Northern Virginia Community College
Information Technology Support Services
IT Security Policy

Reviewed
February 28, 2008
# Table of Contents

**INTRODUCTION** ........................................................................................................................................... 3

**NVCC INFORMATION SECURITY OFFICER** ............................................................................................ 4

**INFORMATION TECHNOLOGY SECURITY SAFEGUARDS** ......................................................................... 4

- **Physical Security** .................................................................................................................................. 4
- **Personnel Security** ............................................................................................................................... 5
- **Data Communications Security** ......................................................................................................... 5
- **Phone System Security** ....................................................................................................................... 6
- **Wireless Security** .................................................................................................................................. 6
- **System Access Security** ....................................................................................................................... 6
  - **Authentication** .................................................................................................................................... 7
  - **Passwords Policy** ............................................................................................................................... 7
  - **Account Creation** ............................................................................................................................... 8
  - **Account Deletion** ............................................................................................................................... 8
  - **Account Maintenance** ....................................................................................................................... 9
- **Data Classification** .............................................................................................................................. 9
- **Legal Safeguards** .................................................................................................................................... 10
  - **Licensing** ......................................................................................................................................... 10
  - **Privacy** .............................................................................................................................................. 100
  - **Legal Disclaimers** ............................................................................................................................ 100
- **Network Usage Policy** ....................................................................................................................... 11
- **Ensuring System Integrity** .................................................................................................................. 12
  - **Virus Protection** .............................................................................................................................. 122
  - **Redundancy and Tape Backups** ....................................................................................................... 122

**SECURITY VERIFICATION** ................................................................................................................... 13

- **Security Logs** ....................................................................................................................................... 13
- **Security Verification Team** ................................................................................................................ 133

**HANDLING NON-COMPLIANCE** ........................................................................................................ 133

**SECURITY AWARENESS AND TRAINING** .......................................................................................... 134

**SURPLUS EQUIPMENT** ....................................................................................................................... 144

**APPENDIX A. DOMAIN ADMINISTRATOR ACCOUNTS** .................................................................... 155

**APPENDIX B. WINDOWS SERVER MINIMUM INSTALLATION** .............................................................. 155

**APPENDIX C. STANDARD NT SECURITY SETTINGS** ........................................................................ 166
Introduction

The objectives of the NVCC IT Security Plan are the following:

- Acquaint employees with the security procedures required to ensure protection of information technology systems at NVCC.
- Clarify employee responsibilities and duties with respect to the protection of information resources.
- Enable managers and other workers to make decisions about information security which are in keeping with standard policies and procedures, and which are responsive to prevailing local conditions.
- Coordinate the efforts of different groups within NVCC so that information resources are properly and consistently protected, regardless of their location, form, or supporting technologies.
- Provide guidance for the performance of information system security audits and reviews.
- Demonstrate upper management support for a strong information security program at NVCC.
- Establish a basis for disciplinary actions when required to protect NVCC information assets.

NVCC is taking appropriate steps to ensure its information systems are properly protected from all security threats. All NVCC information systems shall be protected, regardless of storage or transmission medium.

Two key concepts form the backbone of the security program at NVCC:

1. All information access is granted on a “need to know” basis only.
2. Information security is the responsibility of the individual worker.

All security procedures in this document are written with these two concepts in mind.
NVCC IT Security Officer

The NVCC IT Security Officer has been assigned the following responsibilities:

- Maintain and verify network and host security for all college systems.
- Develop and maintain formal security policies and procedures.
- Maintain and verify RACF user ID and data set security databases.
- Maintain and verify Active Directory group and user ID security databases.
- Verify Windows NTFS and share level access rights.
- Verify Local Area Network switch/router security.
- Develop and maintain a formal security awareness and training program.
- Perform any other activities necessary to secure NVCC information systems.

The NVCC IT Security Officer is Vincent Scrimenti (as of October 2005).

Information Technology Security Safeguards

This security plan requires that good management practices be followed to implement information technology security safeguards based on the NVCC IT Risk Assessment. The following is a list of requirements for all information systems maintained at NVCC.

