RAMAPO COLLEGE OF NEW JERSEY

I.T. HANDBOOK

Last updated: November 9th, 2017

Policies and Procedures Manual

DISCLAIMER

The RCNJ ITS Department regards this document as a work in progress. Because of this, these policies and procedures undergo regular reviews and modifications. Therefore, it is up to each individual employee or associate to remain current on the updated policies and procedures.

Changes in these policies and procedures after the initial agreement signature date does not allow non-compliance or permit the employee or associate to engage in activities contradictory to the modifications made after the initial agreement signature date.

CONTENTS

ADDITIONAL RESOURCES

Acceptable Use Policy

OVERVIEW

This policy establishes the acceptable usage guidelines for all RCNJ-owned technology resources. These resources can include, but are not limited to, the following equipment:

- Computers
    - Desktop Computers, Mobile Devices, Servers, etc.
- Network Equipment
    - Switches, Routers, Network and Communications Cabling, Wall Plates, Wireless Antennas,Wireless Bridge Devices, Fiber Optic Lines, Fiber Optic Equipment, VoIP Phones, etc.
- Audio/Video Equipment
    - Video Codecs, HDTVs, Document Cameras, Projectors, Security Cameras, Miscellaneous Cabling, Digital Cameras and Camcorders, Printers, Copiers, Fax Machines, etc.
- Software
    - Operating Systems, Application Software, etc.
- Resources
    - Group Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at RCNJ, including any and all personnel affiliated with third parties, including vendors. This policy applies to all equipment that is owned or leased by RCNJ.

POLICY

While RCNJ's ITS Department desires to provide a reasonable level of freedom and privacy, users should be aware that all RCNJ-owned equipment, network infrastructure, and software applications are the property of RCNJ and therefore are to be used for official use only. Also, all data residing on RCNJ-owned equipment is also the property RCNJ and therefore, should be treated as such, and protected from unauthorized access.

The following activities provide a general roadmap to use RCNJ's technology resources in an acceptable manner:

- All passwords used to access RCNJ systems must be kept secure and protected from unauthorized use.
- No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Do not transfer personally identifiable information on portable equipment and storage devices.

- Public postings by employees from a RCNJ email address should contain the following disclaimer stating that the opinions expressed are strictly their own and not necessarily those of RCNJ, unless the posting is in the course of business duties:
    - Any views or opinions presented in this message are solely those of the author and do not necessarily represent those of Ramapo College Of New Jersey. Employees of Ramapo College Of New Jersey are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by electronic communications. Any such communication is contrary to RCNJ policy and outside the scope of the employment of the individual concerned. RCNJ will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.
- All computers residing on the internal RCNJ network, whether owned by the employee or RCNJ, shall be continually executing approved virus-scanning software with a current, up-to-date virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders.
- Personally identifiable information cannot be sent via electronic means and should be transferred within the internal network or through secure VPN connections.
- Off-campus work should be completed via a secure VPN connection so that no data is transferred off-network.
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of RCNJ authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing RCNJ-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by RCNJ.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which RCNJ or the end user does not have an active license is strictly prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server environments (e.g., viruses, worms, Trojan horses, rootkits, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a RCNJ computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any RCNJ account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the RCNJ ITS Department is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email [9] for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within RCNJ's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by RCNJ or connected via RCNJ's network.

Accessibility Policy

Overview

This policy establishes the accessibility guidelines for all RCNJ-owned technology resources. The purpose of this policy is to ensure that every RCNJ student, faculty and staff is presented with technological accommodations that provide an equal opportunity to learn and use the required technology equipment for the purpose of their required occupation. These accommodations must be met where any learning impairment exists for any RCNJ student or work limitation exists for any RCNJ employee. These types of accommodations may include, but are not limited to, the following applications or devices:

- Screen reading software
- Screen magnification software
- Stereo headsets or other sound devices

This policy applies to all RCNJ-owned technology resources in labs and other learning areas for student use and in departmental or teaching areas for employee use.

POLICY

The RCNJ ITS Department shall make every effort to ensure that each student and employee has access to and use of information and data that is comparable to the access to and use of the information and data by students/employees who are not individuals with disabilities.

The RCNJ ITS Department will strive to offer technology solutions that help improve the learning environments for all students but will be particularly diligent in ensuring that no student will be unable to learn within a classroom due to a physical impairment or learning disability of some kind. The same will be provided for any employee requiring accommodation due to a physical impairment or learning disability of any kind.

Please note that advance notice of these needs is required and may change due to the request. For instance, additional software needs will take some time to produce an order and install the software. It is imperative that requesters give an adequate amount of time for installation of any accommodations and/or troubleshooting methods.

Please note the RCNJ ITS Department cannot be held liable for issues surrounding software application issues or hardware failures. The ITS department will do our best to assist with troubleshooting issues as they arise. Troubleshooting may include, but is not limited to, the following: contacting outside vendors, basic troubleshooting methods, or referring the requester to vendor resources.

The RCNJ ITS Department will continually strive to ensure that all learning environments have the necessary technology and are adequately structured in a way to provide the most conducive learning environment possible, regardless if a learning disability or physical impairment may be present for any student. The RCNJ ITS Department will also ensure that all employee areas are adequately designed to facilitate a productive working environment as well.

Auditing Policy

Overview

This policy addresses third-party entities and their ability to conduct an internal technology audit. This type of audit is basically a “stress-test” on our technology resources to evaluate the level of security our technology systems present as well as the level of scrutiny it can withstand.

Vulnerabilities are a primary focus for the RCNJ ITS Department. Seeking these vulnerabilities out before they develop into potential problems is best for RCNJ, its resources, employees, associates, and students. To accomplish this, internal audits are necessary to periodically determine what vulnerabilities may exist within RCNJ’s technology resources.

The purpose of this agreement is to set forth a policy regarding network security scanning offered by a third-party audit group to RCNJ. The RCNJ ITS Department shall allow the utilization of various methods (both hardware and software) to perform electronic scans of our networks, firewalls, and other hardware devices located at RCNJ.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents to ensure conformance to the established RCNJ ITS Department’s security policies
- Monitor user or system activity where appropriate

POLICY

This policy covers all computers, equipment, and communication devices owned or operated by RCNJ. This policy also covers any computers, equipment, and communications devices that are present on RCNJ premises, but which may not be owned or operated by Ramapo College Of New Jersey. The third-party audit group will not perform Denial of Service activities at any time during an audit.

When requested, and for the purpose of performing an audit, consent for the access required to perform the scan will be provided to members of the third-party audit group by the RCNJ ITS Department. The RCNJ ITS Department hereby provides its consent to allow the third-party audit group to access its networks, firewalls, and other hardware devices to the extent necessary to perform the scans authorized in this agreement. The RCNJ ITS Department shall provide protocols, addressing information, and network connections sufficient for the third-party audit group to perform network scanning. The access involved in the scan may include:

- User level and/or system level access to any computing, networking equipment, and communications devices
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on RCNJ equipment and/or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on RCNJ networks

Since RCNJ gains access to certain resources from third-party entities, cooperation from these resources may be required to perform a full network scan. For instance, RESNet provides the Internet connections to the RCNJ networks. Because of this, a comprehensive network scan may require the assistance of RESNet or other third-party service providers should part of the scanning activities originate outside the RCNJ network.

