NOTE: The following Enforcement Procedure is included in each of the following IT Policies as approved by PAC, April 24, 2008

ENFORCEMENT PROCEDURE

1. Faculty, staff, students, and patrons at the college should immediately report violations of information security policies to the local Information Security Officer (ISO).

2. If the accused is an employee, the ISO will collect the facts of the case and identify the offender. If, in the opinion of the ISO, the alleged violation is of a serious nature, the ISO will notify the offender's supervisor. The supervisor, in conjunction with the College or System Human Resources Office and the ISO, will determine the appropriate disciplinary action. Disciplinary actions may include but are not limited to:

    a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.

    b. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.

    c. Disciplinary action for faculty and classified staff in accordance with the guidelines established in the State Standards of Conduct Policy.

    **If Domain Administrator is the offender, his/her administrative rights will be disabled and administrative access will be given to Network Administrator Backup (with assistance of campus ISO) until matter is resolved.*

3. In the event that a student is the offender, the accuser should notify the Vice President of Instruction. The VP, in cooperation with the ISO, will determine the appropriate disciplinary actions which may include but are not limited to:

    a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.

    b. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.

    c. Disciplinary action for student offenders shall be in accordance with the college student standards of conduct.

4. The College President will report any violations of state and federal law to the appropriate authorities.

5. All formal disciplinary actions taken under this policy are subject to the Commonwealth's personnel guidelines and the accused may pursue findings through the appropriate grievance procedure.

Subject: Business Impact Analysis, section 2.3

Policy

To keep the most current, up-to-date information, yearly field testing will be conducted in various departments within the college. This information will be kept on file with the campus ISO, and will aid in other process audits that might be conducted. Along with these audits, the BIA process will be completed in its entirety every three years.

Procedure

Business Impact Analysis (BIA) will be initiated from the LIS Division to Department heads for the purposes of Risk Analysis and Critical Systems Identification. This process will be conducted within pre-selected divisions on a yearly basis. Once data is collected, it will be flooded into a yearly BIA template and kept on record with the campus ISO. A full scale BIA process will be conducted every three years and sent to the VCCS for compliance purposes.

Subject: Risk Assessment, section 2.6

Policy

VHCC will conduct risk assessments help to assess whether the IT security controls in place for IT systems continue to be commensurate with sensitivity and risk. The Standard requires, and VHCC will conduct a full risk assessment of each sensitive IT system at least once every three years. An RA is valid only if it is current, so the campus will also conduct an annual self-assessment to determine the continued validity of the formal RA. Validity may be affected by major changes to the IT system, system interfaces or the environment. Major changes are defined as substantial changes that alter the mission, configuration or basic vulnerabilities of the IT system. Changes that may indicate the need for a new RA include new or significantly changed

- Business Requirements,
- Hardware,
- Application Programs,
- External Users,
- Telecommunications,
- Location of the IT system (e.g. a new physical environment)
- IT System Interfaces.

Minor changes that may not require a new risk assessment include such events as the replacement of existing hardware with similar hardware when capacity does not significantly change; the addition of two or three workstations on a network; or small modifications to an application program (e.g., a change in table headings).

Procedure

To keep the most current, up-to-date information, yearly field testing will be conducted within the IT department. This information will be kept on file with the campus ISO, and will aid in other process audits that might be conducted. Along with the BIA audit, the RA process will be completed in its entirety every three years.

Subject: Continuation of Operations Planning, section 3.2

Policy

VHCC's COOP plan was written in May 2007 and has been approved by the college's Emergency Management Team and President; it will be reviewed/approved by the College Board at their July 2007 meeting. This plan meets the requirements identified by the Federal Emergency Management Agency, Virginia Department of Emergency Management and Executive Order 44 of the Governor's Office, and COV ITRM Standard SEC501-01.