Physical Security

- All network servers and network equipment shall be in a locked room or secured in a locked enclosure.
- All network server rooms shall have CO2 based fire extinguishers located within the room. Network Technicians shall be aware of the location of the closest fire alarm. The network server room shall have a smoke detector installed in it.
- The network server room should be monitored for temperature and humidity.
- All network servers shall be run on an uninterruptible power supply (UPS).
- Water detection systems shall be installed with the UPS systems to notify of the presence of water on the server room floor in order to prevent damage to the server equipment.
- An access list of personnel that are approved access to the server room or LAN/Phone closet shall be kept. A logging system shall be set up to document any visitors to the server room or LAN/Phone closet not on the approved access list. All visitors to the server room or LAN/Phone closet shall be escorted at all times.
- No food or drink is allowed around computer equipment.
- Sensitive information shall not be stored on portable computers that are taken outside of secured areas.
**Physical Security-Continued**

- Do not leave confidential information on desks after working hours or in rooms that are un-attended. All media should be clearly marked as to their classification.
- When dealing with confidential information, ensure that no one is watching over your shoulder. This precaution should also be taken when typing in passwords.
- Attended operation is required when printing confidential information to an unsecured location.

**Personnel Security**

Existing state law and regulations impose significant responsibilities on employees for the security of information. If deemed necessary, NVCC will take personnel action based on the following state laws and regulations:

1. The Virginia Employee Standards of Conduct and Performance specifically includes unauthorized use or misuse of state records, falsification of records, the willful or negligent damage or defacing of records and records theft as violations.

2. The **Government Data Collection and Dissemination Practices Act** (formerly the Virginia Privacy Protection Act of 1976) specifically requires that State agencies and institutions take affirmative action to establish rules of conduct and to inform employees involved in the design, development, operation or maintenance of an information system that misuse of personal information, or failure to take steps to ensure that information is accurate and reliable, may result in the individual employee being subject to injunction and assessed the costs of court action.

3. The **Virginia Computer Crimes Act (Code of Virginia § 18.2)** imposes both misdemeanor and felony violations for the unauthorized viewing, copying, alteration or destruction of computer data, software or programs.

Therefore, NVCC has instituted the following personnel security measures:

- Prospective new employees applying for positions, which have access to sensitive data, will be screened as to their trustworthiness in handling sensitive data.
- All individuals with access to sensitive data must be familiar with NVCC policies and procedures relating to sensitive data.
- Technical support personnel will be cross-trained so that procedures can be followed unaffected by the absence of any one key individual.

**Data Communications Security**

A Firewall shall be placed between each campus network and the Network Virginia wide area network which provides NVCC with Internet access. Security logging shall be enabled on the firewall.

Where possible, individuals shall use only encrypted means of access information across the Internet. Where this is not possible, individuals shall not pass sensitive college
information. Encryption methods shall use at least 48 bit encryption keys, with larger encryption keys preferred.

Dial-in access to the NVCC network shall be strictly controlled. A list of all modems connected to the NVCC network shall be kept. No modems shall be connected to the NVCC network without prior approval of the NVCC IT Security Officer. The list of modems shall also specify which modems are granted dial-in access. All dial-in and dial-out shall be accomplished using the NVCC network modem server when available in order to ensure that all network access is logged.

**Phone System Security**

The phone system is meant primarily to handle the business needs of NVCC. To this end, personal use of the NVCC phone system should not interfere with the business operations of NVCC. Also, NVCC should not be charged for personal toll calls. Therefore under normal circumstances 900 numbers shall not be dial-able from NVCC phones. International number shall not be dial-able from public areas.

**Wireless Security**

All NVCC wireless networking will be installed, maintained and monitored by Information Technology Support Services (ITSS). No wireless networking equipment shall be installed by anyone other than ITSS personnel. Monitoring shall be done to ensure that no rogue access points are installed. Any wireless equipment found that was not installed by ITSS, shall be removed immediately by ITSS personnel.

Access to the NVCC network through wireless equipment will be done using 128 bit WEP keys.

Broadcasting of SSID’s on all access points should be disabled.

**System Access Security**

Northern Virginia Community College (NVCC) provides user accounts for all faculty, staff, adjuncts and part time employees of the college. Accounts issued to users are for college use only and will be audited for misuse.

Access to all NVCC network servers, including but not limited to; domain controllers, phone system servers, voice mail servers, email servers, file servers, web servers, ftp servers, terminal servers, print servers and any general purpose server or workstation, and network hardware shall require a username and password, with the following exceptions: NVCC public web servers may allow anonymous access to information that is for public use.