Network performance and/or availability may be affected by the network scanning. The RCNJ ITS Department releases any third-party audit group of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result of the third-party audit group's gross negligence or intentional misconduct.

The RCNJ ITS Department shall identify, in writing, a person to be available should the third-party have questions regarding data discovered or should the third-party require assistance.

RCNJ and the third-party audit group shall identify, in writing, the allowable dates for the audit vulnerability scan to take place. Permission to conduct a vulnerability scan will be obtained from the Director of ITS, the President, or a designee a minimum of 48 hours prior to the test.

Backup Policy

Overview

The RCNJ ITS Department maintains systems to hold and retain all essential data for each individual department. This storage area, or shared drive as it is referred to, is used to securely store all data for any given department. Because of this centralized storage arrangement, the RCNJ ITS Department is able to offer secure backup capability ensuring all data will be accessible in the event of a disaster or other event in which the data would be destroyed.

This policy establishes regular backup schedules for our shared drive storage devices and pertains to all this data. With that said, this does not pertain to individual, departmental, or computer lab devices, mobile devices, or other portable storage medium where the data resides locally on the device or medium. The RCNJ ITS Department does not guarantee backup for any of these types of devices or storage medium.

POLICY

Every effort shall be made by the individual departments and employees at RCNJ to store sensitive, important, and confidential data on their respective shared drive. As mentioned above, the RCNJ ITS Department cannot be held liable for issues with data stored elsewhere.

Regular backup schedules are in place within the shared drive storage device to ensure that backups occur at regular intervals and over a time span to provide ample opportunity for the RCNJ ITS Department to recover a file, folder, or group of such. It should be noted that the RCNJ ITS Department does require immediate notification in the event a file, folder, or collection of either is found to be missing, corrupt or otherwise damaged. Waiting to inform the RCNJ ITS Department decreases the probability of successful recovery.

The hardware that the RCNJ ITS Department uses consists of two Dell EqualLogic storage devices, StorageTek SL500 Tape Library, Sun StoreEdge L25 Tape Library. These storage units reside in the E Wing computer room as well as the ASB basement.

Normal backups do not necessarily retain the same meaning as when used in conjunction with other hardware devices. Because of this, the following descriptions are provided, based on the current hardware being used, so as to better understand the overall backup process.

- Full Backups: These refer to full backup taken on the day the backup is scheduled. These backup will contain all files included in the backup policy.
- Cumulative Incremental Backups: These refer to the backup of the files that are new or changed since the last full backup.
- Differential Incremental Backups: These refer to the backup of the files that have changed since the last backup (whether full or incremental backup)

- Catalog Backups: This refers to the internal databases that contain information about NetBackup backups and configuration. This includes records of the files that have been backed up and the media on which the files are stored. The catalogs also contain information about the media and the storage devices.

- Vaulting: This refers to the process of replicating all data and backups so that a mirror copy is retained at Iron Mountain location for off-site backup capability should a disaster or other issues occur.

Regularly scheduled backups shall be performed by the RCNJ ITS Department using the following schedule:

Daily Cumulative Incremental or Differential Incremental Backups

- 6:00 p.m. – 6:00 a.m.
- Every day, between the hours as noted.

Weekly Full Backups

- Between Friday – Sunday Starting at 6:00 p.m. on Friday and anytime between Saturday - Sunday

Catalog Daily Backup

- 12:01 a.m.

Vaulting Weekly

- 3:00 p.m. – 8:00 p.m.
- Saturday

All restoration processes will follow, at minimum, one of the following methods:

- Copying all files or a subset of files from the backup equipment to the file server
- Utilizing the RCNJ ITS Department’s Disaster Recovery Plan
- Utilizing the RCNJ ITS Department’s Backup Priority List
- Other methods, approved by the RCNJ ITS Department, that do not interfere with access or otherwise cause any data loss on the file server

If it is found that a scheduled backup process is incomplete or missing due to a hardware or software malfunction, then the backup will be completed as soon as possible and a hardware test will be needed to verify no long-term problems exist that may affect backups in the future. Should a hardware test yield results that indicate serious issues, then a replacement for the faulty hardware should be found as soon as possible in order to prevent such issues from occurring in the future.

The following is the maximum number of backups and replications that the RCNJ ITS Department will retain at any one time. Once these backups or replications reach the maximum count, the oldest will be recycled so that the newest may be retained.

- Daily Backup
  - Copies on file: 1 per day
  - 30 days worth of data at daily interval (unless configured differently by request)

- Weekly Backup
  - Copies on file: 1 total
  - 30 worth of data at weekly intervals (unless configured differently by request)

- Weekly Replication
  - Copies on file: 1 total (on essentials servers)
  - 1 week worth

Banner (Ellucian) Maintenance Procedure

Overview

Upgrades and patches are performed on a regular basis based on Banner user population needs. In general, this maintenance is performed at a chosen quiet time, usually Sunday mornings. Notification of the maintenance date is sent out ahead of time to the Banner user population. This gives users the opportunity to confirm the date or request another date for said maintenance. Maintenance is usually performed on a monthly basis or close to that time span. Several requests may be implemented at the same time. Only under pre-approved emergency circumstances will maintenance be performed more than once per month.

Policy

Requests to put upgrades and patches in our test instances can be made via email and must come with the date when testing will be complete. These upgrades/patches will be loaded into both BAN8 and TST8 instances, so these instances will be identical in their structure. To be considerate of other colleagues, testing should take no longer than two weeks.

Requests for copy down to be performed can be made via email and will be performed only when the Banner Production instance and Banner TST8 and BAN8 instances are identical. If there are patches and upgrades being tested out in BAN8 and TST8 and these same patches and upgrades are not in Banner Production, no copy down will occur.

Email requests should be sent to the Director of Applications. The request must either come directly from the unit head or from a representative with the unit head being copied on the request. The Director of Applications or representative will get back to the requestor to confirm.

Change Management – ITS – Changes to Applications

Overview

System applications used by the college are typically updated on a scheduled basis. However, there are instances in which patches and upgrades need to be applied within a certain time frame and usually with the upmost urgency for the business function of the college. The following steps are strict guidelines that are in place in order to create a smooth transition for modifications installed from the Test environment to Production.

Policy

- Requestor contacts Director of Applications either by phone or email. If request is via phone, either Director or Requestor will follow up with an email.
- Director of Applications and Programmer(s) will determine if request can and should be done, or find an alternative, viable solution to the request, if available. Communication to Requestor will be sent for either a no-go or a go-ahead for the requested modification.
- If Modification is given the go-ahead by Director of Applications, Programmer(s) and Director will meet with Requestor to gather more detail on modification, stakeholders and deadlines.
    - o Grand Design - Development of Pseudo Code, fleshing out 'What-Ifs' and Exception reporting take place first. This is a collaboration effort between Requestor/Stakeholders and Programmer(s).
    - o Encoding – This will be done in a Test environment first.
    - o Modification Testing in Test – Requestor/Stakeholders test modification, ask for edits (optional) and approve.
    - o Schedule Modification for Production
    - o Send notification to other users of application of scheduled downtime to apply modification.
    - o Apply Modification – Testing done by Programmer(s) and Requestor/Stakeholders

Data Retention Policy

Overview

This policy will determine how long data shall be retained under the guidelines of federal and state law and within institutional policies as dictated herein.