The plan will ensure that VHCC:

- has the capability to implement the plan;
- campus ISO will collaborate with COOP coordinator for focus on IT related activities and related disaster recovery planning;
- is able to restore essential operations within 48 hours;
- is able to maintain those functions for up to 45 days;
- will implement a regular schedule for training and exercising college personnel, equipment, and internal systems and procedures
- will complete a risk analysis of our facilities and assess the possibility of using our current facilities;
- will maintain a list of alternate sites with reciprocal agreements to be used in the event VHCC's buildings are not inhabitable; and
- **will review this plan annually**.

Procedure

n/a

Subject: IT Disaster Recovery Planning, section 3.3

Policy

Virginia Highlands Community College shall:

I. **Develop a disaster recovery plan.** All community colleges in the state of Virginia dependent on voice telecommunications, data telecommunications, video telecommunications, or computer services for carrying out their missions must develop disaster recovery plan. Each campus is responsible and accountable for its own disaster recovery program.

II. **Maintain and update disaster recovery plan annually.** VHCC shall update its disaster recovery plan at least annually and following any significant change to their computing or telecommunications environment.

III. **Test disaster recovery plan annually.** VHCC will test the DR plan at least once a year. Any deficiencies revealed by the test Agencies shall be corrected. The type and extent of testing adopted by VHCC will depend on:
    - Criticality of agency business functions.
    - Cost of executing the test plan.
    - Budget availability.
    - Complexity of information system and components.

IV. **Train their IT employees to execute the recovery plans.** Training will consist of:
    - Making employees aware of the need for a disaster recovery.
    - Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency.
    - Training all IT personnel with responsibilities identified in the plan to perform the disaster recovery/business resumption procedures.
    - Providing the opportunity for recovery teams to practice disaster recovery skills.

V. **Annually certify the updating and testing of the disaster recovery plan.** Pursuant to SEC501-01, VHCC is responsible for the oversight of their respective campus management and use of IT resources. An annual disaster recovery confirmation letter will be kept on file with the campus ISO each year of

testing. By way of this letter, the campus can verify to the VCCS/APA that the disaster recovery plan has been reviewed, updated, and tested.

Procedure

n/a

Subject: IT System and Data Backup and Restoration, section 3.4

Policy

Critical backups will be made by the Network Administrator on a schedule that ensures the protection of VHCC critical data and user home directory information. Critical backup schedule will be recorded and kept on file with campus ISO for annual review.

Procedure

VHCC uses the Veritas Backup Exec software version 9.1 to perform its backup function.

- The software is installed on a Dell PowerEdge 2850 server with remote agents installed on all protected servers, including but not limited to, Exchange email, home directory, roaming profile, web, and other servers as necessary.
- At least one backup job is run each week night.
- A complete Exchange email server backup will be at least two times each week and incremental backups each week night.
- The home directory, roaming profile, web and other servers will have a complete backup ran each week with incremental backups ran each week night.
- Backup data is written to a RAID 5 array in the backup server and then moved to portable hard drives. These portable hard drives are periodically transported to the LAN Administrator's home 5 miles from VHCC for off-site storage.
- The Backup media is password protected but at present the backup software does not support date encryption.
- Due to limited number of staff, the Network Administrator performs all backups, restores and verifications.

Subject: IT Systems Security Plan, section 4.2

Policy

Critical backups will be made by the Network Administrator on a schedule that ensures the protection of VHCC critical data and user home directory information. Critical backup schedule will be recorded and kept on file with campus ISO for annual review.

Procedure

VHCC uses the Veritas Backup Exec software version 9.1 to perform its backup function.

- The software is installed on a Dell PowerEdge 2850 server with remote agents installed on all protected servers, including but not limited to, Exchange email, home directory, roaming profile, web, and other servers as necessary.

- At least one backup job is run each week night.
- A complete Exchange email server backup will be at least two times each week and incremental backups each week night.
- The home directory, roaming profile, web and other servers will have a complete backup ran each week with incremental backups ran each week night.
- Backup data is written to a RAID 5 array in the backup server and then moved to portable hard drives. These portable hard drives are periodically transported to the LAN Administrator's home 5 miles from VHCC for off-site storage.
- The Backup media is password protected but at present the backup software does not support date encryption.
- Due to limited number of staff, the Network Administrator performs all backups, restores and verifications.

