Information Technology Policy Guidelines

Limestone College
Limestone College’s information systems are only to be used by current employees, enrolled students, and approved vendors. The said constituents may only use Limestone College’s information systems in the intended manner and reason as granted to their account. Any attempt by anyone to access Limestone College’s information systems apart from the approved manner, reasons, and constituents stated in this policy are subject to disciplinary actions that may also include local and federal prosecution.
# Table of Contents

Antivirus Policy ................................................................. 1  
Cellular Use Policy ............................................................. 3  
Copyright Policy ...................................................................... 4  
E-Mail Acceptable Use Policy ............................................... 6  
Employee Departure Checkout Checklist ................................ 9  
Internet Acceptable Use Policy .............................................. 10  
Laptop Policy .......................................................................... 12  
Limited Personal Use of Network Resources ....................... 15  
Add/Move/Change Policy ....................................................... 17  
Password Policy ....................................................................... 18  
Printer Policy ........................................................................... 20  
Server Space Usage Policy ..................................................... 21  
Software Installation Policy .................................................... 22  
Telephone and Voicemail Acceptable Use Policy ............... 24  
Third-Party Access Policy ....................................................... 26  
Server Backup Policy .............................................................. 29  
Devices on the Network ............................................................. 31
**Antivirus Policy**

**Purpose**

A virus is a piece of potentially malicious programming code that will cause unexpected or undesirable events. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, or CDs. Viruses are usually disguised as something else; therefore, their presence is not obvious to the computer user. A virus infection can be very costly to Limestone College in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Limestone College is to provide a computing environment that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Limestone College employees to help achieve effective virus detection and prevention.

**Scope**

This policy applies to all computers that are connected to the Limestone College network. This includes both College owned and personally owned computers connected to the Limestone College network. The definition of computers includes desktop and laptop computers, servers, smartphones, and all other forms of handheld computing devices.

**General Policy**

- Currently, Limestone College uses Microsoft Forefront® software to mitigate potential virus threats. Licensed installations of Microsoft Forefront® can be obtained from the Help Desk at extension HELP (4357). The most current available version of the anti-virus software package will be taken as the default standard.

- All computers attached to the Limestone College network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

- Any activities with the intention to create and/or distribute malicious programs onto the Limestone College network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

- If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report their concerns to the IT department immediately by calling the Help Desk at extension 4357. When reporting his/her virus concerns, include as much information as possible, such as: virus name, extent of infection, source of virus, and potential recipients of infected material.

- No employee should attempt to destroy or remove a virus or any evidence of a virus without direction from the IT department.

- Any virus-infected device will be removed from the network until it is verified as virus-free.

**Rules for Virus Prevention**

- Run the standard anti-virus software provided by Limestone College.

- Do not open any files or macros attached to e-mail from an unknown, suspicious, or untrustworthy source.
• Do not open any files or macros attached to e-mail from a known source, even a coworker, if you were not expecting a specific attachment from that source.

• Be suspicious of e-mail messages containing links to unknown web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

• Don’t copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

• Avoid direct disk sharing with read/write access. Scan detachable devices (i.e.: flash drives) for viruses before using it.

• If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

• Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

**IT Department Responsibilities**

The following activities are the responsibility of the Limestone College IT department:

• The IT department is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted on the Limestone College. Check one of these locations regularly for updated information.

• The IT department will maintain the current version of the anti-virus program in terms of both virus definitions and software version.

• The IT department will install anti-virus software on all Limestone College owned desktop workstations, laptops, and appropriate servers.

• The IT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

• The IT department will perform regular anti-virus sweeps of all computer files.

• The IT department will attempt to notify Limestone College employees of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages to non-IT employees in order to keep network traffic to a minimum.

**Department and Individual Responsibilities**

The following activities are the responsibility of Limestone College departments and employees:

• All employees are responsible for taking reasonable measures to protect Limestone College from virus infections.

• Employees must not attempt to alter or disable anti-virus software installed on any computer attached to the Limestone College network.

**End of Policy**
Cellular Use Policy

Authorized Use Policy
Limestone College Cellular Telephone Service & Equipment

The Limestone College Computer Services Department issues cellular telephone equipment and services to Limestone employees based on the needs expressed by Limestone College Vice Presidents and Department Heads. All Limestone issued cellular telephone equipment (including chargers, cords, batteries, carrying cases and any other attending accoutrements) is the property of Limestone College and must be returned to the Computer Services Department in good working order upon request.

Employees who are issued a Limestone College owned cellular telephone are responsible to maintain the equipment in good working order and to observe all Limestone College policies regarding its service and use. Abuse or misuse of equipment or disregard of the Authorized Use Policy may result in suspension or revocation of cellular telephone privileges as well as disciplinary action.