All NVCC systems will be configured to allow least privilege access to users. NTFS permissions will be used to ensure that users will not have access to any system which is not part of their job function. The use of Active Directory OU’s or Windows 2000 account groups may be used to group similar users and permissions assigned for the entire group. The “Everyone Group” should be replaced with “Authenticated Users”.
Authentication

The identity of each individual who accesses college information, must be verified before access is given to the information. This identification process is normally performed using the user ID/password process. The user ID determines who the user is claiming to be. The submission of a correct password is taken to mean that the person is actually who the user ID claims them to be.

- Use of shared user ID’s is discouraged and shall be limited to workstations allowing only single function use (such as workstations secured so that they can only be used to browse the web) and must be approved by the IT Security Officer.
- All users shall be forced to change their passwords every 90 days.
- NVCC Systems shall be set to lock out further logon attempts for at least 5 minutes after 5 failed attempts have occurred.

Passwords Policy

First time users must call the IT Help Desk. At first logon, the user will be required to choose a new password using the following format:

- Passwords must be at least eight characters long.
- Passwords may not contain your user name or any part of your full name.
- Passwords must contain characters from at least three of the following four classes:

<table>
<thead>
<tr>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>English upper case letters</td>
<td>A, B, C, ... Z</td>
</tr>
<tr>
<td>English lower case letters</td>
<td>a, b, c, ... z</td>
</tr>
<tr>
<td>Numerals</td>
<td>0, 1, 2, ... 9</td>
</tr>
<tr>
<td>Non-alphanumeric (&quot;special characters&quot;)</td>
<td>~@#$%^&amp;*()_+</td>
</tr>
</tbody>
</table>

In addition, to maintain good security, individual passwords should not have any relationship to other passwords in use. That way if an attacker obtains one password, they will not be able to gain access to other passwords maintained by the same person. Passwords should not be accessible by anyone except by the owner of the password. Passwords should be changed regularly.

- Passwords should not be cyclical. When a password expires, do not name the new password as an identifiable iteration of the last password (i.e, pass1, pass2, pass3, etc.)
- Passwords used in the college should not be used on systems outside the college
- Do not share passwords with others.
- Passwords must not be stored in readable form in batch files or other locations unless sufficient security precautions are taken to ensure the security of the password.
• All vendor default passwords must be changed upon system installation.
• If a suspected disclosure of passwords has occurred, all involved passwords shall be immediately changed.
• Proof of identity is required to obtain a reset password.
• New passwords will be issued in a state that requires immediately changing the first time the user logs on.

Account Creation
All users requesting a LAN, SIS, or mainframe account on the NVCC network, MUST submit form “NVCC 105-45, Computer Access Request Form” prior to receiving their account. This includes, but is not limited to; Faculty, Staff, Adjuncts and Part Time Employees. No account will be created until the 105-45 has been approved and submitted to IT Security.
• The 105-45 must be filled out completely and signed by the new users’ supervisor and Campus Dean, Chairman or Coordinator.
• 105-45’s may be faxed to IT Support Services (ITSS) after obtaining signatures, but original must be submitted in regular mail.
• Each new user must complete the Security Awareness Training provided by NVCC within 7 days of receiving their NVCC account. If a signed form has not been received by the NVCC IT Security Department after 7 days, the users’ account will be disabled until the form is received.

Account Deletion
IT Security will be notified by Human Resources (HR) at the end of each month, with a list of users that have left the college in the past month. If IT Security has not received this list by the 1st of the month, a reminder email will be sent to HR requesting this information. After the completion of each semester, the Payroll Department will provide a list of the most current employees on the payroll, including full and part time faculty and staff.
• User accounts whose names are on the list provided by Human Resources, will be disabled for 30 days prior to deleting the LAN, email and web accounts. CICS accounts will be deleted immediately.
• Users whose names are not on the most current payroll, will be disabled for 30 days prior to deleting the LAN, email and web accounts. CICS accounts will be deleted immediately.
• User accounts that have been disabled for more than one year will be deleted.
Account Maintenance

Routine account maintenance will be performed to remove disabled accounts and accounts that have not been used in the past year.