Subject: IT System Hardening, section 4.3

Policy

Operating systems baseline security configurations

VHCC will apply preconfigured baseline security settings from the NIST (National Institute of Standards and Technology) and Microsoft. These templates apply a wide range of industry recommended security settings automatically when applied through group policies. Three levels of security are available for each system type: Default Security, Enterprise Security, and Specialized Security-Limited Functionality. An appropriate template configuration should be selected based on system usage and risk. For most VHCC systems, the Enterprise Security templates will be utilized. For specialized servers, special security templates tailored to function will be applied. After testing the selected template on a test machine, the templates will be assigned through group policies at either a local or GPO level at initial system setup. Any changes to the group policy configuration should be reviewed and documented by the VHCC Network Administrator. Security configurations will be reviewed at least yearly or whenever operational requirements warrant a review or modification.

Network devices baseline configurations

VHCC will maintain compliance with VCCS standards and guidelines relating to network device (Routers, Switches, Firewalls,) security configurations. The VHCC Network Operation Manager has overall responsibility to implement any recommended security configuration changes. Changes may include IOS updates, access list configurations, or other specialized security configuration recommendations. Other industry recognized best practices, procedures and tools should be used when possible to further harden and protect VHCC's infrastructure. One such tool is the Center for Internet Security (CIS) Cisco Pix and Cisco router benchmarks. The benchmarks provide industry approved best practices and lists of actions to be taken to improve the overall security of these network devices. Copies of all network device security configurations will be maintained on file in the office of the Network Administrator.

Application hardening

Applications cover a broad area of IT resources. Both server applications such as: web servers, DNS servers, SQL Servers, Microsoft Exchange Server, etc and client applications such as: Outlook

email client, Internet Explorer web browser, Office etc may require hardening to address security weaknesses that these applications present.

Hardening of these IT resources will include:

- Installation of the latest vendor software patches, hot fixes, and updates whenever a security bulletin is released.
- Following manufacturer recommended best practice security guidelines.
- Use of Operating system user authentication to restrict access to the application to only those who must use it.
- Utilization of expert security configuration guides such as the National Security Agency security configuration guides.

Vulnerability Scanning

Vulnerability scans will be conducted by authorized VHCC IT staff periodically to assess the continued effectiveness of VHCC IT system security configurations. The CIS NG Scoring Tools (such as RAT – Router Audit Tool) will be used as the scanning tool. Modifications to security configurations will be made if the results of scanning determine that the current configurations are insufficient. Any modifications made to security configurations will be documented and filed in the office of the VHCC Network Administrator. Scanning is to be performed at the following intervals:

- Yearly
- Whenever a new system is introduced
- When a change is made to existing configurations

Procedure

n/a

Subject: Malicious Code Protection, section 4.5

Policy

- In order to prevent malicious code propagation, no executable software, regardless of the source, may knowingly be installed on devices connected to VHCC/COV networks without prior IT Department review.
- IT staff will verify that software is free of malicious code before it is installed onto a device.
- Users must not intentionally disable virus detection software unless directed to do so by Network Administrator.
- If symptoms of malicious code are detected, users shall immediately alert their campus ISO or available IT staff.
- Users must not try to eradicate malicious code without the assistance and direction of college IT staff. Procedures shall be established and relayed to users for handling malicious code contamination incidents.
- Only devices approved by agency IT staff may be connected to a VHCC/COV network.

- Procedures for obtaining and updating virus pattern files and clients shall be implemented and conform to State standards (COV ITRM Standard SEC501-01).

- Email and attachments from external sources will be scanned for malicious code characteristics. If the presence of malicious code is indicated, these messages or attachments will be blocked from further distribution in the email system, quarantined, and eventually deleted.