- Daytime cell phone talk-time minutes are pooled. The school is allotted a set amount of minutes from which all school cell phones must draw. If the allotment is exceeded the school incurs additional charges. It is expected that employees will be conscientious in cell phone usage so that the pooled minutes are not exceeded. Daytime is 7:00 AM to 9:00 PM Monday – Friday.
- AT&T to AT&T cell phone calls are free of charge. These do not count against school minutes.
- Each cell phone has 5000 Night and Weekend minutes of talk time per month. Night is 9:00 PM to 7:00 AM Monday – Thursday. Weekend is 9:00 PM Friday – 7:00 AM Monday.
- Data Usage - Unlimited data is included with all smart phone plans.
- Text Messaging - Unlimited text messaging is included with all smart phone plans.
- Cellular phone use is for conducting school business only. Personal use is not authorized without express permission from the employee’s supervisor.
- Cellular phones are not to be used at any time while operating a motor vehicle.
- It is required that all school issued smart-phones and tablets be protected by enabling pass-code lock.
- Calls to third-party billing numbers such as 1-900 numbers are prohibited.
- Directory assistance calls to 411 are prohibited as these calls are charged to the school. If necessary, free directory assistance can be obtained at 800-FREE-411.
- Any form or harassment, threats, intimidation, pranks or disruption of business made with cellular telephones or service is expressly forbidden.
- Swapping phones between employees, altering equipment or services, tampering with, swapping, removing or altering SIM chips is expressly forbidden.
- Loss or damage of a phone or equipment must immediately be reported to the Computer Services Department.
- Phones must not be taken out of the continental United States without prior authorization from the Computer Services Department.
- Any disruption of service, malfunction or failure of cellular equipment or service should be immediately reported to the Computer Services Department.
- Upon leaving employment or transfer of position, all cellular equipment (phone, case, charger, etc.) must be turned in to the Computer Services Department. The pass-code and activation locks must be removed from equipment when turned in. Immediate supervisors or department heads will be responsible to ensure collection and return of equipment.

Any questions, concerns, issues, trouble or requests regarding cellular service or equipment should be directed to the Limestone College HELP DESK at ext. 4357 or to the Manager of Telecommunication at ext. 8353.
Copyright Policy

Introduction

Limestone College believes in respecting and protecting the rights of intellectual property owners. This is not only a question of ethics, but also of law. Advances in electronic communication and technology, such as the Internet, have had a dramatic impact on the way Limestone College conducts business, and have greatly facilitated our access to a wide range of information and media. As a result, the risk of copyright infringement, either intentional or accidental, is of increasing concern.

Copyrighted works include, but are not limited to: text (e.g. articles), images (e.g. photographs), graphics (e.g. logos), sound recordings (e.g. MP3s), video recordings (e.g. movies), or software programs. The following materials are not considered copyrighted materials: ideas, facts, processes, methods, systems, government works, and works in the public domain.

The goal of this policy is to inform employees at Limestone College on rules and procedures relating to copyright law compliance.

Referenced Copyright Laws

Copyright Act (Title 17 of the US Code) – Authorized in Article I of the US Constitution, which states that Congress is allowed to pass legislation “to promote the Progress of Science and useful Arts by security for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”

Digital Millennium Copyright Act of 1998 – This law provides recourse for owners of copyrighted materials who believe their rights have been infringed on the Internet.

Copyright law provides educators with a separate set of rights in addition to fair use to display (show) and perform (show or play) others’ works in the classroom. These rights are in Section 110(1) of the Copyright Act and apply to any work, regardless of the medium.

College Copyright Policy

• Limestone College reserves the right to monitor user systems and the content stored therein. Limestone College also reserves the right to remove, delete, modify, or otherwise disable access to any materials found to be infringing on copyright.

• Employees of Limestone College will indemnify and hold Limestone College harmless for any breach of this policy or copyright law.

• No employee of Limestone College may reproduce any copyrighted work in violation of the law.

• Copyrighted materials in the US are not required by law to be registered, unlike patents and trademarks, and may not be required to carry the copyright symbol (©). Therefore, a copyrighted work may not be immediately recognizable. Assume material is copyrighted until proven otherwise.

• If a work is copyrighted, you must seek out and receive express written permission of the copyright holder to reproduce the copyrighted work in order to avoid violation.
Compliance Procedure

If an employee needs help determining if a work is copyrighted or not, or has questions regarding any other copyright issue, he/she should contact the Information Technology Help Desk at extension 4357.

To obtain permission to reproduce a copyrighted work, contact the copyright holder.

Procedure for Copyright Infringement Claims

Employees at Limestone College are encouraged to report all instances of actual or suspected copyright infringement to Limestone College’s copyright agent named below.

In compliance with the Digital Millennium Copyright Act (DCMA), Limestone College will respond to all appropriate notices of copyright infringement. Limestone College may, under appropriate circumstances, remove and/or disable access to material claimed to be infringing upon the intellectual property rights of others.

