New River Community College

Information Technology Policy and Procedure Manual

Table of Contents

Asset Management

I. PURPOSE

The purpose of this policy is to manage changes in a rational and predictable manner so that users can plan accordingly.

II. DEFINITION

Information technology resources at NRCC require occasional outages, upgrades, maintenance and troubleshooting. Unplanned outages may occur; however, all planned outages and changes should be conducted in a manner that minimizes the impact of the outage/change on college users.

III. POLICY

Every IT change at NRCC, including changes to operating systems, hardware, networks, and applications, is subject to this policy and must be managed by the college Information Security Officer.

Customer notification must be completed for each scheduled or unscheduled outage or change.

A review of each change or outage must be performed to determine the degree of success and identify potential needs for fine tuning.

All changes and outages must be logged. The log records should contain date, description of the affected system or resource, name of the data owner or custodian, nature of the change, and an indication of success or failure.

Violations of this policy must be reported to the college's Information Security Officer (ISO) for investigation and follow-up.

IV. DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action up to and including dismissal. All users are subject to the revocation of access privileges or limited access to college IT systems. In the case of college personnel or the public, the determination and execution of disciplinary action must include the Vice President for Finance and Technology (who receives a recommendation from the ISO), the Human Resource Officer, the President, and the appropriate supervisor. In the case of students, the Vice President for Instruction and Student Services will also be included in the determination and execution of disciplinary action.

AUTHENTICATION POLICY

I. PURPOSE

The purpose of this policy is to ensure that the person supplying an identity is the person to whom the supplied identity has been assigned.

Authentication: Authentication is the process of verifying the identity of users. Generally, it is accepted that the forms of authentication come in three types that may be used separately or together: something the user knows (e.g., a password), something the user carries (e.g., an ID card) or something about the user (e.g., a fingerprint).

II. POLICY

The system owner or his or her designee for the system involved will, with input from data owner(s) and system administrator(s), make the decision about the level and type of authentication that will be deployed. The following types of authentication listed in order of strength are permitted for use on NRCC systems:

A. Network Address/Physical Location: May be used to restrict access to data or a particular service to persons using a specific networked device or any NRCC networked device in general. "Proxy"-type services may be deployed where it is necessary to provide this access to NRCC users who are not physically attached to a NRCC network segment (e.g., library databases). An additional form of authentication will be necessary to ensure that the person accessing this proxy mechanism is indeed a member of the NRCC community and as such authorized to access the network address-protected services.

B. Personal Identification Number (PIN): PIN authentication will be available for use as a security measure for mobile phones. The PIN must be 4 to 5 digits. Users will be responsible for safeguarding the integrity of their PIN.

C. Password: Passwords or passphrases may be used for applications where access to data or information systems requires individual or personal identification, and where this single password or passphrase is sufficient to authenticate this identity. Passphrases differ from passwords in that they are much longer (typically 20 to 40 characters) making them more secure against “dictionary attacks.” The secure password or passphrase should be used for systems requiring a high-level of individual accountability. See the Password Management policy for more information on the use of passwords.

D. Authentication Device: This level of protection makes use of password token technology in addition to a password, for systems requiring a higher level of individual accountability than a password alone can provide. The user must physically possess the device and know the associated PIN, in addition to knowing the password associated with the account.

E. Biometrics: Biometric authentication verifies a user's identity by requiring the capture of a biometric sample (e.g., fingerprint) and comparing that sample to a stored biometric sample that was enrolled by the user. This level of protection is appropriate for systems requiring a higher level of accountability than a password can provide and when a system for secure enrollment of users' biometric samples is present.

All sensitive data and information used for authentication either stored or in transit, must be protected. The data must be encrypted and only the minimum amount of access necessary should be granted to allow the authentication process to function.

BREACH NOTIFICATON POLICY

I. PURPOSE

Confidential personal information compromised by a security breach may lead to identity theft and invasion of privacy for affected individuals. NRCC may be required by law to take specific action in the event of a breach to the confidentiality of such information.