- Additional measures may be taken at the enterprise level to prevent the introduction or proliferation of malicious code within the network. These measures include, but are not limited to; blocking specific IP source addresses or IP ports, blocking specific email messages or attachments, or blocking specific email sender addresses or domains. These measures can provide immediate protection from malicious code before virus patterns can be written and distributed.

- Users shall be periodically exposed to awareness materials on computer viruses and other forms of malicious code. Users shall receive training on safe computing practices to reduce the chance of introducing malicious code into the VHCC/COV computing environment (See Pol. 8.3 - Security Awareness Training).

Procedure

n/a

Subject: Account Management, section 5.2

Policy

Local administrator rights (or the equivalent on non-Microsoft Windows-based IT Systems) will be granted only to all users during account creation due to VCCS guidance.

Procedure

The following procedure is used by college supervisors to request computer access for their employees to the VHCC Local Area Network (LAN), VHCC Email System, VCCS Mainframe System, VCCS Student Information System (SIS) and the VCCS Administrative Information System (AIS) and MOAT Security Awareness Training Database.

1. The employee's direct supervisor will complete the Computer Access Request Form (see Appendix B) after securing required signatures and **submit it to the Network Administrator upon hire of employee AND IMMEDIATELY when an employee leaves employment with the college.** For student workers, include EmplId or EmployeeID.

2. The Network Administrator will create a network/email account for employee, and forward the form on to the AIS/SIS administrator who will send email notification of requested account activation to the supervisor, the employee and the MOAT Administrator. Upon notice of termination or resignation, a notice of account deactivation will be sent to the employee, the supervisor and to the MOAT Administrator.

3. MOAT Administrator will enter employee and supervisor information into Security Awareness Training system and will generate notification to the employee to complete training with 7 days. After this period, notification will be generated to the Network Administrator of those employees who have missed their training deadline.

4. After receipt of the Non Compliance Notification, the Network Administrator will disable the employee's network account.

5. The Network Administrator will re-activate disabled accounts only after verification by MOAT Administrator.

6. Network Access Admin provides requested network services to employees who are certified and disables the accounts of those who have not completed annual training.

Subject: Password Management - Network, section 5.3a

Policy

Local administrator rights (or the equivalent on non-Microsoft Windows-based IT Systems) will be granted to all users during account creation due to VCCS guidance. A screen saver lockout period (after a maximum of 10 minutes of inactivity) for COV devices will be enforced. (COV devices with access to sensitive systems or those devices in less physically secure environments must have the before mentioned lower time out interval documented and enforced.)

Procedure

All VHCC faculty, staff and administrators are assigned a unique userid composed of their first initial last name and a trailing sequential number in cases where a duplicate condition might exist. VHCC uses Microsoft Active Directory for the account management functions and policies are established within the Active Directory which requires each account to have a password. This system supports LAN access, Exchange email and publishing to the VHCC web server.

- Within the Microsoft Active Directory polices are applied that require user passwords to have the following properties:
  1. Minimum Password Length=8 characters.
  2. Maximum Password Age=90 days.
  3. Enforce Password History=24 passwords remembered.
  4. Minimum Password Age=42 days
  5. Store Password Using Reversible Encryption=No
  6. Account Lockout Duration=10 minutes
  7. Account Lockout Threshold=4 invalid attempts.
  8. Reset Account Lockout Counter After=60 minutes.
  9. Complexity rules=Enabled

- Microsoft Active Directory stores all passwords in its hierarchical datastore. Only the LAN admin has access to make modifications to this datastore.

- VHCC does not use Public Key Certificates

- VHCC uses SSL to encrypt user ID's and password when users are accessing the VHCC email system via the internet. The SSL certificate uses a 128bit encryption key. Windows XP is the predominant desktop operating system which uses Kerberos when users logon to the LAN. Thus passwords are never transmitted over the LAN in an unencrypted state.

- VHCC does not utilize VOLT (Virginia On Line Transaction) certificates.

Subject: Password Management – AIS/SIS, section 5.3b

Policy

Local administrator rights (or the equivalent on non-Microsoft Windows-based IT Systems) will be granted only to Network Administrator and authorized IT technician(s). All other account creation will be based on least privilege.