Please use the following process to notify Limestone College of any copyright issues. Claims of copyright infringement must include all of the following in order to be effective:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
- Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single claim, a representative list of such works at that online site.
- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit Limestone College to locate the material.
- Information reasonably sufficient to permit Limestone College to contact you, such as an address, telephone number, and if available, an electronic mail address where you may be contacted.
- A statement that you have a good faith belief that the disputed use of the materials is not authorized by the copyright owner, its agent, or the law.
- A statement that the information in the notice is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

End of Policy
E-Mail Acceptable Use Policy

E-mail is a critical mechanism for business communications at Limestone College. However, use of Limestone College’s electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of Limestone College.

The objectives of this policy are to outline appropriate and inappropriate use of Limestone College’s e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope
This policy applies to all e-mail systems and services owned by Limestone College, all e-mail account users/holders at Limestone College (both temporary and permanent), and all institution e-mail records.

Account Activation/Termination
E-mail access at Limestone College is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account and password information.

E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Contractors
- Interns
- Longer term temporary employees (more than one week)

Applications for these temporary accounts must be submitted in writing to Dr. Scott Berry, Director of Server Services, X4525, sberry@limestone.edu. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement.

E-mail access will be terminated when the employee or third party terminates their association with Limestone College, unless other arrangements are made. Limestone College is under no obligation to store or forward the contents of an individual’s e-mail inbox/outbox after the term of their employment has ceased. It is the responsibility of the employee supervisor to determine what email stored contents of a departed employee are retained for business purposes; thereafter, to contact Server Services to make arrangements for transfer of the kept email.

General Expectations of Users
Important official communications are often delivered via e-mail. As a result, employees of Limestone College with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important college announcements and updates, as well as for fulfilling business- and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove him or herself from the list, and is responsible for doing so in the event that their current e-mail addresses changes.

E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.

Appropriate Use
Individuals at Limestone College are encouraged to use e-mail to further the goals and objectives of Limestone College. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of Limestone College, and clients within the context of an individual’s assigned responsibilities.
• Acquiring or sharing information necessary or related to the performance of an individual’s assigned responsibilities.
• Participating in educational or professional development activities.

Inappropriate Use

Limestone College’s e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others’ use and enjoyment of Limestone College’s e-mail system and services. E-mail use at Limestone College will comply with all applicable laws, all Limestone College policies, and all Limestone College contracts.

The following activities are deemed inappropriate uses of Limestone College systems and services and are prohibited:

• Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
• Use of e-mail in any way that violates Limestone College’s policies, rules, or administrative orders, including, but not limited to, the College Faculty and Staff Handbook.
• Viewing, copying, altering, or deletion of e-mail accounts or files belonging to Limestone College or another individual without authorized permission.
• Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 10 MB or less.
• Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
• Sharing e-mail account passwords with another person, or attempting to obtain another person’s e-mail account password. E-mail accounts are only to be used by the registered user.
• Excessive personal use of Limestone College e-mail resources. Limestone College allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Limestone College prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-Limestone College commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.
• Using the Limestone College email system to transmit social security numbers and credit card numbers.

Monitoring and Confidentiality

The e-mail systems and services used at Limestone College are owned by the college, and are therefore its property. This gives Limestone College the right to monitor any and all e-mail traffic passing through its e-mail system. While the College does not actively read end-user e-mail, e-mail messages may be inadvertently read by IT staff during the normal course of managing the e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with Limestone College’s records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If Limestone College discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.
Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of Limestone College become the property of the receiver. A good rule is to not communicate anything that you wouldn’t feel comfortable being made public. Demonstrate particular care when using the “Reply” command during e-mail correspondence.

**Reporting Misuse**

Any allegations of misuse should be promptly reported to Dr. Scott Berry, Director of Server Services, x4525, and sberry@limestone.edu. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

**Disclaimer**

Limestone College assumes no liability for direct and/or indirect damages arising from the user’s use of Limestone College’s e-mail system and services. Users are solely responsible for the content they disseminate. Limestone College is not responsible for any third-party claim, demand, or damage arising out of use the Limestone College’s e-mail systems or services.

**End of Policy**
Employee Departure Checkout Checklist

This checklist explains the employee departure checkout process. Follow these steps for any employee departure, whether voluntary or involuntary. This checklist assumes that appropriate written notification of pending departure has either been supplied by the employee in the event of resignation, or will be supplied to the employee in the event of termination.

- Notify the appropriate personnel in IT in advance that an employee will be departing so that they can take appropriate security measures. If the employee is being terminated, notify IT that all of the employee’s accounts (network, e-mail, voice, database) will need to be deactivated at a particular date and time. Ideally, deactivation should take place while the employee is being notified of his or her termination.

- Notify the employee in advance any equipment and files that should be in the employee’s possession and must be returned.

- Employee’s supervisors should conduct an exit interview. At this interview, the following must be addressed:
  - Review any confidentiality and non-disclosure requirements. Remind employee that all files and documents are property of Limestone College and cannot be destroyed, removed, modified, or copied without approval from the direct supervisor.
  - Ensure return of all College property to the employee’s supervisor, or make arrangements for its immediate return. Institution property includes all keys, access cards, identification cards, tools, books, reference materials, software, and equipment (such as laptop computers and mobile devices).
  - Gather and/or confirm the employee’s forwarding information, including home address and e-mail address (if appropriate).
  - Have the employee disclose all usernames and passwords to all accounts and/or applications to the employee’s supervisor for IT related records management and redistribution purposes.
  - Review the status of any and all projects or work in progress.