II. POLICY

Actual or suspected security breaches involving confidential personal information must be reported immediately to the Vice President of Finance and Technology. Once the nature and extent of the breach has been determined, NRCC will notify affected individuals as necessary. Violations of this policy may lead to disciplinary action up to and including termination.

All faculty, staff and contractors that process, store, transmit or otherwise use confidential personal information entrusted to NRCC are required to notify immediately the Vice President of Finance and Technology in the event of a suspected or actual breach of the confidentiality of such information.

Personal information that is lawfully available to the public from a government record is not subject to this breach notification policy. In addition, personal information rendered unreadable to an unauthorized party through use of encryption is not subject to this breach notification policy. Accordingly, all computers and other electronic data storage devices where confidential personal information may reside must be encrypted in accordance with the Information Technology Plan.

BREACH NOTIFICATION PROCESS:

A. Where it is suspected or evident that an unauthorized disclosure of personal information, a privacy breach, has occurred, the individual or individuals who are aware of the potential privacy breach shall immediately notify the Vice President of Finance and Technology.

B. The VP will forthwith strike a privacy breach committee composed of the Director of Human Resources, an administrator representing the department experiencing the privacy breach, and an information technology representative when necessary, to investigate the potential breach.

C. This privacy breach committee will:

1. identify the scope of the potential breach and take the necessary steps to contain it;
2. identify those individuals whose privacy was breached;
3. evaluate the nature of the information disclosed;
4. evaluate whether and how notification of the affected individuals should occur;
5. evaluate who in addition to the affected individuals should be advised of the privacy breach and so advise those individuals; and
6. review policies and procedures relating to the circumstances resulting in the privacy breach and provide recommendations to the appropriate persons to prevent future breaches.

D. Notification by one or more of the following methodologies, listed in order of preference:

1. Written notice to the last known postal address in the records of the individual or entity;
2. Telephone Notice;
3. Electronic notice;
4. Emergency Notification system; or
5. Substitute Notice- if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
    a. Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
    b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
    c. Notice to major statewide media.

E. Notification will consist of:

1. A general description of what occurred and when
2. The type of personal information that was involved
3. What actions have been taken to protect the individual's personal information from further unauthorized access
4. A telephone number that the person may call for further information and assistance, if one exists; and
5. What actions the agency recommends that the individual take.

Change Management

I. PURPOSE

The purpose of this policy is to manage changes in a rational and predictable manner so that users can plan accordingly.

II. DEFINITION

Information technology resources at NRCC require occasional outages, upgrades, maintenance and troubleshooting. Unplanned outages may occur; however, all planned outages and changes should be conducted in a manner that minimizes the impact of the outage/change on college users.

III. POLICY

Every IT change at NRCC, including changes to operating systems, hardware, networks, and applications, is subject to this policy and must be managed by the college Information Security Officer.

Customer notification must be completed for each scheduled or unscheduled outage or change.

A review of each change or outage must be performed to determine the degree of success and identify potential needs for fine tuning.

Violations of this policy must be reported to the college's Information Security Officer (ISO) for investigation and follow-up.

IV. CORRECTIVE ACTIONS

In the event of a violation, the college's ISO will investigate and recommend appropriate action (including disciplinary action) to the Vice President of Finance and Technology. Where disciplinary action is recommended, the President and Human Resource Officer, and in the case of students, the Vice President for Instruction and Student Services, must be included in the resolution.

HARDWARE AND SOFTWARE PROCEDURE

I. PURPOSE

New River Community College shall maintain in accordance with the approved technology models, standards, and guidelines a computer infrastructure that satisfies the administrative and instructional needs of faculty, staff, and students.