Procedure

New Accounts

New users are directed to the new Password Wizard the first time they log into My VCCS. These users must create a password in My VCCS before they will be able to log into enterprise applications (SIS, AIS, Blackboard, student email) directly.

Additionally, existing accounts with default passwords (DOB) are not able to access enterprise resources until they have used the Password Wizard in My VCCS to create a secure password. My VCCS directs users with blank passwords in DS2 to the Password Wizard. The Password Wizard requires First Name, Last Name, Date of Birth (DOB), and National ID (SSN). Users are instructed to contact their college helpdesk if any of the following issues occur:

- First and Last name doesn't match that which is in SIS exactly (ignoring case).
- Users that have a blank National ID (SSN) in SIS
- Users with an invalid SSN in SIS. Invalid SSNs begin with a 9.
- Users that try to access applications directly with default passwords (DOB) will be automatically directed to the Password Wizard.

The Password Wizard will also serve as a mechanism to allow users who may have forgotten their password to create a new one. A link to the Password Wizard will be available from enterprise applications and will read: "I cannot access my account.> My password does not work.> Reset your password here."

Password Reset Feature Used by SIS Help Desk Staff

SIS and AIS users who are unsuccessful with the Password Wizard are directed to the college's own support page on its web site. In order to assist these users, the current password reset feature of My VCCS is used by SIS help desk staff. This allows help desk personnel to temporarily set a user's password to their date of birth (DOB). Password resets are initiated by clicking the Reset Password button on the Person/Info Lookup page. The Reset Password feature should only be used after the college staff member has taken adequate steps (as defined by their college policy) to confidently authenticate the user. When authenticating a user, college staff uses the information available from Person/Info Lookup and other sources can be used only to confirm the information received *from* the user.

Following a help desk password reset, the user is only able to log into My VCCS (not the applications directly). Additionally, the user is required to immediately set a new secure password, security question and answer. Once a new secure password has been created, the user is able to access applications directly (after waiting about 10 minutes for the password synchronization to complete). The user has only 24 hours to use the temporary DOB password. If the user does not log into My VCCS to change the password within 24 hours, the password is erased and access to enterprise applications is disabled. The user will then need to contact the college to request another password reset.

The college help desk staff informs users who have had their password reset by college staff of the need to log into My VCCS rather than enterprise applications directly. They are also informed of the 24 hour limitation of the temporary password (DOB). These restrictions only apply to resets done by college staff.

Users who reset their own password with the Password Wizard create secure passwords which are not temporary.

Password Wizard

The Password Wizard creates passwords for new users, users with an expired password (because of either a default password or age), and allows users who have forgotten their password to create a new one. The Password Wizard requires First Name, Last Name, DOB, and National ID (SSN). Once the user has been authenticated, he/she is permitted to create a secure password.

Security Question

The Password Wizard and Change Password feature of My VCCS requires users to supply a security question and its answer. This question serves as an additional authentication mechanism the next time that the user is authenticated by the Password Wizard.

Users who have not supplied a security question see an icon when they log into My VCCS. This allows them to create a security question without going through the Password Wizard or Change Password feature.

Security questions that are provided by My VCCS:

- In what city were you born?
- What is the name of your favorite pet?
- What is the model of your favorite car?
- What is your mother's maiden name?
- What is the high school you last attended?

Alternatively, users may submit their own question instead of using one of the questions provided.

Expired Passwords

Passwords expire after 180 days. Users who log into My VCCS are warned of impending expiration starting 14 days prior to expiration. At 180 days and beyond, users who log into My VCCS are required to change their password using the Change Password feature of My VCCS.