Policy

All data shall be retained, at minimum, the time frame as specified in any current, standing federal or state law. No data residing within any RCNJ facility or technology equipment will knowingly be destroyed prior to this timeframe unless such laws are modified to reflect a new time frame. If such changes do occur, the new timeframe will be susceptible to the new law and all data will be retained within the new specifications.

Under no circumstances is data to be removed, discarded, disposed of, or otherwise destroyed that will compromise legal compliance, data integrity, or institutional needs. The RCNJ ITS Department shall make every effort to extend the data retention timeframes of all data as long as the institution requires access without compromising any legal statues set forth regarding storage or destruction of such data. No data will be destroyed prior to or retained longer than any legal requirement dictates.

The RCNJ ITS Department will continually utilize backup equipment, secondary-site storage, and regular backup schedules to ensure that critical data is retained and kept from corruption or other types of data loss. Every effort shall be made to ensure the institutional data needs are given top priority in the event of a loss of data, corruption of data, or if data recovery is necessary.

This policy shall never decrease the retention time under any state or federal law but may only increase the retention timeframe required by the institution. This increase may only be applicable as long as it does not compromise the integrity, storage capability, or otherwise degrade the overall storage capability of the system being used.

Electronic Communications Policy

Overview

Electronic communication is necessary to fulfill multiple roles and activities here at RCNJ. Because of the varying types of electronic communication, we will focus on those used primarily here at RCNJ:

- Email
- VoIP
- Videoconferencing
- Digital Signage

Email is the official method of communication at RCNJ, both for students and employees. Business is conducted every day via email. Since email has both positive and negative connotations, it is imperative that we recognize that the positive aspects greatly outweigh the negative aspects. However, we must also realize that the negative aspects exist and ensure that this method of communication is used effectively, efficiently, and for its' intended purpose.

RCNJ's VoIP phone system is used to transmit and receive audio/video within the institution to facilitate direct communication amongst employees and departments. It is also used to transmit and receive audio outside the institution to facilitate direct communication with vendors, students, other institutions, and other third-party entities. Because of this capability, we must ensure that it is used for work purposes.

Videoconferencing equipment is used primarily for instructional classrooms requiring connectivity to other RCNJ locations and to local area high schools. Videoconferencing equipment is also used to facilitate conferences and meetings with other institutions, state agencies, or other third-party entities. Since this type of communication conveys not only audio, but video as well, it is particularly important for it to be used for its intended purposes.

Digital signage is used on campus to convey student activities, important academic dates, campus events, and other information to students, employees, and visitors. Since this is also a visual and auditory communication mechanism, it is also important to ensure it is used for its intended purpose as well.

Policy

Regardless of the type of technology being used, electronic communication is meant to serve the needs of the college by sharing information with students, employees, vendors, other state agencies, campus visitors, and other individuals. Because of the unique capabilities of each system it is important to realize that each type of communication method contains unique issues that must be addressed on a case-by-case basis; however, general rules can be set forth to ensure that any communication method is used wisely and according to its intended purpose.

In general, RCNJ's electronic communication mechanisms are to be used to share information with students, employees, vendors, other state agencies, campus visitors, and other individuals.

It is also important to note that the true definition of information sharing at RCNJ is to adequately convey the appropriate knowledge so that the College mission is not hindered but enhanced. This information is always to be distributed under the following assumptions:

Electronic communication from a RCNJ resource:

- is always understood to represent an official statement from the institution.
- shall never be used for the creation or distribution of any information that meets the following criteria:
    - Disruptive
    - Offensive
    - Derogatory
    - Specific comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
    - Any information that could be used to sabotage institutional progress
    - Any personally identifiable information
- shall not be used for personal gain
- shall not be used extensively for personal use
- shall not be used to distribute malicious or harmful software or information.

Emergency Notification Policy

Overview

RCNJ maintains an emergency notification system that is used to notify students and employees who have opted in to the service via Web Self Service. This system is updated daily to reflect the current student data available so that any notification message will be delivered to the required student and employee list.

Policy

The RCNJ Emergency Notification System is to be used, at all times, for emergency purposes or purposes deemed necessary by the President or designee only. The notification system is to be used to send messages via text to email addresses and mobile phones, via voice to office phones, personal phones, and mobile devices, and via applications to desktops and office phones.

At no time shall this system be used for normal messaging, notifications, or otherwise standard contact as this would compromise the importance of these messages and may create an environment where students and employees are able to overlook these types of messages because of the frequency with which they could occur.

With that said, tests of this system shall be conducted once a semester at minimum to ensure the system is functioning properly. Additional tests may be conducted but are not required; however, more than four tests per semester may be too many to retain the importance of such messages when an actual emergency arises requiring the system to be operational.

Only users defined below shall be able to send emergency notification messages via this system:

- RCNJ Vice Presidents
- Other designee deemed necessary by the President

Encryption Policy

Overview

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

While RCNJ employees do not typically use encryption methods to a great extent, it is wise to follow the policy below if encryption of information is necessary on any device residing on campus.

Policy

A proven, standard algorithm such as Advanced Encryption Standard (AES) should be used as the basis for encryption technologies. This algorithm represents the actual cipher used for an approved application.

Additionally, the NSA mentions that AES encryption with 128-bit keys provides adequate protection for classified information up to the SECRET level so this should be the minimum level utilized by any encryption tool. Similarly, Ephemeral Unified Model and the One-Pass Diffie Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA) using the 256-bit prime modulus elliptic curve as specified in FIPS PUB 186-3 and SHA-256 provide adequate protection for classified information up to the SECRET level. During the transition to the use of elliptic curve cryptography in ECDH and ECDSA, DH, DSA and RSA can be used with a 2048-bit modulus to protect classified information up to the SECRET level.

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 the RCNJ ITS Department. 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.

Recent developments in the field of encryption have indicated that it is possible for an encryption key to stay resident in volatile memory long enough after shutdown for it to be stolen and used to break the encryption protecting the associated computer. Because of this, even though the use of encryption is recommended, specific rules are required in order to protect the encryption and, therefore, the data on the drive.

Data at Rest:

- Never leave any PC unattended that contains confidential RCNJ data or a method to access confidential RCNJ data.
- If you must leave a PC unattended that contains confidential information (i.e. in an open office or a conference room), only do so if proper encryption has been enabled and the PC has been powered off for no less than 5 minutes.

- Never authenticate the encryption on a computer which contains confidential RCNJ data or a method to access confidential RCNJ data and leave it unattended, allow a non-RCNJ user to utilize the device, or permit the device to be copied in any way.
- Never disable or bypass the encryption on a computer which contains confidential RCNJ data or a method to access confidential RCNJ data.

Wireless Data Access:

- Any mobile device (I.E laptops and/or cellular device) used to access the RCNJ network must be capable of using wireless encryption for network communication.

Key Management:

- Key management responsibilities may only be delegated to RCNJ administrators who have signed a confidentiality agreement.
- Keys used for digital signatures, digital certificates, and user authentication shall not be given or included in any key arrangements with any third party vendors.