- Every 3 months, January, April, July and October, a list of NVCC LAN user accounts will be generated. Unused accounts, older than 1 year, will be disabled for a period of 30 days, prior to deleting.
- Twice a year, January 31 and June 31, a complete review of accounts will be conducted. A request will be sent to Richmond for a report that lists users which have access to mainframe databases. (PeopleSoft, FRS, TSO, NOTIS, FOCUS, ALEX, ALICE, CARS, CIPPS, DMV, STARS, and PMIS). These reports will be compared to the current list of Windows Server accounts. Paperwork will then be submitted to Richmond to have old user access removed from the appropriate database.
- PeopleSoft access will be changed to LWEB for each account that is disabled or deleted.
- The mainframe automatically revokes access if the account has not been accessed in 3 months.
- Adjunct accounts may be disabled for up to one year, because they may only teach one semester per year.
- LAN account passwords will be scanned a minimum of once a year to verify that strong passwords are being used. Accounts with weak passwords will be disabled.

Data Classification

All sensitive information shall be labeled either [confidential], [employee data] or [student data] in the document containing the sensitive information. At least once per year, the NVCC IT Security Officer will search the NVCC network to ensure that confidential and internal use only documents are not accessible to the general public.

- All personal data shall be treated as confidential information.
- All storage medium shall be classified to highest level of information they may contain.
- All storage medium must be destroyed or securely wiped, using approved methods, before disposal.
Legal Safeguards

Licensing

- NVCC must have documentation proving compliance with software license agreements. If an end user loads personal software on their PC, they must provide the NVCC IT Help Desk with a copy of software license and proof of purchase or a statement saying that the user has in their possession a legal license for this software.
- NVCC is committed to obeying intellectual property laws such as the U.S. copyright law as it relates to electronic information and copyrights.
- The NVCC IT Security Officer will perform a periodic review of software licensing to ensure that NVCC is in compliance its software license agreements.

Privacy

- NVCC shall attempt to ensure privacy of communications over its telephone and data networks. However, it should be noted that messages sent over NVCC internal electronic mail systems are not subject to the privacy provisions of the Electronic and Communications Privacy Act of 1986, and therefore may legally be read by NVCC management and system administrators if deemed necessary to meet business requirements.
- All NVCC information systems, consisting of the equipment and information stored in NVCC information systems, are considered Virginia State property and as such may accessed, moved, read, etc. as needed to meet NVCC business requirements.
- Statistical information derived from college information systems may be disclosed to parties outside the college only if the individuals can not be identified by the information released.

Legal Disclaimers

Legal disclaimer shall be placed on all network access points. Disclaimers shall be set up as a logon banner upon network logon and as a link at the bottom of all NVCC web pages.

Workstation/Server Logon Banner:

“Clicking “OK” below indicates you have read and agree to the terms of the Information Technology Ethics Agreement and further consent to monitoring of your activities by technical support personnel during routine diagnostics of college-owned equipment. You can link to the Ethics Agreement from the bottom of the College’s home page at www.nvcc.edu.”
**Web Disclaimer:**

“Information may be posted and maintained on Individual sites by NVCC faculty, staff, and student organizations ("Individual Authors"). NVCC wishes to allow the academic community the greatest possible freedom to use these resources creatively and responsibly. Therefore it does not undertake to screen, verify, edit, monitor, or censor information posted by Individual Authors, whether or not originated by Individual Authors or third parties, and does not accept any responsibility or liability for such information. Individual Authors and third parties are solely responsible for the content and organization of information posted by them, even if such information is accessed through the NVCC Web site. Should any NVCC Web site user discover something out of date, please contact the individual author at the email address given at the Web site. If a user notices something in conflict with NVCC or VCCS policy, regulations or statutes of the Commonwealth of Virginia, or federal policy or law, please contact the College Webmaster and the individual author.”

**Router Logon Banner:**

“State law (article 7.1 of title 18.2 of the Code of Virginia) classifies damage to computer hardware or software (18.2-152.4), unauthorized examination (18.2-152.5) or unauthorized use (18.2-152.6) of computer systems as (misdemeanor) crimes. Computer fraud (18.2-152.3) and use of a computer as an instrument of forgery (18.2-152.14) can be felonies. The VCCS’ internal procedures for enforcement of its policy are independent of possible prosecution under the law.”

**Network Usage Policy**

- Any program adversely affecting NVCC information systems may be removed at the discretion of the NVCC IT Security Officer or designee. Programs may be considered to adversely affect NVCC information systems by consuming excessive processor time, disk space, processor memory, or network bandwidth.