- Have the employee disclose the location of key work-related documents and records.

- Have all work-related computer files transferred for secure review by the departing employee’s successor or supervisor. These files will be deleted, stored, or forwarded to the appropriate staff member.

- Arrange for return of personal print and computer files to the employee.

- Arrange for the departing employee’s e-mail to be temporarily forwarded to the employee’s supervisor.

End of Policy
Internet Acceptable Use Policy

This document will be updated periodically. Please review the online Information Technology Policy Guidelines document occasionally in order to keep up to date on Limestone College’s Internet Acceptable Use Policy.

The goals of this policy are to outline appropriate and inappropriate use of Limestone College’s Internet resources, including the World Wide Web, electronic mail, the intranet, and FTP (file transfer protocol). Your account provides you with access to networks around the world through these services. Use of these services is subject to the following conditions.

Your Account
Internet access at Limestone College is controlled through individual accounts and passwords.

Appropriate Use
Individuals at Limestone College are encouraged to use the Internet to further the goals and objectives of Limestone College. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of Limestone College, and clients within the context of an individual’s assigned responsibilities;
- Acquiring or sharing information necessary or related to the performance of an individual’s assigned responsibilities;
- Participating in educational or professional development activities.

Inappropriate Use
Individual Internet use will not interfere with others’ use and enjoyment of the Internet. Users will not violate the network policies of any network accessed through their account. Internet use at Limestone College will comply with all Federal and State laws, all Limestone College policy, and all Limestone College contracts. This includes, but is not limited to, the following:

- The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- The Internet may not be used in any way that violates Limestone College’s policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of Limestone College, misrepresents Limestone College, or violates any Limestone College policy is prohibited.
- Individuals should limit their personal use of the Internet. Limestone College allows limited personal use for communication with family and friends, independent learning, and public service. Limestone College prohibits use for mass unsolicited mailings, access for non-employees to Limestone College resources or network facilities, and the dissemination of chain letters.
- Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Limestone College or another individual without authorized permission.
- In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments.
Security
For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user’s account password is strictly prohibited. Users are required to obtain a new password if they have reason to believe that anyone has learned their password. Users are required to take all necessary precautions to prevent unauthorized access to Internet services. If someone asks for your password, report this to the IT department.

Failure to Comply
Violations of this policy will be treated like other allegations of wrongdoing at Limestone College. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of the Internet may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
- Disciplinary action according to applicable Limestone College policies;
- Legal action according to applicable laws and contractual agreements;

Monitoring and Filtering
Limestone College may monitor any Internet activity occurring on Limestone College equipment or accounts. If Limestone College discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

Disclaimer
Limestone College assumes no liability for any direct or indirect damages arising from the user’s connection to the Internet. Limestone College is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

We encourage you to use your Internet access responsibly. Should you have any questions regarding this Internet Acceptable Use Policy, feel free to contact Dr. Scott Berry, Director of Server Services, ext. 4525.

End of Policy
Laptop Policy

A limited number of laptop computers are available for short-term checkout from the IT Department. These units are not intended to replace primary work site computers. They are available to employees that:

- Need to perform work off-site that they are unable to perform at their primary work site.
- Need to make presentations at meetings, conferences, or symposia requiring visual digital demonstrations.

Employees are allowed to have only one laptop checkout at a time.

Loan Procedure

Reservations for laptops must be placed in advance by contacting the IT Department’s Help Desk (x4375). This is necessary in order to adequately schedule the distribution of laptops and IT staff time. Information that you must offer in your Laptop Loan Agreement Form includes:

- Timetable for use
- Intended use
- Anticipated travel with unit

Loans are for a maximum of two weeks. The IT Department cannot guarantee that a laptop will be available. Laptops are provided on a first come, first served basis.

Employees are required to report any problems experienced with the laptop during their loan period. If a laptop is not returned by the predetermined deadline, the employee will be contacted and asked to return it. If the employee is not able to be contacted, the employee’s supervisor will be contacted and asked to return it.

Hours and Contact Information

All laptop loan arrangements must be made through the IT Department. The contact for this service is:

- Help Desk
- Extension HELP (4357)

Laptops are to be picked up and dropped off during regular business hours at the PC Technician Lab, located in Cooper East, room 205. If other arrangements need to be made for pickup and drop off, the IT Department must be given at least 48 hours notice.

The working condition of the laptop will be assessed upon its return. Please allow sufficient time for this assessment to take place.

Orientation

Orientation sessions are mandated for first time borrowers of laptop units. These 15-minute sessions include basic instruction in use of the laptop and terms and conditions for loan. Please allow adequate time prior to picking up the laptop unit to receive instruction. Longer orientation sessions are available upon request.
Laptop Computers Supported

To provide consistent service, adequate user support, and to ensure network compatibility, Limestone College offers and supports only computers purchased with College funds.