Passwords Rules

New Passwords **cannot**:

- Be the same as the user's username
- Be the same as the current password
- Be the same as the user's date of birth
- Be all numbers
- Contain spaces
- Contain any of the following characters
    - ~ Tilde
    - & Ampersand
    - ` Acute or Back Quote
    - { Open or Left Curly Brace
    - } Close or Right Curly Brace
    - [Open or Left Square Bracket
    -] Close or Right Square Bracket
    - " Quote
    - | Or or Vertical Bar
    - ' Apostrophe or Single Quote
    - \ Reverse Solidus or Backslash

- / Solidus or Forward Slash

New Passwords **must**:

- Be at least 7 characters long, but not longer than 10 characters
- Contain at least one upper case letter (A–Z)
- Contain at least one lower case letter (a-z)
- Contain at least one number (0-9)

Subject: Remote Access, section 5.4

Policy

Only accounts in the active directory VPN users group can access the VPN. Currently this is Adam Rhea and Glen Johnson. A configuration file containing the crypto key is required on any client computer used to connect to the VPN server. This file is stored in a secured location on the VHCC LAN when only members of the Domain Admins group have access.
VPN access is used to troubleshoot server problems, change the phone system greeting during inclement weather or for after hours server maintenance.

VHCC uses a Cisco PIX 515e firewall which is also configured as a VPN server.
The VPN configuration utilizes the IPSEC encapsulation which encrypts all traffic using a DES encryption algorithm.

Procedure

n/a

Subject: Data Storage Media Protection, section 6.2

Policy

1. Connection of *ANY* storage media to VHCC network **without prior approval** is currently allowed as per VCCS guidance.

2. The storage of COV data (sensitive) data on mobile data storage media, including laptops as well as any non-network drive (except for backup media created by Network Admin) is prohibited unless encrypted.

- **Note:** Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, and digital music players owned by employees, contractors, and students (in non-research environments, i.e. administrative computers).

Exemption: Any computer with Deep Freeze installed is exempt from policy.

Procedure

Encryption mechanism should be requested from campus ISO if the transport of sensitive data is required.

Subject: Encryption, section 6.3

Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or

Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Mountain Empire Community College's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Virginia Highlands is in the process of reviewing encryption methods for future use, as we are not using any such method at the present. As this is a Network issue, users are restricted from using non-approved encryption methods without prior approval from campus ISO or designee.

Procedure

n/a

Subject: Facilities Security – Physical Security, section 7.1

Policy

- Only authorized IT Personnel will have access to VHCC IT systems. (See Appendix D – *Physical Security Procedures*)

- The college will protect the confidentiality, integrity, and availability of its Information Systems by preventing unauthorized physical access to, tampering with, and theft of these systems and the facilities in which they are located, while ensuring properly authorized access is allowed.

- Information System Resources containing Sensitive Data will be physically located in areas where unauthorized access is minimized. The external doors must have appropriate protections against unauthorized access.

- The level of protection provided for Information System Resources containing Sensitive Data will be proportionate with identified risks provided in VHCC's Risk Analysis documentation. An annual field test assessment of risks to the facilities storing Information Systems with Sensitive Data (full test will be conducted every three years) will be performed by ISO.

- An annual inventory of all physical access controls used to protect Information Systems resources with Sensitive Data and hosting facilities will be performed. All repairs and modifications to the physical components of facilities that are related to security will be
- documented. This documentation must be stored with Risk Assessment documentation in the office of the ISO.

- All physical access rights to areas where Information Systems Resources containing Sensitive Data are maintained will be clearly defined and documented and limited to authorized IT Personnel only.

- Employees will be encouraged to report unescorted strangers or anyone not wearing visible identification. All visitors with a requirement for access to the facility must show proper identification and sign in prior to gaining physical access to areas where Information System resources containing Sensitive Data are located.

Procedure

All employees will be issued a bar code ID card that must be scanned when entering buildings after hours or when entering the campus server room. Restricted Area Access logs must be signed when entering any IT closets as well.