If any user is unsure of the appropriate encryption standard to use or if encryption is necessary, he/she may take advantage of RCNJ's open-door policy and request assistance and information regarding these encryption standards and how to encrypt his/her data to secure it appropriately.

Enforcement Policy

Overview

This policy is to establish enforcement guidelines to ensure that all RCNJ ITS Department policies and procedures are adhered to and observed by all departments and individuals at RCNJ including students, employees, visitors, vendors, etc. Anyone using technology resources at RCNJ will be required to operate within the parameters described in this document or the following enforcement options may be administered.

Policy

All policies herein are applicable to any and all users of technology resources at RCNJ. If it is found that any individual, department, or external entity disobeys the policies and procedures set forth within this document, whether knowingly or unknowingly, then the enforcement of such policy may include, but may not be limited to:

- Forced compliance with the policy
- Suspension of computer privileges
- Disciplinary action including termination of employment, if an employee
- Disciplinary action including expulsion from the College, if a student
- Termination of vendor contract and or service agreement
- Prosecution to the fullest extent of the law

The RCNJ ITS Department should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of any campus computer systems and/or networks. The user community is expected to cooperate with the ITS Department in its operation of computer systems and networks as well as in the investigation of misuse or abuse.

All violations can be reported to the RCNJ ITS Help Desk: 201-684-7777 or helpdesk@ramapo.edu. In the case of an emergency please call the Department of Public Safety, 201-684-6666.

Equipment Configuration Policy

Overview

This policy has been established to create a standard configuration for all technology resources at RCNJ. Because of the variances between the types, makes, models, configurations, builds, versions, and brands of technology resources available, it is necessary to standardize all technology resources to make service and maintenance easier and also to help keep costs down.

Policy

All employees shall order and utilize equipment that is serviceable and recommended by the RCNJ ITS Department. Since equipment availability changes over time, especially when referring to technology, a comprehensive list indicating appropriate hardware would be virtually impossible to create. Because of this, any individual or department wishing to purchase technology equipment should first consult a RCNJ ITS Department personnel member for current specifications for any given piece of equipment.

This applies to any and all technology equipment including, but not limited to:

- Computers (Servers, Desktop, Laptop, Tablets and Mobile Devices, etc.)
- HDTVs
- Printers, scanners, copiers, fax machines, or all-in-one devices
- Projectors, screens, and SmartBoards
- VoIP phones Digital cameras and camcorders Software (Application, Operating System, Network-Based, etc.)
- Other technology equipment not specifically mentioned here

For assistance with set up or configurations place contact the RCNJ ITS Help Desk at 201-864-7777 or helpdesk@ramapo.edu.

Guest/Visitor Access and Technology Use Policy

Overview

RCNJ maintains an atmosphere that is open and allows guests and visitors access to resources, as long as such access does not compromise the integrity of the systems or information contained within the campus and does not introduce malicious software or intent to the internal network.

Policy

Guest and visitor access shall be classified into two types as described below:

- Standard – Access granted to internet resources and institutional resources located online.
- Special – Access granted above plus any internal access as requested by an individual with the authority to do so:
    - Vice President for Fiscal Services, Vice President for Academic Affairs, President, or other designee deemed necessary by the President

Under no circumstances should visitors be given special access unless permission has been obtained from the appropriate administrative personnel (i.e. a signature from one of the personnel above) along with detailed description of access.

For vendor access, please see the appropriate vendor access policy included herein.

Illegal File Sharing

Overview

Legal compliance is a primary focus at RCNJ. Because of this, we have set forth this policy which addresses illegal file sharing legislation, legal alternatives to illegal file sharing, and penalties for violating state and federal copyright laws.

This policy applies to all RCNJ employees, students, vendors, or visitors utilizing RCNJ-owned computers, equipment, or the RCNJ network.

Policy

File sharing (peer-to-peer) software programs have led to significant increases in anti-piracy efforts and legislation. Peer-to-peer software allows the sharing of files often consisting of copyrighted content such as music, movies, and software which usually occurs without the consent of the owner.

It is the policy of RCNJ to respect copyright ownership and protection given to authors, owners, publishers, and creators of copyrighted work. It is against RCNJ policy for any employee, student, affiliate, or visitor to copy, reproduce, or distribute any copyrighted materials on RCNJ-owned equipment or the RCNJ-managed network unless expressly permitted by the owner of such work.

RCNJ also discourages the use of any file-sharing program as these types of programs may allow copyrighted material to be downloaded to a RCNJ-owned computer or device. Many of these programs automatically place downloaded files in a shared folder on your computer, which means you could be sharing files without your knowledge. This also means that you may be held responsible for illegal file sharing, whether you are aware that copyrighted files are being shared or not.

RCNJ also employs the use of network appliances, equipment, and rules to limit the amount of file-sharing traffic on the RCNJ network. Active blocking of peer-to-peer traffic is used to protect the RCNJ network from unwanted traffic and the presence of potentially malicious files introduced through file-sharing programs.

RCNJ encourages employees, students, affiliates, and visitors to utilize legal alternatives to illegal file sharing. There are a variety of free and pay-per-use options available that can be used instead of illegal file sharing programs. Several of these free and pay-per-use options are listed below; however, this is in no way an all-inclusive list. RCNJ leaves it to the discretion of the employee, student, affiliate, or visitor to decide which alternative to utilize. They are provided herein for reference only and RCNJ does not endorse or provide any guarantee or support for any of the legal alternatives located below.

Educause – Legal Sources of Online Content

Pay-per use services (Per-Song, Per-Album, Per-Movie, etc.) or Subscription-based services (Per-Month)

Amazon: Books/Newspapers, Video, Music, Games

CinemaNow
Zune (Music, Video)
Napster
MP3
AmieStreet
GameTap
OnLive

Netflix
Walmart MP3 Downloads
Blockbuster On Demand
eMusic
I-Tunes
GameFly
Hulu Plus

Free services

Shoutcast
Pandora
Blip.fm
Hulu
Clicker
Music Rebellion
Slacker
ESPN360
CBS
FOX

Live365
Last.fm
YouTube
Joost
[adult swim]
Clicker
iLike
ABC
NBC

Incident Management Procedure

This procedure addresses how incidents should be handled when related to technology. This includes thefts, data corruption, etc.

1. Determine scope of incident.
2. Follow the outlined steps under “Reporting an Incident”.
3. Ensure supervisor of employee that incident has been reported.
4. Inform the Director of ITS.
5. Administration will be notified of incident.
6. Resolution will be drafted given incident scope and individuals involved.

Reporting an Incident

1. Call the Public Safety Department at 201-684-6666 (or extension 6666 if using an internal Ramapo College phone) or come to the Public Safety Department Office located on the ground floor of C-wing, Room C-102. Ramapo College Public Safety TDD 201-684-7011.

2. Provide a clear and distinct description of what the incident was about, who was involved, where it took place, when it took place, and, if you know, how or why it came about. Be as specific as possible and give your own name and those of other witnesses.

3. If the emergency appears to be immediately life or public safety threatening, or involves the commission of a serious crime, call 9-911. (Calls from internal Ramapo phones, including those in the residence facilities, must be made by dialing “9” first and then 911, otherwise 911.) Be advised that ambulances, which are staffed by volunteers, are dispatched only by the Mahwah Police. Similarly, the volunteer Fire Department is sent to the College by the Mahwah Police Department. Do not call 9-911 unless an immediate and true emergency exists. The non-emergency Mahwah Police phone number is 201-529-1000.