The College prohibits installing any personally additional software or hardware to the laptop units.

Unauthorized copying of software is illegal, as copyright laws protect software.

Maintenance

All laptops are covered under the laptop manufacturer’s limited warranty. Damage not covered by the manufacturers warranty or the IT Department includes:

- Accident.
- Unreasonable use, abuse, neglect, and alternations.
- Improper service, improper installation, and improper connections with peripherals.
- Other causes not arising out of defects in materials or workmanship.
- Any service or repair provided outside the scope of the limited warranty.
- Damage to or loss of any programs, data, or removable storage media, whether it occurs during warranty repair or other repair service.

Any attempts to dismantle or repair the laptop unit oneself will invalidate the manufacturer’s warranty and may result disciplinary action.

Employees using the laptop loan service may contact the Help Desk at extension HELP (4357) for standard system support or in order to notify the IT Department of any problems encountered during their loan period.
Security

Users are responsible for damage to and/or loss or theft of loaned laptop units. To avoid loss or theft, please follow these guidelines:

- **Airports:** Do not leave the laptop unattended. Do not check the laptop as baggage. Exercise diligence in watching the laptop as it is passed through any x-ray devices.
- **Cars:** Keep the car locked and the laptop out of view. Ensure that the laptop is securely stored so that it does not slide while driving. Avoid storage of the laptop in a car during very hot or very cold weather.

If the laptop is lost or stolen, a written claim must be filed within 24 hours to the IT Department and notice given to the appropriate police authorities. If a laptop is lost, damaged, or stolen, the employee responsible for that laptop must attend an investigative disciplinary hearing where the circumstances surrounding the loss, damage, or theft will be discussed in depth.

Users are responsible for performing their own data backups. The IT Department is not responsible for any files left on any laptop or for loss of, or damage to, a user’s files during the loan period. The IT Department is also not responsible for any computer viruses transferred to, or from, a user’s diskette while using the laptop.

Visiting Laptops

Employees may wish to use a privately owned laptop computer at Limestone College. Visiting laptops must not be plugged into any network port without permission and assistance from the IT Department, since it could be disruptive or destructive to the network. If an employee chooses to bring in a visiting laptop and connected to the College’s network, employees are may connect their device to the wireless network using their own network login credentials. Employees should not connect their personally owned devices to any data ports.

Short-term contract workers or consultants in the employment of Limestone College will be provided with a laptop for the duration of their stay, if required. If they wish to provide their own laptop, the same visiting laptop rules apply. In the event of laptop loan from the IT Department, the loan of a laptop must be sponsored by a current Limestone College employee overseeing the work of the contractor or consultant.

Visiting laptops are not supported by the IT Department.

End of Policy
Limited Personal Use of Network Resources

Policy

Internet access is provided to employees of Limestone College for the purpose of advancing the goals of the College, as well as for professional development and the education or training of employees. This must be the primary rationale for Internet use.

Authorized users of the institution Internet connectivity may also use the Internet for limited personal use. This is a privilege, not a right, and may be removed at any time by employee’s supervisor. Limestone College does not accept liability for any loss or damage suffered by an employee as a result of that employee using the College Internet connection for personal use.

Detailed Parameters

Primary Use: Your primary and overriding rationale for using your Internet connection should be the performance of your role in advancing the business of Limestone College. This may include, but is not limited to:

- Communication with, and providing service to, clients and customers.
- Conducting the business of your department or unit (such as using the tools available on the College intranet).
- Communicating with other employees for work-related purposes.
- Gathering information relevant to your duties or to expand your expertise.

Limited Personal Use: This is defined as any personally-initiated online activity (including e-mail and Web usage) that is conducted for purposes other than those listed above. It is limited by the following considerations:

- It shall not cause any additional expense to the institution or department.
- It shall be infrequent and brief.
- It shall not have a negative impact on overall employee productivity.
- It shall not interfere with the normal operation of your department or work unit.
- It will not compromise your department or the institution any way.
- It will be ethical and not contravene acceptable use policies of the institution.
• Personal Judgment: In limiting personal use, the Limestone College expects employees to exercise the same good judgment that they would use in all work situations.

Examples of Limited Personal Use: Personal use is, by definition, up to the individual. We offer these examples only to illustrate the kinds of situations where it is hoped employees would exercise their good judgment.