Subject: Access Determination and Control, section 8.2

Policy

1. Background checks are conducted on all new employees, with the exception of work study.
2. All areas housing critical network systems are considered restricted areas. Only authorized IT personnel are allowed in these areas. Visitors must be accompanied by an authorized employee and must sign in/out on the VHCC Restricted Area Access Log (See Appendix C – *Restricted Area Access Log*).
3. Upon employment/termination employee access rights to all VHCC systems is enabled/disabled per Computer Access Request Form. (See Appendix C – *CARF*).
4. All new hires/terminates are evaluated by HR via Orientation/termination checklist.
5. All employees must be evaluated yearly to review EWP. Separation of Duties will be monitored via this process.
6. All access to VHCC network systems are based on the Least Privilege philosophy.
7. All new employees must read, agree to and sign a Computer Acceptable Use Agreement which is kept on file with the Network Administrator.

Procedure

n/a

Subject: IT Security Awareness and Training, section 8.3

Policy

All employees must complete MOAT SAT within 10 days of employment. (See Appendix C - *MOAT Procedures*, also available on web)

Procedure

See Policy 5.2 – *Account Management.*

Subject: Acceptable Use, section 8.4

Policy

All employees must sign a Computer Acceptable Use Agreement upon employment, and acknowledge acceptance within MOAT yearly thereafter. (See Appendix C – *Computer Acceptable Use Agreement*).

Procedure

n/a

Subject: Threat Detection, section 9.2

Policy

- Network Administrator is responsible for IDS system.
- Firewall logs must be reviewed regularly by the Network Administrator, and audited regularly by the campus ISO.

- The College's ISO must maintain regular communication with security organizations (Cyber Security Alerts from the US-CERT, SAN, Microsoft, ISS, McAfee, Cisco as well as HP website through electronic mail). ISO will forward any pertinent alert information to the Network Administrator.

Procedure

n/a

Subject: IT Security Monitoring and Logging, section 9.3

Policy

VHCC Network Administrator is responsible for monitoring IT system event logs. Logs are reviewed regularly as required by Policy 4.3 – System Hardening and Policy 9.2 - Threat Management.

Procedure

n/a

Subject: IT Security Incident Handling, section 9.4

Policy

VHCC's Incident Response Team will be responsible for responding to suspected or known breaches to IT security safeguards. An Incidence Reponse Plan will be updated and tested annually. All incidents will be documented and kept on file with campus ISO.

Procedure

Step One—Identification
In this phase of the process, the IT Dept will determine whether or not an incident exists and if so report the incident to the Chief Information Officer within 24 hours of discovering occurrence.

** An *event* is defined as any observable occurrence in a system and/or network. An *incident* is defined as an adverse event in a system and/or network or the threat of such an event.

Step Two—Containment

After the IT Dept has identified that an incident has actually occurred, the next step in the process will be to contain that incident. Some tasks that occur during the containment phase include:

- **Prevent further contamination of the system or network**
  - Remove the network cable or isolating the system on a separate VLAN
  - Use a firewall or access lists to prevent into or out of the system
  - Change DNS entries to direct traffic away from compromised system
- **Preserve Evidence** (example: image the entire system or part of the system or capture volatile data, such as running process, ram, network connections, and so on.)

Step Three—Eradication

It is during this phase that the IT Dept will analyze the information that has been gathered to determine how the attack took place. (To prevent the incident from happening again, it is important to understand how it was carried out

Step Four—Recovery

The recovery phase of this methodology is where the IT Dept will place the system back into the production environment. This involves testing the system to make sure that all business processes and function are back to normal. This might also involve monitoring the system or processes to ensure that the system is not compromised again and to look for additional signs of attack.

Step Five—Lessons Learned

In this final step, IT will utilize what was learned during the handling of the incident to enhance and improve VHCC's incident-handling process

This will include:

- Complete the incident report and present findings to management.
- Look for ways to improve the process both from a technical and administrative aspect.
- Have a clearly defined plan for implementing these improvements.