II. POLICY

New River Community College shall maintain adequate personal computers that meet hardware and software technical or useful life definitions as defined by VCCS models, standards, and guidelines (http://system.vccs.edu/its/guidelines/DesktopGuidleLine.htm) for the following:

Operational Requirements:

- Each full-time faculty member and part and full-time staff members shall have their own personal computer at their workstation with the most appropriate configuration for their use level.

- Colleges will provide personal computers on campus for adjunct faculty at a minimum ratio of 1 personal computer for every 20 full-time equivalent adjuncts. Colleges shall ensure that all adjunct faculty members have access to a computer on campus. The College shall also provide Microsoft Office software and anti-virus software to all adjunct instructors for home use at no charge.

- Computers for student use in classrooms, labs, or other student accessible locations shall be at a minimum ratio of 1 personal computer for every 7 full-time equivalent students (FTES).

- Computers meeting the minimum resource requirements to run specified software shall be provided for functions such as library and student information kiosks.

- Colleges shall use the currently supported Operating System for their Windows and Macintosh computers. Operating systems which have reached the end of their life cycle should be upgraded to a current version.
    A. All Windows computers shall use Windows XP Pro for operating system.

B. Computers running unsupported Operating Systems in order to run obsolete instructional software shall not be connected to the college network.

- General office software shall be kept current. All college Windows computers for students, faculty and staff shall have Office 2003 or Office 2007.

- Instructional software shall be kept current. Each College should not be more than one generation behind the current version (i.e., about 18 months maximum behind a current release). Each College shall document exceptions for bona fide instructional purposes, such as personal computer repair programs.

- College list will be reviewed annually as part of the technology process.

INCIDENT RESPONSE

I. PURPOSE

The purpose of this policy is to set requirements for efficient and effective response to incidents affecting the security of information technology (IT) resources and systems.

II. POLICY

The New River Community College IT Security Incident Response Policy and subordinate procedures define standard methods for identifying, tracking and responding to network and computer-based IT Security Incidents.

Reporting Incidents:

> All IT system users are responsible for promptly reporting any suspected incidents to the Information Security Officer either directly or through their supervisor, or Help Desk.
>
> A preliminary investigation into all suspected incidents will be conducted to determine if the event is an actual incident requiring a coordinated incident response.

Notification:

New River Community College Information Security Officer is responsible for ensuring that incidents are reported promptly upon discovery.

Virginia Information Technologies Agency (VITA) must be notified of incidents within 24 hours of when NRCC discovered or should have discovered their occurrence, as directed by the Code of Virginia 2.2-603 (F).

The affected system owners, data owners and the Vice President for Finance and Technology will be notified immediately upon discovery of an incident.

The Information Security Officer will notify law enforcement for further investigation if criminal activity is suspected and will cooperate and assist in any investigation as requested.

A. **Identification of Incidents:** Any member of the NRCC community or individual or organization outside of NRCC may refer an activity or concern to the Information Security Office. The ISO itself can also identify an Incident through its proactive monitoring of NRCC's network and information system activities. Once identified, the

ISO will use standard internal procedures to log and track Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in the remainder of this policy.

B. **Establishment of an IT Security Incident Response Team:** The Information Security Office (ISO) is responsible for Incident interdiction and remediation of computer-and electronic communication -based resources affected by these incidents. ISO will consult key representatives of NRCC Administrators, Security, Technology Services, Academic and Administrative Systems Departments, or other units, as warranted, to establish an IT Security Incident Response Team appropriate to respond to a specific Incident.

C. **Risk Assessment Classification Matrix:** The ISO will establish an internal risk assessment classification matrix to focus the response to each Incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an "escalation" of contacts across the college, and will indicate which authorities at NRCC to involve and which procedure would be applicable for each class of incident.

D. **Documentation and Communication of Incidents:** The Information Security Office will ensure that Incidents are appropriately logged and archived.

   Wherever possible, documentation of such Incidents will cross-reference other event databases within the college, such as the Information Security Office help desk and network monitoring systems, and NRCC Security Reports.