<table>
<thead>
<tr>
<th>Limited Personal Use</th>
<th>Access Abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice keeps in touch with a circle of friends from high school via e-mail. Occasionally she will take a few minutes to read and respond to an e-mail from one of those friends.</td>
<td>Rob is the convener of a local amateur sports association. He has given his work e-mail out as his main contact. During the sports season, he spends up to 90 minutes each morning responding to queries and complaints, and otherwise conducting league business.</td>
</tr>
<tr>
<td>Nauman is a big fan of international cricket. During the world championships he takes a few minutes every morning to check a Web site that carries the overnight scores from Asia.</td>
<td>Mike frequents Web sites that are clearly prohibited by the College’s acceptable use policy. Co-workers have been offended by some of the images clearly displayed on Mike’s computer.</td>
</tr>
<tr>
<td>Mary reads a review of a new novel by Stephen King. While at work the next day, she logs onto Amazon.com and purchases the book for delivery to her home address.</td>
<td>Todd needs a new fishing rod and spends over an hour browsing different models at a sporting goods Web site.</td>
</tr>
</tbody>
</table>

Acceptable Use: While some limited personal use is allowed, all prohibitions described within the Limestone College’s acceptable use and security policies remain fully in force. For example, limited personal use does not include (see other policies for a more extensive listing):

• Providing internal network access to any other users.
• Using institution resources for personal commercial gain.
• Propagating, transmitting, accessing, downloading, or otherwise communicating any content that is likely to be deemed racist, sexist, harassing, abusive, obscene, or likely to cause offence to a recipient.
• Misrepresenting the institution brand for your own gain.
• Using your account to gain unauthorized access to external networks and systems.

Sanctions for inappropriate use of the Internet may include, but are not limited to, one or more of the following:

• Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
• Disciplinary action according to applicable Limestone College policies;
• Legal action according to applicable laws and contractual agreements.

Network Monitoring: Limestone College employs monitoring software for the purpose of enforcing acceptable use policies. This includes blocking access to certain Web sites for which access is deemed to be a contravention of these policies.

End of Policy
Add/Move/Change Policy

Purpose

On occasion, it’s necessary for desktop computing equipment and user account information to be moved, added, or changed in some way. The goal of this policy is to outline guidelines for end-users to request a move, add, or change to their desktop computing environments. This procedure has been designed with the objective of minimizing disruptions to both the IT department and end-users.

Eligible Items

All move, add, or change requests must be requested by a designated supervisor by completing the employee form for add/moves/changes located at the Switchboard:

- Move a desktop system (e.g. PC, telephone) or peripheral (e.g. printer, scanner) to another location.
- Add/disable an employee account (network, e-mail, voicemail, database).
- Add/remove a service to/from an existing employee account.
- Add/remove a new employee desktop system.
- Add/remove software or hardware to/from an existing desktop system.
- Change an employee’s name or other personally identifiable information in the system.

Scheduling

All move, add, or change requests must be received a minimum of (2) business days in advance of the requested action date. However, to ensure that your preferred action date can be met, it is recommended that you submit your request as far in advance as possible. In order to minimize disruptions and maintain efficiency, all regular moves, adds, and/or changes will be scheduled to take place during normal working hours.

In the event of a pressing need, an alternative time may be scheduled. These will be handled on a case-by-case basis.

Most moves, adds, or changes involve system downtime for the user. Outage windows will be minimized whenever possible. If a window is to exceed 2 hours, affected users will be notified in advance.

While all approved moves, adds, and/or changes will be carried out in as timely a manner as possible, they may be delayed in the event of an IT-related problem or emergency. IT Department will notify the employee as soon as possible if there will be any delay.

End of Policy
Password Policy

Purpose

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees of Limestone College are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

Scope

This policy applies to all employees of Limestone College who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any Limestone College facility, has access to the Limestone College network, or stores any non-public Limestone College information.

Policy

General

• Passwords must be changed every 180 days.

• Old passwords should not be re-used for a period of 1 year.

• All passwords must conform to the guidelines outlined below.

Password Construction Guidelines

Passwords are used to access any number of institution systems, including the network, e-mail, the Web, voicemail, and database. Poor, weak passwords are easily compromised, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

• Passwords must contain at least (10) characters.
• Passwords must contain at least one alphabetic character
• Password must contain at least one upper case character
• Password must contain at least one lower case character
• Password must contain at least one number
• Password cannot contain user profile data
• Passwords must not be based on the College’s name or geographic location.

Password Protection Guidelines

• Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person, administrators, superiors, other co-workers, friends, and family members, under any circumstances.

• If someone demands your password, have them contact the IT Department.

• Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to institution resources via the institution’s Citrix solution or SSL-protected Web site.
• No employee is to keep an unsecured written record of his or her passwords, either on paper or in an unencrypted electronic file.

• Do not use the “Remember Password” feature of applications.

• Passwords used to gain access to institution systems should not be used as passwords to access non-Limestone accounts or information.

• If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately.

• The IT Department may attempt to crack or guess users’ passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

End of Policy
Printer Policy

Purpose

Printers represent one of the highest equipment expenditures at Limestone College. The goal of this policy is to facilitate the appropriate and responsible business use of Limestone College’s printer assets, as well as control Limestone College’s printer cost of ownership by preventing the waste of paper, toner, ink, and so on.

Scope

This Printer Policy applies to all employees of Limestone College, as well as any contract employees in the service of Limestone College who may be using Limestone College networks and equipment.