4. Crimes or violations of College policies may also be reported to employees who do not work in the Public Safety Department but who are involved with student and campus activities. **All College personnel who learn of a crime must report the incident to the Public Safety Department.** Employees who are told about the commission or probable commission of a crime must report this information promptly to the Public Safety Department by going to room C-102 or calling extension 6666. The Public Safety Department will, in turn, notify the Mahwah Police Department so a formal investigation can begin. The staff of the Center for Health and Counseling Services is exempt from this specific reporting requirement, although, if a client discusses with a counselor knowledge of a crime, the counselor will explore options with the client including the voluntary reporting of that crime to the proper authorities.

5. Reports concerning campus crimes made to any College official become part of the official crime statistics for the College which are then published in accordance with the Jeanne Clery Disclosure of Campus Public Safety Policy and Campus Crime Statistics Act. Each year representatives from the Office of Student Conduct, the Public Safety Department, and Student Affairs meet to compile the crime statistics and prepare the annual report. In addition, the Public Safety Department consults with the Mahwah Police Department to corroborate all data. Public notices regarding campus crimes will be published on short notice if a danger to the College community persists.

Information Sensitivity Policy

Overview

Information sensitivity is a primary focus at RCNJ. Since we are an educational entity, we deal with many different types of information, some for public use, some not. To make these distinctions, this document will address both types of information.

This policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of RCNJ without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as via phone and videoconferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect confidential information (e.g. confidential information should not be left unattended in conference rooms.).

NOTE: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your supervisor or the RCNJ ITS Department. Questions about these guidelines should be addressed to the RCNJ ITS Department.

Policy

By grouping information into two different categories, we can adequately address the needs of each type of information. The first type, public information, is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the institution. The second type, confidential information contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as specific personnel information, student data, billing information, etc. Also included in confidential information is information that is less critical, such as telephone directories, personnel information, etc., which does not require as stringent a degree of protection.

A subset of the latter is third-party confidential information. This is confidential information belonging or pertaining to another corporation which has been entrusted to RCNJ by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into RCNJ's network to support our operations.

RCNJ personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor and/or the RCNJ ITS Department for more information and instructions on how this information should be handled.

The sensitivity guidelines below provide details on how to protect information at various sensitivity levels. Use these guidelines as a reference only, as RCNJ Confidential Information at each level may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the RCNJ Confidential Information in question.

- Minimal Sensitivity
  - Description: General information, some personnel, and technical information.
  - Access: RCNJ employees, associates, or third-parties with a business need to know.
  - Distribution internal to RCNJ: Approved electronic mail and approved electronic file transmission methods.
  - Distribution external to RCNJ: Approved electronic mail and approved electronic file transmission methods.
  - Storage: When viewing data, do not allow viewing by unauthorized individuals. Do not leave data open and/or unattended in any format. Protect data from loss, theft, or misplacement. Electronic information should have individual access controls where possible and appropriate.
  - Disposal/Destruction: Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.
- More Sensitive
  - Description: Business, financial, technical, and most personnel information.
  - Access: RCNJ employees, associates, or third-parties with signed non-disclosure agreements with a business need to know.
  - Distribution internal to RCNJ: Approved electronic file transmission methods.

  - Distribution external to RCNJ: Approved electronic file transmission methods via a private link to approved recipients external to RCNJ locations.

  - Storage: Individual access controls are highly recommended for more sensitive electronic information.

  - Disposal/Destruction: Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

- Most Sensitive

  - Description: Operational, personnel, financial, source code, and technical information integral to the security of the institution.

  - Access: Only those individuals (RCNJ employees and associates) designated with approved access and signed non-disclosure agreements.

  - Distribution internal to RCNJ: Approved electronic file transmission methods.

  - Distribution external to RCNJ: Approved electronic file transmission methods to recipients within RCNJ. Strong encryption is highly recommended.

  - Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored on a physically secured computer.

  - Disposal/Destruction: A necessity. Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

Internal P-Shared Access Policy

Overview

This policy establishes the official rules set forth to allow users to access and manipulate information shared through the network P - shared drive.

Policy

Any user who seeks to request access to the network shared drive must complete and submit a Request for Shared Network Drive Creation and Rights form. Please note any user seeking to gain access to the P-Drive must have approval from their department administrator. The form must be submitted to the ITS Help Desk; please allow a maximum of two (2) business days for the rights to be granted.

Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of RCNJ's entire network. As such, all RCNJ employees (including contractors and vendors with access to RCNJ systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to RCNJ, resides at any RCNJ location, has access to the RCNJ network, or stores any RCNJ information.

Policy

All passwords will meet the following criteria:

- It is suggested that all system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- It is suggested all user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used for various purposes at RCNJ. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every RCNJ employee should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password or a subset of the password is a word found in a dictionary (English or foreign)

- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - The words “RCNJ”, “ramapo”, “state”, “college” or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain between 8 and 32 characters
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain at least one number (e.g., 0-9)
- Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
- Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
- Does not contain personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

NOTE: Please do not use either of these examples as passwords!

Do not use the same password for RCNJ accounts as for other non-RCNJ access (e.g., personal ISP account, option trading, benefits, etc.). Do not share RCNJ passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential RCNJ information.

Here is a list of “dont’s”:

- Don’t reveal a password over the phone to ANYONE.
- Don’t reveal a password in an email message.
- Don’t reveal a password to a supervisor.
- Don’t talk about a password in front of others.
- Don’t hint at the format of a password (e.g., “my family name”).
- Don’t reveal a password on questionnaires or security forms.
- Don’t share a password with family members.
- Don’t reveal a password to co-workers.
- Don’t reveal a password to vendors.
- In short, don’t reveal a password to ANYONE.

- Do not use the “Remember Password” feature of applications (e.g.,Internet Explorer, Firefox, Chrome, Safari, ect.).
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer without proper encryption.
- Change passwords at least once every three months.

Other items to remember:

- If someone demands a password, refer them to this document or have them call the RCNJ ITS Department to determine the validity of their request.
- If an account or password is suspected to have been compromised, report the incident to the RCNJ ITS Department immediately and change all passwords as soon as possible.

Password cracking or guessing may be performed on a periodic or random basis by the RCNJ ITS Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Never give your password out to anyone. This may or may not include your supervisor, a friend or relative, a student or part-time worker, or even a co-worker.

Physical Security Policy

Overview

This policy will establish physical security guidelines that apply to all computing and networking equipment locations. It is important to note that incremental degrees of security will be needed for each area depending on the actual equipment configuration and critical need to the institution.

Policy

All areas will be classified into two categories:

- Office
  Office areas are simply that, office locations for RCNJ ITS Department employees. These areas contain computing equipment and other data that should be protected at all times.

- Restricted
  Restricted areas are those areas that belong to the RCNJ ITS Department and contain equipment owned and/or operated by the RCNJ ITS Department or a third-party vendor (i.e. ResNet) such as:

  - Switch closets
  - Server rooms
  - Telecommunications rooms
  - ITS Department storage areas

At the time of this policy, our current physical security offerings are somewhat limited so more advanced options cannot currently be used. As upgrades occur, recommended options will be changed to required options to increase and enhance security.