- Personal use of the NVCC network must not interfere with normal business activities. It must not involve solicitations or be associated with any for-profit outside business activity.
Ensuring System Integrity

Virus Protection

- It is the responsibility of each individual to scan their documents for viruses before sharing them with other people, both inside and outside of NVCC.
- Virus protection on the workstation should be configured to automatically update it’s virus definition files.
- It is the responsibility of each individual to immediately notify the NVCC IT Help Desk upon finding a virus.
- The virus protection system implemented at NVCC shall scan attached files while in the MS Exchange inbox.
- The virus protection system shall scan files immediately upon their being saving to a file server or workstation.

Redundancy and Tape Backups

- All college data shall be stored in at least two separate locations.
- Where possible, the NVCC network shall be set up to limit the number of single points of failure in the system.
- Monthly full tape backup sets shall be stored for a minimum of six months.
- If necessary, as server disks become full with archived data, migration of the archived data to CD/DVD shall occur. Two copies of the archival CD/DVD shall be made. One copy shall be given to information owner and one copy shall be kept in safe under IT staff control.
Security Verification

Security Logs

All actions relative to system security must be accountable. Therefore NVCC information systems shall meet the following requirements:

- System security logs shall list logon and logoff times and all other relevant security events in order to support security audits.
- System security logging shall be balanced to insure logging of relevant security information while limiting the growth of the security log to a manageable size.
- All event logs must be stored for a minimum of 4 weeks.
- A method of automatic clock synchronization shall be set up on the NVCC network in order to insure accurate time information in the security logs.
- All security related logs shall be reviewed on a consistent basis to ensure that NVCC security is not being compromised.
- Administrators shall not have rights to clear or alter security logs in order to insure that the NVCC IT Security Officer has accurate security information in the security log.

Security Verification Team

A security team shall be set up to test the security of the network using known techniques used by people who try to gain access to networks. This security team shall be identified in writing to appropriate members of admin council when testing of the NVCC network is about to take place. No testing of network security will take place without the written authorization from the V.P. of Instructional & Information Technology (I&IT). If the security team is unsuccessful in obtaining entry into the NVCC network and are identified as intruders, they will then refer to the written authorization from the V.P. of I&IT. Upon completion of the security testing, full documentation as to the methods used and the results of the test shall be delivered to the V.P. of I&IT.

Handling Non-compliance

If individual managers believe they have a circumstance that requires exception to the NVCC IT Security Plan, upon agreement with the NVCC IT Security Officer they will be allowed to sign a "risk acceptance memo." By signing the risk acceptance memo, the manager is indicating that either they believe that other control measures compensate for the control indicated by NVCC IT Security Plan, or they are willing to assume the risk of being out-of-compliance with NVCC policy.

It is mandatory that all employees of NVCC report all suspected security incidents to the NVCC Information Security Officer. They may do so by calling the NVCC IT Help Desk or calling the NVCC Information Security Officer directly. All reported security incidents must be investigated.
Security Awareness and Training

All individuals involved in the management, operation, programming, maintenance, or use of information technology must be aware of their security responsibilities and know how to fulfill them. To this end NVCC has set up the NVCC IT Security Awareness Training program.

All individuals involved with information technology at NVCC shall receive security awareness training. New employees must complete this training within 30 days of their employment start date at NVCC. New employees must have a signed IT Security Awareness Agreement form in their HR personnel folder, stating they have received the security awareness training materials, read them, understood them, and will complete the online IT Security Awareness training course within 60 days from their employment start date at NVCC. (COV ITRM Guideline SEC2001-01.1).

All employees will be required to participate in yearly refresher training. Beginning the Spring 2008 semester, NOVA has contracted with Awareity to provide an online training course using their Managed Ongoing Awareness Tools (MOAT). Users will be notified through email when they need to take the refresher training and sent reminders. After notification, users will have 20 – 30 days to complete the Security Awareness Training. If after 20 - 30 days, users have not completed the training, their campus Information Technology Manager will contact them. Then after approximately one month, their account may be disabled until the training has been successfully completed through MOAT.

Individuals assigned responsibilities for information technology security shall be provided with in-depth training regarding security techniques, methodologies for evaluating threats and vulnerabilities that affect specific information technology systems and applications and selection and implementation of controls and safeguards.