General Policy

- Printers are to be used for documents that are relevant to the day-to-day conduct of business at Limestone College. Limestone College printers should not be used to print personal documents.
- Installation of personal printers is not allowed at Limestone College.
- If you come across an unclaimed print job, please stack it neatly and place near the printer.
- Make efforts to limit paper usage by taking advantage of sending documents electronically or using duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
- Make efforts to limit toner use by selecting light toner and lower dpi default print settings.
- Avoid printing large files when possible, as this puts a drain on network resources and interferes with the ability of others to use the printer.
- When possible, omit printing of e-mail messages. This may be wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
- Avoiding printing a document just to see what it looks like; rather, try to use the print preview option available in most applications.
- Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.
- Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with IT to find out which machines can handle these specialty print jobs.
- Typically, color printing is not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.
- Printer paper is available at the Business office. Desktop and multifunctional printer toner cartridges may be requested by calling Sharp Business Solutions at the telephone number listed on the printer. IT will replace the toner cartridges for the large multifunctional printers located in the copier room of Curtis Hall.
- If you encounter a physical problem with the printer (paper jam, out of toner, etc.) please try to remove the jam. If you cannot remove the jam, please contact the IT Helpdesk.
- Report any malfunction of any printing device to IT as soon as possible.

End of Policy
Server Space Usage Policy

Limestone College has established a Server Space Usage Policy to preserve the finite amount of storage space available on network servers. This policy is designed to curtail the increasing use of College server space for unauthorized, non-business-related files.

Appropriate Files for Storage

Files that directly pertain to the business of Limestone College may be saved on a server. These include most business files created through the use of IT Department-approved and installed software.

Inappropriate files include non-business-related MP3s, games, executables, visual basic scripting files, and any other employee software not approved by the IT Department. Not only do such files consume valuable server space, but they can introduce damaging viruses into the network.

Attempts will be made to block the storage of all non-business-related files. If such files are detected on the server, you will be asked to remove them.

Personal pictures may be saved to the local hard drive. The My Documents folder is actually a server folders; therefore, you are not allowed to save personal pictures at this location.

Tips for Conserving Storage Space

It is the responsibility of every employee to ensure that they use their server storage space allocation wisely. Identify, remove and/or archive items that are:

- Outdated, such as preliminary draft versions of current documents;
- Out-of-use or orphaned files;
- Duplicated files; and
- Non-business related or non-critical files.

IT Department Contact

If you have any questions regarding this policy, need a larger server storage space allocation, or require support in managing your space allocation, please contact:

- Dr. Scott Berry
- Ext. 4525
- sberry@limestone.edu

End of Policy
Software Installation Policy

Introduction

The purpose of this Software Installation Policy is to address all relevant issues pertaining to appropriate software installation and deployment on Limestone College computing systems.

Supported Software

The IT Department supports College owned software that is installed by IT staff.

The following is a list of some of the fully supported, standard software installed on all college-owned personal computers:

- Microsoft Windows
- Microsoft Office
- Microsoft Internet Explorer
- Microsoft Windows Media Player
- MS Forefront
- Adobe Acrobat Reader

Other supported software titles, available upon request, include:

- Microsoft Project
- Microsoft Visio
- Mozilla Firefox
- Mozilla Thunderbird
- Chrome

Restricted software titles available to individuals with a demonstrable business need include:

- Adobe Creative Products
- Jenzabar
- PowerFaids
- Blackbaud Raiser’s Edge

The IT Department will not support any software not installed by IT staff.

Software Requests

Contact the IT Help Desk (x4357) or email (helpdesk@limestone.edu) to request the desired software be reviewed for installation.
This includes all software titles listed above, currently unlisted titles, and privately owned and licensed titles. The IT Department reserves the right to reject any software installation request for any reason.

**Software Installation**

Software titles are to be installed on college-owned equipment by IT staff member, or under IT staff member direct supervision.

All software installed on Limestone College systems (including all commercial and shareware products) must be used in compliance with all applicable licenses, notices, contracts, and agreements.

The IT Department reserves the right to uninstall any unapproved software from a college-owned machine.

**Periodic Audits**

The IT Department reserves the right to monitor software installation and usage on Limestone College’s computer systems. The IT Department will conduct periodic audits to ensure compliance with this Software Installation Policy. Unannounced, random spot audits may be conducted as well. During such audits, scanning and elimination of computer viruses may also be performed. Other unsanctioned software may also be uninstalled at this time.

**End of Policy**
Telephone and Voicemail Acceptable Use Policy

Purpose

Telephone communication is an essential part of the day-to-day operations of Limestone College. Telephone and voicemail services are provided to employees of Limestone College in order to facilitate performance of Limestone College work. The goal of this policy is to balance the business need for telephone and voicemail use by Limestone College with the costs involved.