   The Information Security Office or IT Security Incident Response Team representatives will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.

E. **Subordinate Procedures:** The ISO will maintain standard subordinate procedures for the response and investigation of each Incident, as well as securing the custody of any evidence obtained in the investigation. The procedures will specify the location and method of custody for each incident, if custody of evidence is required.

F. **Role of NRCC Personnel, Training:** NRCC personnel are required to report Incidents to the Information Security Office.

G. **Relationship to State and Federal Agencies:** A response plan or remediation defined by this policy may be preempted as required or at NRCC's discretion by the intervention of federal and state executive officials.

H. **Incident Prevention:** Wherever possible, the college will undertake to prevent Incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its IT resources.

I. **Modifications and Adjustments:** This policy and its procedures will be reviewed at least annually to adjust processes, identify new risks and remediations.

III. DEFINITIONS

Incident: The term incident refers to any suspicious or abnormal event involving IT resources and systems which poses a threat to University IT resources, systems, data, services or system users. Incidents may include, but are not limited to, malware affecting multiple systems, unauthorized intrusion or damage to a web site or page, unauthorized intrusion into a computer system or network or other threats..

LOGICAL ACCESS

I. PURPOSE

The purpose of this policy is to identify the requirements for granting, maintaining and terminating users' access to College information technology (IT) resources and systems.

II. POLICY

In general, access to and use of New River Community College-owned IT resources and systems will be limited to persons directly affiliated with NRCC. Exceptions to this limitation are permitted under certain conditions subsequently described.

A. NRCC Affiliated: Direct affiliation in this context means faculty, staff and students of New River Community College. Faculty includes persons holding either permanent or temporary appointments as well as adjunct faculty, instructors, retired faculty and visiting faculty. Faculty also includes those persons with faculty status such as research associates, research scientists and academic and service professionals. Staff includes all those non-faculty persons employed directly by NRCC, either part-time or full-time, as well as retired staff. Students include any persons enrolled or who have signified their intent to enroll (by paying an admissions deposit) in the established academic programs of NRCC, including full or part-time students and degree or non-degree seeking students.

B. Not NRCC Affiliated:

1. **Nature of the Work**: Access to and use of IT resources and systems by persons not directly affiliated with NRCC must involve work to be performed which satisfies at least one (1) of the following conditions:

   a. the work relates directly to or is in support of NRCC sponsored activities.

   b. the work involves use of IT resources and systems available only from NRCC and can be accommodated without disruption to established NRCC workloads.

2. **Approval for Access:** Requests for access by persons not directly affiliated with NRCC must be sponsored by a NRCC employee who agrees to assume responsibility for use and adherence to the Acceptable Use of Information

Technology Resources and Systems Policy. Requests must be submitted by the sponsor in writing to the Vice President of Finance and Technology for approval.

Requests must identify the person(s) needing access, describe the access needed, indicate the duration of the access (not to exceed 1 year), and provide names, addresses and phone numbers for technical contact individuals.

C. Granting Privileges**:** Access to NRCC IT resources and systems is granted only for the resources and systems that are necessary for an individual to perform his or her duties, is explicitly granted by the owner or designee to an individual and is assigned via a unique access account/ID. Authentication is required at the time of access through the use of a password, ID card, etc. (see Authentication Policy).

D. Accountability: The owner of an access account/ID is accountable for its use. It is the ID owner's responsibility to protect the integrity of accessible systems and preserve the confidentiality of accessible information as appropriate. Beyond the account/ID creation process any subsequent access to any discrete resources and/or data must be authorized by the appropriate data owner. Under no circumstances can the data owner, the data owner's authorized alternate or any other individual authorize access for him or herself.

E. Terminating Access:

1. **General Requirements:** Access will be promptly terminated when the need for that access no longer exists. The Information Security Officer or his or her designee reserves the right to suspend and/or terminate any access privileges he or she determines to be a potential threat to the confidentiality, integrity or availability of any sensitive IT resources and systems.