At minimum, all office and restricted locations require the following security mechanisms:

- Solid wood or steel door
- Either keyed handle or deadbolt lock

All RCNJ ITS Department restricted and office locations should contain the following recommended security mechanisms:

- Reinforced steel doors and frames
- Keyed deadbolt locks
- ID card access

Personally Identifiable Information Policy

Overview

This policy will establish RCNJ's definition of Personally Identifiable Information (PII) and indicate what information may be shared, if any, with third-party entities.

Policy

It is important to note that information should never be shared without cause or requirement, unless dictated by state or federal government regulations such as annual reporting guidelines and statistical reporting data, in the course of preset institutional operations or vendor agreements, or due to the request of RCNJ's President or designee.

PII is the type of information that should be kept safe using the highest level of security. PII is described as information about an individual that identifies, links, relates, or is unique to, or describes him or her. This information may include:

- Name
- Social Security Number
- Address(es)
- Phone Number(s)
- Birth date
- Birth place
- Mother's maiden name
- Family names
- Other family data such as addresses, contact information, etc.
- Financial information such as bank account information, account balances, etc.
- Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have a personal knowledge of the relevant circumstances, to identify the student with a reasonable certainty
- Information requested by a person who the educational agency or institution believes knows the identity of the student to whom the educational record directly relates

Under no circumstances should PII be transported off-campus. On-campus storage of PII should meet other policy requirements as dictated herein. Off-campus use of this type of data may be facilitated via the RCNJ ITS Department's Remote Access Policy.

Personal Technology Service Policy

Overview

This policy will set forth the rules and regulations which will determine how the RCNJ ITS Department personnel are to perform work on personally-owned employee or student technology products.

The RCNJ ITS Department does not service technology equipment for individuals who are not RCNJ employees or students.

Policy

The RCNJ IT Systems Department always strives to ensure that RCNJ employees, students, affiliates, and visitors receive the best possible technology assistance available for us to provide. However, this can leave something to be desired for non-RCNJ, personally-owned technology equipment owned by employees, students, affiliates, and visitors.

This policy will set forth the rules, regulations, and guidelines for which the RCNJ ITS Department personnel may provide services for personally-owned technology equipment and/or projects outside of normal work hours.

NOTE: All technology requests for configuration or connectivity to the RCNJ network from personal technology devices will be handled at no cost. This policy applies only to technology issues related to the personal needs of the user.

All requests for personal technology assistance will begin with a preliminary diagnosis and troubleshooting process which is provided for FREE. If additional work is authorized by the user then the accompanying Helpdesk Ticket Form must be read and signed before any work may begin.

The RCNJ ITS Department offers no implied warranty or guarantee on any work performed on personal technology equipment. All work is performed as-is as a service to our students and as a cost-saving alternative for their benefit. However, it is beneficial to note that all work is performed on the same level as comparable service on RCNJ owned equipment.

All personal technology work will be performed within the following restrictions:

- Personal technology work may be performed during regular business hours, only if such work does not directly interfere or delay the normal operations or job duties of the RCNJ ITS Department employee.
- No on-site work. All equipment must be brought to the RCNJ IT Systems Department for a preliminary diagnosis and troubleshooting.

- No parts purchases. All parts to be installed must be purchased by the user.
- No illegal software. Only legally licensed software may be installed.
- No work without proper authorization signature on consent form.

All issues should be expected to take approximately 24-48 hours to complete; however, they may take longer depending upon the severity of the problem at hand. Please expect to leave any equipment for a minimum of 48 hours for proper problem resolution.

Ramapo College Of New Jersey cannot be held responsible for any work done after hours by RCNJ ITS Department personnel on any personal technology equipment. All work provided is not warranted or guaranteed. By signing the Helpdesk Ticket Form, you agree to these terms and conditions and waive any damages which may occur due to any work on your personal technology equipment. All work is done and once completed is left as is and no standing warranty or guarantee is implied.

Remote Access Policy

Overview

This policy establishes the official rules set forth to allow users to remotely access and manipulate personally identifiable information, network applications, and other data from off-campus.

Policy

Any user who seeks to work off-campus for the purpose of working from home or at another location can facilitate this through the use of the VPN connection. All users needing access to SCT or other applications requiring network connectivity to the campus can facilitate this by connecting from home via a VPN connection.

This type of connection establishes a secure, encrypted connection, to the campus network to allow the user to manipulate and access the data at a distance. At no time should any personally identifiable information be transferred off-campus on any type of device. If a given user wishes to work while off-campus, he/she should use the enclosed Remote Access Procedure to obtain a secure connection to the network and work from a distance.

This type of connection allows the user to remotely manipulate and access the data without actually transferring any data off-site thus ensuring all personally identifiable information and other data is kept safe and secure from unauthorized access.

Please note to request access to the VPN, a user must contact the ITS helpdesk and request it. Instructions and access will be provided at that time pending approval.

Software Lifecycle ITS

Overview

Ramapo College has a small IT group, so homegrown procedures (homegrowns) and applications are held to a minimum. When proven necessary and economical, however, the unit does have the ability and skill set to create homegrowns.

Policy

Our business process is as follows:

• A Unit representative requesting an application/procedure contacts the Director of Applications either by email or phone. If by phone, the Director of Admissions records request in an Excel-like file. That file will be utilized throughout the entire request/development/implementation process. The file will be stored on the P Share Drive.

• Director of Applications brings in programmer(s) and other ITS stakeholders to examine and research the viability of requested process. All will investigate to see if something already in place will provide the same or similar results. If it is deemed that there is no other alternative to the request and we have the skill set to handle the project, we will meet with the requestor to nail down requirements, stakeholders and deadlines. Once that is done, below is the lifecycle:

o Grand Design – This is where most of the time should be spent…examining the process and going through the 'what-if's', developing error reporting, documentation, deciding on the correct tools, languages to use. The Grand Design Stage is a collaboration effort between programmer and user.
o Encoding – Beginning coding will be based on what comes out of the Grand Design Stage.
o Test/Edit Encoding
o User Draft Testing
o User Edits Encoding
o Beta Stage – This stage will last the cycle of unit's business process this project relates to
(ie, Admissions Slate to Banner – cycle is the full Admissions year – August to August).
o Edits to Beta Stage – improvements discovered over Beta Stage.
o Maintenance mode

Student Rights and Responsibilities Policy

Overview

It is the understanding of all students, upon being admitted to RCNJ, that the technology resources and equipment provided are for the benefit of all students. This policy explains what rights students have with respect to this technology and also what responsibilities are expected of each student.

Policy

Every student that attends RCNJ shall be given an equal opportunity to learn and equal access to technology to help facilitate learning. All students, regardless of major, classification, student-type, housing location, or other identifying factor shall receive the same technology access as any other student.

Students should expect to receive access to wireless connections in classrooms, learning areas, common areas, dorms, etc. Students should also expect up-to-date computers in labs and teaching areas, multimedia equipment in most classrooms, state-of-the-art instructional television classrooms, and easily accessible online systems such as Blackboard, RCNJ e-mail, student account, etc. Students should also expect to receive reliable, free internet service while on campus at speeds unobtainable through any normal ISP.

