law is apparently violated, then the research shall be conducted in conjunction with appropriate legal authorities in order to protect legal evidence.
- 5.1.3. The College President will report any alleged violations of state and federal law to the appropriate authorities.
- 5.1.4. If the alleged offender is an employee, the IT Security Officer will notify the offender's supervisor. The supervisor, in conjunction with the college or system Human Resources Officer and the IT Security Officer will follow the Human Resource published procedure for adjudication of the alleged offense.
- 5.1.5. If the alleged offender is a student, the IT Security Officer will notify the Vice President of Academic and Student Services. The vice president, in cooperation with the IT Security Officer, will follow the published student procedure for adjudication of the alleged violation.
- 5.1.6. All formal disciplinary actions taken under this policy are grievable and the accused may pursue findings through the appropriate grievance procedure.
- 5.1.7. The IT Security Officer reserves the right to disable any account or service that poses an immediate threat to ESCC's information technology resources.

Exception Handling

Exceptions to ESCC's IT Security Policy and Procedures must receive written approval from the Vice President of Finance and Administration. The attached form Form SEC 001 – Information Technology Security Exception Request is to be used for this purpose. Documentation of approved requests will be kept on file by the IT Security Officer as long as the exception is in effect.

No exception will be granted that is determined to undermine the security of sensitive or critical systems. The Vice President of Finance and Administration may revoke the approval at any point if any active exception handling procedure is determined to compromise critical or sensitive resources.

Glossary of Terms

Critical – required for operation; necessary to continue doing essential college business

Encryption – use of scrambled data to transfer or store it in a format readable only by selected parties

Firewall – device or software technology used to block intrusion by outsiders

Generic account – a network account that is intended to be shared among multiple users, usually because there is not justification for creating individual accounts for the purpose intended

Hacking – intentionally trying to gain access to a system's resources when the perpetrator has no justification for having that access

Information technology resources – any software, data, or equipment that is considered an asset belonging to the college, the VCCS, or the state

Intrusion detection system – software or hardware technology intended to monitor suspicious activity and alert the appropriate personnel to attempted break-ins

IP telephone – special digital phone used on a computer network

Kiosk – any workstation designed for open public access

Malware – any software designed to destroy or compromise a system's data or programs; includes those programs that track a user's actions

Password cracking software – a program used to gain access to accounts by determining their passwords

Patch – program code, usually distributed by the software manufacturer, to correct flaws or oversights in the original design

Sensitive – containing personal or private data or information that must be protected from unauthorized access

Server hardening – performing those preparatory tasks on a computer that are recommended by security experts to eliminate as many vulnerabilities as possible before the machine is placed in a production environment

Spyware – programs designed to track the actions or habits of the user; programs vary in severity from reporting the web page viewing habits of users to trapping keystrokes in order to gain access to sensitive information such as bank account access codes

System logs – text files containing status messages trapped by the operating system when preselected events occur

UPS – uninterruptible power supply; a device that supplies electricity on an emergency backup basis when there are short-term losses in power; most also protect against power surges

Virus – any malicious program capable of spreading itself from one machine to another; usually via some user intervention

Worm – a malicious program that spreads from one machine to another over a network without user intervention

Contact Information

Name	Title	Email	Phone
Cheryl Thompson-Stacy	President, ESCC	cstacy@es.vccs.edu	757-789-1775
Cynthia Allen	Vice President of Finance & Administration, ESCC	callen@es.vccs.edu	757-789-1768
Cynthia Hodges	Information Technology Security Officer, ESCC	chodges@es.vccs.edu	757-789-1770 (office) 757-710-1591 (cell)
Malcolm White	Backup Security Officer, ESCC	mwhite@es.vccs.edu	757-789-1771 (office) 757-710-5590 (cell)