***All Incidents are to be reported to the Campus ISO immediately. (*See Appendix C - *Incident Reporting Form)*

Subject: Data Breach Notification, section 9.5

Policy

VHCC will abide by the Information security standards to protect personally identifiable information from compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or other situations where unauthorized persons have access or potential access to personally identifiable information for unauthorized purposes. If a data breach occurs, VHCC will provide notice to affected persons (e.g., students or other customers) about the occurrence of a data security breach involving personally identifiable information via a Data Breach Notification Form.

Procedure

Prevention
VHCC is responsible for implementing policies, procedures and systems to receive, store, transmit and destroy Consumer Data in a secure manner and to protect against data breaches.

Detection, Investigation and Escalation
VHCC is responsible for ensuring that it implements commercially reasonable policies, procedures and systems to detect the occurrence of a data breach within its systems. Those policies and procedures should include escalation of any breach to appropriate personnel within the institution in a timely fashion, and in the case of customers (i.e. students/patrons), prompt notice to them and the designated security contact.

If a data breach is known or suspected, the Security Officer will immediately commence and diligently pursue an investigation of the circumstances to determine (i) if a data breach has actually occurred, (ii) the scope of the data breach, including the type and amount of data affected, (iii) the risk that the affected data will be misused, and (iv) what steps are necessary to prevent further unauthorized access to customer data.

Notification of Breach

If VHCC knows or reasonably suspects (i) that customer data has been lost, stolen or otherwise subject to unauthorized access and (ii) that misuse of such information has occurred or is reasonably possible, the ISO will be informed and will document the following findings concerning the data breach incident:

1. Approximate cause(s) of the breach incident
2. Approximate date of the breach incident
3. Approximate size of the affected population (victims)
4. The type of data exposed

A Notification of Breach will immediately be sent to affected customers with above information.
(See Appendix C – *Security Breach Notification Breach Letter*)

Subject: IT Asset Control, section 10.2

Policy

- All IT assets will reviewed and updated on IT Inventory list annually or as needed.
- All data will be removed in accordance with the COV SEC2003-02.1.
- Non-COV owned equipment will not be permitted to be connected any COV/VHCC owned system without prior approval of IT Dept.

Procedure

IT Assets Inventory List will be updated as changes to inventory are made. A full inventory will be taken every three years during Business Impact Analysis process.

Subject: Software License Management, section 10.3

Policy

- All software must be approved by the Division Dean and College Information Security Officer (ISO) or designee prior to installation. This State requirement is not to circumvent department or division decisions to spend individual budgets as they choose but to:
    - Verify college systems can properly run the software.
    - Verify that proper security measures are contained within and utilized in the software installation and use.
    - Assist the department or division in setting up proper access controls and overall installation if required.
    - Ensure IT maintains a record of all software licensing for audit purposes.

Procedure

- Prior to entering requisitions for software employees must complete Software Approval Form (See Appendix C – *Software Approval Form*) and forward it to the Division Dean for approval before sending on to campus ISO. (The electronic forwarding of the approval form from the Deans mailbox will signify their signature). Once ISO has approved, this form will be kept on record with campus ISO. The Administrator and/or ISO will maintain their own logs of software purchases to keep track of all software information. Logs *may* include the:
    - Software name.
    - Software version.
    - Software serial number.

- Date of purchase.
- Purchase order number.
- Vendor information.
- Expiration date of license.
- Maintenance agreement information, if purchased.
- College department code.
- The physical location of where the software was installed.
- Primary users.
- Owner of the software.

- Departments and divisions should maintain purchase order copies, license agreements, registration cards, floppy disks, CD's or other media used to install the program and original manuals and documentation.

- Monthly scans will be conducted on all campus workstations and a software inventory will be collected. Any machine with unapproved software (not included on VHCC Software List) found on 1st scan will be reported to the division dean, 2nd scan will be reported to Vice President, 3rd scan will be reported to the agency head and network account will be disabled until resolved.

- No personal software may be installed on College owned equipment.

Subject: Configuration Management and Change Control, section 10.4

Policy

VHCC's Network administrator is responsible for any changes made to network systems. All changes will be documented and audited by the ISO on a regular basis.

Procedure

n/a