With all of these rights and amenities, the RCNJ ITS Department does make some responsibilities and assumptions of our students. These responsibilities are as follows:

- Students are expected to activate their email accounts prior to the start of class.
- Students are expected to maintain their respective email account through their career at RCNJ.
- Students are expected to utilize their RCNJ e-mail address as it is the official method of communication with RCNJ.
- Students are required to safeguard login credentials and not share user accounts.
- Students are expected to respect others privacy and equipment.
- Students are expected to use only permissible equipment on campus:
    - o Computers such as laptops, desktops, mobile devices, etc.
- Students are to observe prohibited devices in dorm areas:
    - o Personal routers, wireless access points, bridges, or other network equipment.
- Students are expected to observe all local, state, and federal laws concerning technology.
- Students are required to comply with all policies included in this document.

Vendor Access Policy

Overview

This policy will set forth parameters for vendors to abide by when access to our internal or external network, workstations, or servers is required. All vendors, regardless of status, frequency of visitation, work being performed, or size of entity shall abide by this policy at all times unless such work does not require access to the RCNJ network or computing resources.

Policy

All vendors shall notify their contact on campus of any work that will require access to any of the following RCNJ resources:

- Internal network
- External network
- On-campus workstation(s)
- On-campus server(s)
- Network infrastructure
- Any other computing device on campus

Upon notification of the need for access, the RCNJ ITS Department shall create login credentials and access requirements necessary to facilitate the access required for the vendor to complete their job function. Access shall always be restrictive meaning un-warranted or un-needed access will not be available until deemed necessary by the requirements of the project. All requests for access shall be evaluated on a case-by-case basis to ensure that proper access is granted and no un-warranted or un-needed access is given without cause.

At all times, the vendor shall:

- Fulfill their primary job responsibility only.
- Not seek to undermine or circumnavigate the access which has been provided.
- Not tamper or adjust security settings on existing network infrastructure or devices.
- Ensure that access credentials are not shared with anyone other than those individual approved for access.
- Work to ensure that RCNJ's information is kept safe and secure from loss or theft.
- Never disclose any information he or she may come to know from working with or on any RCNJ technology resource with a separate third-part entity.
- Notify the RCNJ ITS Department IMMEDIATELY upon any inclination that loss or theft has occurred, access has been lost or tampered with, or there is a concern that any other type of access violation has occurred.
- Never seek to use any of RCNJ's information for personal or other monetary gain.
- Not use any access or technology resource in a manner that has been prohibited for employees, students, or visitors in any of the other, enclosed policies herein.

Wireless Communication Policy

Overview

Wireless implementations are a benefit to RCNJ as well as its' faculty, staff, and students. Maintaining this equipment can be a tedious process but is a necessity.

At present, this policy allows access to the RCNJ wireless network via any data communication device containing the hardware required to connect. Authenticated faculty, staff, and students, grants users to RCNJ's internal network.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of RCNJ's wireless networking access points. This includes any form of wireless data communication device capable of transmitting packet data.

Policy

All wireless data communication devices connected with RCNJ's wireless network will be required to have current virus-scanning software installed with the most recent updates and perform a full system scan a minimum of once per week.

At no time shall any device connected to the RCNJ wireless network operate outside the parameters defined in the Acceptable Use Policy provided herein. All wirelessly connected devices may be monitored and their information such as IP address, MAC address, general hardware profile, etc. be archived for future use. Random scans may also be performed to ensure the security of the wireless networks and connected devices and to obtain a general device survey to further enhance the accessibility and usability of RCNJ's wireless networks.

RAMAPO COLLEGE OF NEW JERSEY

ITS Helpdesk - E-116 – 201-684-7777	
Student Name:	Extension / Cell:
Dorm / Residence:	
Date / Time Dropped Off:	
Dropped Off: Desktop □ Laptop □ Power Adapter □ Bag □ Other(Please Specify) □ ________________	
Computer Brand:	Password:
Problem:	Solution:

Hardware Problem Checklist:	
Keyboard/Mouse/Touch Pad ___ Stuck Keys (List: ________________) ___ Missing Keys (List: ________________) ___ Broken Touch Pad	Ports ___ HDMI ___ Power Adapter ___ USB ___ Headphone/Audio ___ Ethernet ___ Microphone
Display ___ Cracked Screen ___ Dead Pixels	Speakers/Audio ___ Speakers ___ Microphone
___ Hard Drive	___ Cooling Fan
___ Memory Card Reader (SD, Micro SD, etc.)	___ CD/DVD/Blu-Ray Drive
___ Webcam	___ Other: ______________________________

As a client of the Ramapo ITS Help Desk, I have provided on this inventory the most complete and accurate list of any damage to the hardware I have brought to ITS. I understand neither ITS, nor the Help Desk Technicians are responsible for this damage and I am entitled to no redress over the damage listed above. Any other damage to said hardware existing at the time of hardware drop-off, but not included in this list is not the responsibility of ITS or the Help Desk Technicians. I also understand that some viruses may corrupt the operating system and/or other installed programs on my computer. ITS will do everything we can to ensure your data is retained, however, issues may occur that cause data loss beyond the control of the ITS Department. ITS is not liable for the results of any viruses already on the computer. By signing my name below, I acknowledge that I understand the above policies and agree to be bound by them.

SIGNATURE: ____ DATE: ___________________

Incident Management Procedure

This procedure addresses how incidents should be handled when related to technology. This includes thefts, data corruption, etc.

1. Determine scope of incident.
2. Follow the outlined steps under "Reporting an Incident".
3 . Ensure supervisor of employee that incident has been reported.
4. Inform the Director of IT Systems.
5. Administration will be notified of incident.
6. Resolution will be drafted given incident scope and individuals involved.

Reporting an Incident

1. Call the Public Safety Department at (201) 684-6666 (or extension 6666 if using an internal Ramapo College phone) or come to the Public Safety Department Office located on the ground floor of C-wing, Room C-102. (Ramapo College Public Safety TDD (201) 684-7011.)

2. Provide a clear and distinct description of what the incident was about, who was involved, where it took place, when it took place, and, if you know, how or why it came about. Be as specific as possible and give your own name and those of other witnesses.

3. If the emergency appears to be immediately life or public safety threatening, or involves the commission of a serious crime, call 9-911. (Calls from internal Ramapo phones, including those in the residence facilities, must be made by dialing "9" first and then 911.) Be advised that ambulances, which are staffed by volunteers, are dispatched only by the Mahwah Police. Similarly, the volunteer Fire Department is sent to the College by the Mahwah Police Department. Do not call 9-911 unless an immediate and true emergency exists. The non-emergency Mahwah Police phone number is (201) 529-1000.

4. **All College personnel who learn of a crime must report the incident to the Public Safety Department.**

Terms and Definitions

Appropriate Measures

Refers to the measures that the RCNJ ITS Department is authorized to take to secure RCNJ's computing resources. This may refer to measures concerning RCNJ owned hardware or software, data, employees, students, associates, visitors, etc. The RCNJ ITS Department must maintain an appropriate measures option so that RCNJ is protected, concerning both equipment and information.