The NVCC Information Security Officer, under the direction of the Director of Information Technology Support Services and the Vice President of Instructional and Information Technology, shall be responsible for documenting and maintaining security training records through MOAT. The NVCC Information Security Officer identifies those who did not complete the required online training and takes the necessary action.

Surplus Equipment

In accordance with COV ITRM Standard SEC2003-02.1 prior to the surpling, transfer, trade, replacement or disposal, of all computer hard drives and electronic media, must be wiped of all Commonwealth of Virginia data. The approved methods of cleaning are detailed in COV ITRM Standard SEC2003-02.1
Appendix A. Domain Administrator Accounts

Administrator accounts will be maintained locally at each campus.

Appendix B. Windows Server Minimum Installation

When installing a new operating system on a server or workstation, the following procedures shall be completed before putting the server or workstation in service.

All drives shall be formatted NTFS.

Apply the latest service pack and security patches to the operating system. This can be done by going to http://windowsupdate.microsoft.com.

Apply the latest service pack and security patches to Microsoft Office. This can be done by going to http://officeupdate.microsoft.com.

- Install Network Associates anti virus protection. Anti virus should be configured as follows:
  - Schedule antivirus to update automatically daily from Mcafee’s ftp site.
  - Scans should scan all files, including compressed files.
  - Action should be set to clean or disinfect and delete if unable to clean.

- Guest account disabled.

- Administrator account should be renamed to something other than administrator and shall not contain the word admin.

- Administrator account password should be changed to the standard administrator password used by the group installing the software.

- NVADM/Domain Admins should be added to the local administrator group. This should be done even if the server or workstation is a standalone or belongs to another domain.

- Set screensaver to lock and require a password after 15 minutes of idle time.

- Any software or services that are not required should not be installed or should be disabled. This should include web, ftp, telnet, snmp and terminal services.
Appendix C. Standard NT Security Settings

This section is under development.

- **Standard Group membership**
  - Administrators – Domain Admins (may have up to 3 additional users defined as administrators, and there should be at least one other local administrator account that is a member of the local Administrators group)
  - Users – Domain Users (if the computer is a standalone computer, local accounts may be added to the local Users group)

- **Rights to files and directories**
  - Rights to files and directories should be limited to users needing access to these files.
  - The Everyone right should be removed and replaced by Authenticated Users.

- **Rights to printers**
  - Administrators – Full
  - Creator Owner – Manage Documents
  - Authenticated Users – Print
  - Power Users - Full

- **Rights to the registry**
  - Under Construction

- **Account Policies**
  - Enforce password history = 18 passwords remembered
  - Maximum password age = 90 days
  - Minimum password age = 1 day
  - Minimum password length = 8 characters
  - Password must meet complexity requirement = enabled
  - Store passwords using reversible encryption = disabled
  - Account is locked out duration = 5 minutes
  - Account lockout threshold = 15 invalid passwords
  - Reset account lockout counter after 5 minutes

- **Audit Settings for Accounts, Files, Printers, and the Registry**
  - Audit account logon events-Success and Failure
  - Audit account management-Success and Failure
  - Audit directory service access-Failure
  - Audit logon events-Success and Failure
  - Audit object access-Failure
  - Audit policy changes –Success and Failure
  - Audit privilege use-Failure
  - Audit process tracking-Failure
  - Audit System events-Success and Failure
• Event log settings
  o Maximum application log size 24000 kilobytes
  o Maximum security log size 24000 kilobytes
  o Maximum system log size 24000 kilobytes
  o Prevent local guests group from accessing application log Enabled
  o Prevent local guests group from accessing security log Enabled
  o Prevent local guests group from accessing system log Enabled
  o Retain application log 7 days
  o Retain security log 7 days
  o Retain system log 7 days
  o Retention method for application log By days
  o Retention method for security log By days
  o Retention method for system log By days
Review and Testing History

**Policy Review:** 11/2005: Vincent Scrimenti, Information Security Officer

**Penetration and Assessment Testing:**

**Penetration Testing Review, Policy Review, and Action Items:** 12/2005:
Vincent Scrimenti, Lowell Ballard, Randy Dotson, Allen Sinner

**Policy Audit:** 12/2005 – 02/2006 Vincent Scrimenti, Information Security Officer

**Policy Review:** 01/2006 – 02/2006: Lowell Ballard, Information Technology Director