2. **Specific Requirements:**

a. Faculty and staff:

(1) Faculty and staff access will be terminated when notified by Human Resources of employment termination.

(2) Faculty and staff access will be suspended if a leave of absence from the college is over a 30 day period of time.

(3) Faculty and staff access will be suspended immediately upon disciplinary action. It is important to use the same security measures for suspended employees as are used for separating employees. In addition, extended leaves of absence may require these measures, at the supervisor's discretion, taking into consideration such factors as level of access, nature and scope of computer applications and permissions, and duration of absence.

b. Retirees: E-mail and portal access for retirees will be reviewed every six months for inactivity and inactive accounts will be subsequently removed.

c. Students:

(1) Access granted for students as part of their employment by the College will expire no later than the end of each term.

d. Vendors: Vendors with access to computers and networks should meet many of the same standards placed on employees. They should understand the security policies and practices. Their access should be limited to just what is necessary for them to meet their contract requirements. When appropriate, vendors should be escorted into physically restricted areas. When their job is complete, they should return all access devices, and their log-on privileges should be terminated.

F. Access Reviews: At a minimum, all access to sensitive data, as defined by the Business Impact Analysis/Risk Assessment Policy, will be reviewed for accuracy by the data owner(s) on an annual basis.

G. Exceptions and Exemptions: Exceptions to or exemptions from any provision of this policy must be approved in writing by the Vice President of Finance and Technology or his or her designee.

PASSWORD MANAGEMENT

I. PURPOSE

Effective password management is the most central single element in assuring the overall security of New River Community College's information technology (IT) resources and systems and the protection of college data. The purpose of this policy is to ensure that all users are aware of their responsibilities in effective password management and to ensure that appropriate password standards are applied to all College IT systems.

II. APPLICABILITY

This policy applies to all IT systems whether connected to the network or standalone, hosted internally or externally or administered by Technology Services or another department.

III. DEFINITION

Password Management: Password management is the selection, distribution, use, modification and testing of computer system passwords.

IV. POLICY

All who participate in the use and administration of NRCC's IT resources and systems share responsibility for effective password management. Specific responsibilities are assigned as follows:

A. Password Standards: Passwords will be required on all College sensitive IT systems and other IT systems where passwords are necessary for accountability, as well as on College mobile devices (e.g., smart phones). Technology Services will provide Minimum Password Standards that must be applied to all College IT systems that utilize passwords for authentication; however, more rigorous password requirements will be applied to IT systems commensurate with the systems' sensitivity and risk. The actual password requirements applied to the IT system will be documented in the IT system security plan.

a) NRCC Password Requirements:

- MUST NOT contain all or part of the user's account
- MUST be at least 8 characters in length
- MUST contain characters from 3 of the following four categories:
  - English uppercase characters (A through Z)

- English lowercase characters (a through z)
- Base number (0 through 9) or a non-alphanumeric character (e.g., !, $, #, %)
- Prohibit use of passwords that can be found in a dictionary. This includes hardware passwords.

- Password must be changed every 90 days.

** Account passwords expire every 90 days unless they are a user of sensitive IT systems which include network systems. These users will change their passwords after a period of 42 days. Users will be notified 2 weeks out to change their password.

b) NRCC Password Requirements for mobile devices:

- All mobile devices require a four to five digit pin in order to protect sensitive data issues.

B. Password Testing: Technology Service reserves the right to monitor the overall security of NRCC's IT environment by testing the strength of passwords on all College IT systems, both those it administers and others.

C. Personal Ownership of Password Management: Ultimately, individuals using NRCC's IT resources and systems are responsible for assuring effective password management. To fulfill this responsibility, they shall be aware of and follow the Minimum Password Standards. Most notably, this includes creating strong passwords and safeguarding their passwords' integrity. Passwords represent an individual's identity to the IT system and should never be disclosed to or used by others.