Approved Electronic File Transmission Methods

Includes supported FTP clients including, but not limited to, FileZilla, SecureFTP, and SmartFTP. This also includes supported Web browsers including, but not limited to, Microsoft Internet Explorer, Mozilla Firefox, Chrome, Safari, Netscape Navigator, and Opera. If you have a business need to use other mailers contact the RCNJ ITS Department prior to implementation.

Approved Electronic Mail

Includes all mail systems supported by the RCNJ ITS Department. This includes, but is not limited to, RCNJ G-mail, Outlook configured email, and configured email on mobile devices. If you have a business need to use other mailers contact the RCNJ ITS Department prior to implementation.

Approved Encrypted Email and Files

Techniques include the use of AES and others. Please contact the RCNJ ITS Department for further information.

Asymmetric Cryptosystem

A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Chain email or letter

An email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck and/or money if the directions are followed.

Configuration of RCNJ-to-Third Party Connections

Connections shall be set up to allow third parties requiring access to the RCNJ campuses, networks, data, etc. These connections will be setup in order to allow minimum access so that third-party entities will only see what they need to see, nothing more. This involves setting up access, applications, and network configurations to allow access to only what is necessary.

Domain Name System

Essentially serves as the Internet “phone book” by associating various domain names (i.e. http://www.connorsstate.edu, http://it.connorsstate.edu) with their counterpart IP addresses that the computers and networking equipment need to transmit data.

Email

The electronic transmission of information through a mail protocol such as SMTP, IMAP, or Exchange. Typical email clients include Mozilla Thunderbird and Microsoft Outlook.

Encryption

This refers to the modification and storage of data by manipulating the way it is stored through the use of an algorithm. An encryption key is required to gain access to the original data and therefore provides the security desired.

Encryption Key

A software key used to gain access to encrypted data.

Expunge

To reliably erase or remove data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac’s normal erasure routine keeps the data intact until overwritten which may allow the PC to actually retain the “deleted” information for some time after the deletion took place.

Forwarded email

Email received from one sender and then sent to another recipient.

Information System Resources

Information System Resources include, but are not limited to, all computers, peripherals, data, and programs residing on the RCNJ Campuses, networks, servers, etc. These resources also include all paper information and any information for internal use only and above.

Information Technology Systems

The technology department responsible for managing RCNJ’s computing resources.

Individual Access Controls

Methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. This includes the utilization of passwords, screensavers, hardware encryption, etc.

Insecure Internet Links

All network links that originate from a locale or travel over lines that are not totally under the control of RCNJ. These types of connections can allow an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection.

Internet

A worldwide, publicly-accessible series of interconnected networks used to transmit packets of data via the Internet Protocol (IP).

Internet Protocol

A data-oriented network protocol used to transmit data across a packet-switched network such as the Internet.

Local Area Network

A computer network covering a small geographic area. These can include a single campus, a single building, or even a single room.

One Time Password Authentication

This type of authentication is accomplished by using a one-time password token to connect to a network resource or reset a network account. As long as the connection remains open the password token is retained and access is allowed.

Personal Computer

A device used by a single user to access local programs and files, network resources, or the Internet. This can include desktop, laptop, tablet, or portable computers.

Physical Security

Physical security refers to the actual physical security mechanisms in place to prevent unauthorized access to technology resources. This can also mean having actual possession of a computer or by locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room, in a vehicle, on an airplane seat, etc. Make arrangements to lock the device in a secure location such as a hotel safe or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer, cabinet, safe, etc. or simply take it with you.

Private Link

An electronic communications path for which RCNJ has control over the entire distance. These types of links typically use a VPN tunnel or other means to connect two or more locations. For example, all RCNJ networks are connected via a private link.

Proprietary Encryption

An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Public Link

An electronic communications path for which RCNJ does not have control over the entire distance. This connection does not utilize any special connection scheme. A connection from any RCNJ computer to the Internet is an example of a public link.

Secure Internet Links

All network links that originate from a locale or travel over lines that are either under the control of RCNJ or utilize technology to form a secure “pipe” for information to traverse. These types of connections prohibit an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection by solely utilizing the RCNJ network or utilizing a secure authentication mechanism to connect.

Sensitive information

Information is considered sensitive if it can be damaging to RCNJ, its employees, students, associates, etc. This information can include personnel data, student information, purchasing information, etc.

Symmetric Cryptosystem

A method of encryption in which the same key is used for both encryption and decryption of the data.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to individuals, either internal or external to RCNJ, who do not have a need to know that information.

User Authentication (Local)

A method by which the user of a system can be verified as a legitimate user on that system only.

User Authentication (Network)

A method by which the user on a network can be verified as a legitimate user independent of the computer or operating system being used.

Virtual Private Network

A network that functions as a single, secure network that is usually comprised of several locations residing in separate geographic areas. This is accomplished through the use of secure, authenticated connections from one network to another.

Virus Warning

Typically, these are emails containing warnings about virus or mal-ware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users. However, the RCNJ ITS Department occasionally sends out virus warning should the need arise. In these cases, recipients should heed the warnings provided by the ITS Department employees rather than treat the information as potentially misleading.

Wide Area Network

A computer network covering a large geographic area. The Internet is an example of a WAN.

Ramapo College of New Jersey
Information Technology Services
Request for Shared Network Drive Creation and Rights

Please completely fill out this form in order for us to create and maintain rights to shared directories on the network (P:Drive) between users and departments. Submit the completed form to the ITS Help Desk. Please allow a maximum of two (2) business days for the rights to be granted.

Name ____ **Date** ____________________
Dept ____ **Extension** __________________

☐ ***CREATE A NEW DIRECTORY***

I wish to ***create a new directory*** on the network (P drive) for file sharing purposes.
Name the directory: ________________________________ .
Please allow the following users from the following departments to access this directory:

Ramapo Email UserID	Dept	Available Permissions to Grant (Circle ***only*** ONE per user)*	
______________________	____________	Full Access (Read, Write, Erase)	Read Access Only
______________________	____________	Full Access (Read, Write, Erase)	Read Access Only
______________________	____________	Full Access (Read, Write, Erase)	Read Access Only
______________________	____________	Full Access (Read, Write, Erase)	Read Access Only
______________________	____________	Full Access (Read, Write, Erase)	Read Access Only

☐ Check here and continue on the back of this sheet ***if* you have more users to add** to this list.

☐ ***EDIT ACCESS TO AN EXISTING DIRECTORY***

I wish to ***change user permissions*** for a directory on the network (P drive).
What is the name of the directory on the network? P:\Shared\_______________________________________

Email User ID	Circle Desired Change	Email User ID	Circle Desired Change
__________	Add read-only access Add full access Convert to read-only access Convert to full access Revoke all access	__________	Add read-only access Add full access Convert to read-only access Convert to full access Revoke all access
__________	Add read-only access Add full access Convert to read-only access Convert to full access Revoke all access	__________	Add read-only access Add full access Convert to read-only access Convert to full access Revoke all access

Check here and continue on the back of this sheet *if* you have more users to add to this list.

OFFICE USE ONLY:
Directory Path: ____
Group Name(s): ____
OU Where Group Resides: ___________________________ Directory Owner: ___________________________

THIS PAGE WAS INTENTIONALLY
LEFT BLANK