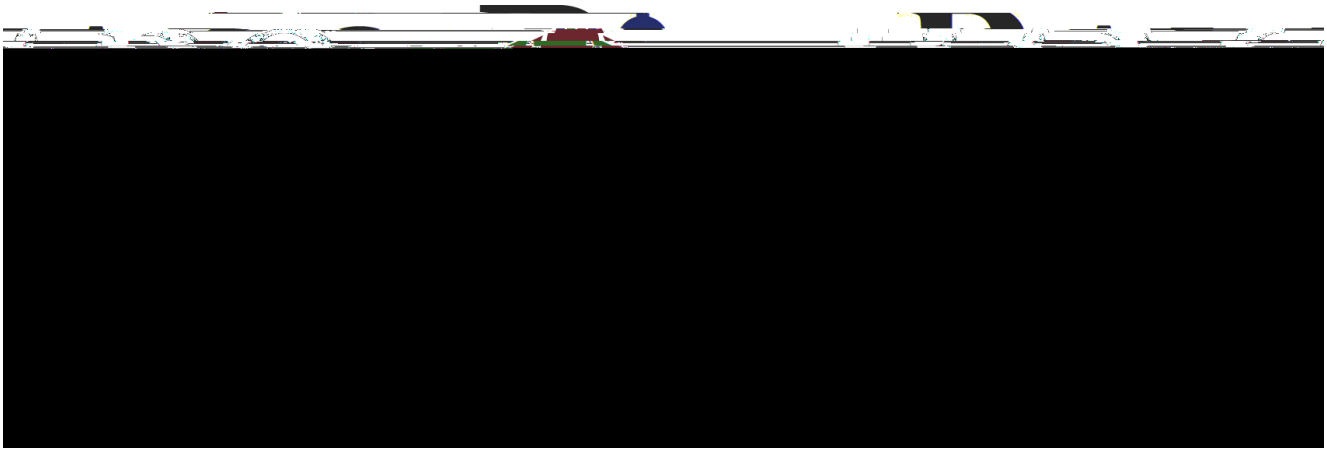

I.T. HANDBOOK

Last updated: November 27, 2018

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.

Table of Contents

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

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be

Accessibility Policy

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

Auditing Policy

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

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

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,

- 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.

-

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

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.

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

Data Retention Policy

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.

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

Electronic Communications Policy

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:

-

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
    - Of >>BsruptiveEuets /TT0 1 Tf0 Tw 12 0 0 12 p5y<FEFF0009>>> BDC ( )TjE

Email Security Maintenance

Email security maintenance for the college is performed to prevent unauthorized users/accounts from soliciting/Spamming the college with unauthorized/unapproved content. The maintenance also provides authorized users to only send a received appropriate content to certain groups depending on their security level.

- 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.

Equipment Configuration Policy

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.

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

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.

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:

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

Amazon: Books/Newspapers, Video, Music, Games

CinemaNow
Netfix
Zune (Music, Video)
Walmart MP3 Downloads
Napster
Blockbuster On Demand
MP3
eMusic
AmieStreet
I-Tunes
GameTap
GameFly
OnLive
Hulu Plus

Free services

Shoutcast
Live365
Pandora
Last.fm
Blip.fm
YouTube
Hulu
Joost
Clicker
[adult swim]
Music Rebellion
Clicker
Slacker
iLike
ESPN360
ABC
CBS
NBC
FOX

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

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 con f dential 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

- 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.

  -

Internal P-Shared Access Policy

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

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

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.

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

- 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.

Personal Technology Service Policy

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.

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 onm[a.4912 Tm>>B(o)4h000F0010045H7. orvt2

- 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.

RCNJ Email Account Creation Procedure

Anyone with an active student or employee record at Ramapo College is entitled to an RCNJ email account. These accounts are created on an automated basis. As of Class of 2010, RCNJ Alumni are provided email for life. After graduation, their email account is switched over to an alumni account. For those RCNJ Alumni who do not already have an RCNJ email account, they can request one by contacting alumni@ramapo.edu.

For RCNJ Applicants/Students:
When an applicant to Ramapo College is accepted by the institution, the applicant is placed into the email procurement process.

For RCNJ Employees:
Once an employee is hired, they will have an active employee record. When that record is activated, they are placed into the email procurement process.

Email Procurement Process:
To be successfully processed, the person must have a date of birth, Banner ID, First Name and Last Name. During the weekdays, this process runs on an hourly basis during work hours. On the weekend, the process runs once daily. Once the account is processed, the person can activate their email by going to:

Email Activation:
To activate their email, the student or employee must enter their Banner_ID and Date of Birth. They then must check the box agreeing that their RCNJ email is an official form of correspondence. See screenshot below:

Notes:
The Email Username (The email account minus ‘@ramapo.edu) and password are also used for logging into a laptop or workstation on campus, as well as for other processes on campus that require a secure login.

Remote Access Policy

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.

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

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.

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 file. That file will be utilized throughout the entire request development

Student Rights and Responsibilities Policy

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.

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:
    - Computers such as laptops, desktops, mobile devices, etc.
- Students are to observe prohibited devices in dorm areas:
    - 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.

Wireless Communication Policy

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.

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.

ITS Helpdesk - E-116 ï 201-684-7777	
Student Name:	Extension / Cell:
Dorm / Residence:	
Date / Time Dropped Off:	

Dropped Off: Desktop Laptop Power Adapter Bag Other(Please Specify)_____

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.

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

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

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

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

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 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