D. Responsibility to Report Compromise: All users are required to immediately contact the Help Desk and change their password if at any time they suspect their password has been compromised.

V. CORRECTIVE ACTIONS

In the event of a reported security breach, as a result of notification or monitoring, the college's ISO will investigate and recommend appropriate action (including disciplinary action) to the Vice President of Finance and Technology. Where disciplinary action is recommended, the President and Human Resource Officer, and in the case of students, the Vice President for Instruction and Student Services, must be included in the resolution.

PHYSICAL ACCESS

I. PURPOSE

The purpose of this policy is to establish the rules for the granting, control, monitoring, and removal of physical access to New River Community College's information technology resources and systems facilities. These facilities include areas containing sensitive data and telecommunications equipment.

A. COV IRTM Information Technology Security Standards

1. Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

2. Access to "critical" computer hardware, wiring, displays and networks must be controlled by rules of least privilege.

3. A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks must be implemented (e.g. badges, cameras, access logs).

II. POLICY

All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

All facilities must be physically protected in proportion to the criticality or importance of their function at NRCC.

Access to facilities must be granted only to authorize personnel whose job responsibilities require access to that facility.

Access to facilities must include the approval of the person responsible for the facility.

All facilities must track visitor access with a sign in/out log based upon the criticality of the facility being protected. Visitors must be escorted by the appropriate NRCC information technology staff member.

Access logs (authorized personnel, visitors, etc.) for facilities must be kept for routine review by the person responsible for the facility based upon the criticality of the facility being protected.

Vendors with access to facilities should meet many of the same standards placed on employees. They should understand the security policies and practices. Their access should be limited to just what is necessary for them to meet their contract requirements. When appropriate, vendors should be escorted into physically restricted areas. When their job is complete, they should return all access devices, and their log-on privileges should be terminated.

At a minimum, access to facilities will be reviewed for accuracy by the person responsible for the facility on an annual basis.

Security Awareness and Training

I. PURPOSE

The purpose of this policy is to identify the conditions necessary to provide information technology system users with appropriate awareness of system security requirements and of their responsibilities to protect information technology resources and systems.

II. DEFINITION

Information technology system users at NRCC include faculty, staff, retirees, students and any other individual approve for access by the college's Information Security Officer (ISO).

III. POLICY

A. Awareness

Basic security awareness topics include malicious code protection, proper disposal of data storage media, proper use of encryption products, password management, intellectual property rights (including software licensing and copyright issues and other concepts) as required. IT system users are requires to document acceptance of security policies by signing the Information Technology Employee Ethics Agreement.

B. Training

All NRCC IT users are required to complete IT security training on an annual basis through the Commonwealth of Virginia's MOAT system. MOAT training includes college-specific policies and procedures which must be accepted before completion of training can be certified.

IV. ENFORCEMENT

The college's ISO is responsible for ensuring that all users complete the training within the specific guidelines.

Security Monitoring

I. PURPOSE

The purpose of this policy is to ensure that IT security controls are in place, are effective, and are not being bypassed.

II. POLICY

The System Owner or his/her designee will ensure that security monitoring is used to confirm that security practices and controls are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other logs and error files

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. Wherever possible, a security baseline has been developed and the tools report exceptions in:

- Internet traffic
- Electronic mail traffic
- LAN traffic, protocols, and device inventory
- Operation system security parameters

In addition, the following checks (monitoring) will be performed at least annually, with or without the use of automated tools.

- Password strength
- Unauthorized network devices
- Unauthorized web servers
- Unsecured sharing of devices
- Operating system and software licenses

III. CORRECTIVE ACTIONS

In the event of a reported security breach, as a result of notification or monitoring, the college's ISO will investigate and recommend appropriate action (including disciplinary action) to the Vice President of Finance and Technology. Where disciplinary action is recommended, the President and Human Resource Officer, and in the case of students, the Vice President for Instruction and Student Services, must be included in the resolution.