Telephone and Voicemail Services

- PBX: Nortel Meridian Option 11
- Voicemail: Callpilot
- Cellular: AT&T
- Local and Long Distance Telecommunication: AT&T

Basic Policy

As with all Limestone College resources, the use of telephones and voicemail should be as cost effective as possible and in keeping with the best interests of Limestone College. All employees must operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Limestone College.
- The IT Department is responsible for installation and repair of all Limestone College telephone equipment and administration of telephone and voicemail accounts.
- Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring IT is notified of any adds, moves, or changes (2 days in advance) required to telephone or voicemail services.
- All voicemail boxes will be protected with a password. Passwords must be changed every year to aid in mailbox security.
- Voicemail boxes are to be checked and emptied as often as possible. Voicemail messages will be automatically deleted after 14 days.
- Voicemail is to be used as a backup in the event you are not available to answer a call, and should not be used to “screen” calls. Each user is expected to respond to voicemail messages in a timely manner.
- If you will be away from the office for more than one business day, you are expected to change your temporary voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.
- Use of directory assistance (i.e. 411) is prohibited since a fee is incurred with each use. If you are unsure of a number, please consult print or online telephone directories.

Unacceptable Use

Limestone College telephone and voicemail services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.
• Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.
• Using the telephone system or breaking into a voicemail box via unauthorized use of a password.
• Broadcasting unsolicited personal views on social, political, or other non-business related matters.
• Soliciting to buy or sell goods or services unrelated to Limestone College.
• Calling 1-900 phone numbers.
• Making personal long-distance phone calls without supervisor permission.

Misuse of telephone and voicemail services can result in disciplinary action.

Limited Personal Acceptable Use

In general, personal use of telephone and voicemail services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed under the following circumstances:

• An employee’s work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.
• Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).
• The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.
• The employee needs to make arrangements for emergency repairs to his or her residence or automobile.
• A call that reasonably could not be made at another time and is of moderate duration.

Any personal long-distance calls that must be made (excepting toll-free 1-800 calls) should be charged to the employee’s home telephone number, personal credit card, personal calling card, or be charged to the called party. If a personal long-distance call must be made that will be billed to Limestone College, the employee should receive permission from a supervisor to make the call first. Regardless, employees are expected to reimburse Limestone College for the cost of any long-distance calls within 10 days of receipt of the relevant bill.

Monitoring

Limestone College reserves the right to monitor telephone and voicemail use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

Service and Repair

The IT Department requires 2 days notice to set up a standard telephone service and voicemail box.

If there is a problem with an existing telephone or voicemail box, contact the IT Department immediately at Help Desk ext. 4357 or email (helpdesk@limestone.edu). Fixes are typically made within 1 day.

End of Policy
Third-Party Access Policy

Purpose

The Purpose of the Limestone College Third-Party Access Policy is to establish the rules for third-party access to Limestone College information systems and the computer room, third-party responsibilities, and protection of Limestone College information.

Scope

The Limestone College Third-Party Access Policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of the Limestone College personnel responsible for the contracting and/or supervising of the third party. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

Policy

Computer Room Third Party Policy Guidelines

- All third-party access to the Information Technology Data Center (ITDC) should be scheduled to occur during regular business hours. If this is not possible, a point person from the IT department will be scheduled after hours to accompany the third party.
- When third parties are scheduled to have access to the computer room, the Information Technology Services staff must be notified in advance of the date, time, and type of work to be performed.
- When the third party arrives, he/she will report to the staff contact that scheduled the visit. The staff contact will escort the third party to the Information Technology Services area. At this point, the third party is to be informed that he/she will take further direction from the IT staff point person in relation to their activity in the computer room.
- Prior to the onset of any work, the third party will describe the activities that are planned.
- The IT staff point person is responsible for explaining what measures need to be taken to protect the computer hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the IT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the IT staff to do what needs to be done to protect the computer systems before starting their work.
- The third party will report to and receive instructions from the IT staff point person regarding their work in the computer room. The IT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed before leaving the area.

Information Systems Third-Party Policy Guidelines

Any third-party agreements and contracts must specify:

- The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.
- The Limestone College information that the third party should have access to.
- The minimum-security requirements that the third party must meet (i.e., method for remote access).
- How Limestone College information is to be guarded by the third party. Signing of a non-disclosure agreement is typically required.
• Strict use of Limestone College information and information resources for the purpose of the business agreement by the third party. Any other Limestone College information acquired by the third party in the course of the contract cannot be used for the third-party’s own purposes or divulged to others.

• Feasible methods for the destruction, disposal, or return of Limestone College information at the end of the contract.

• The return of College property such as a laptop or cellular phone after the completion or termination of the agreement.
  • The third party must comply with all applicable Limestone College standards, agreements, practices and policies, including, but not limited to:
    • Acceptable use policies.
    • Software licensing policies.
    • Safety policies.
    • Auditing policies.
    • Security policies.
    • Non-disclosure policies.
    • Privacy policies.
  • Limestone College will provide an IT point of contact for the third party, whether it is one person from the IT department or an interdepartmental team. This point of contact will liaise with the third party to ensure they are in compliance with these policies.
  • The third party will provide Limestone College with a list of all additional third parties working on the contract. The list must be updated and provided to Limestone College within 4 hours of any staff changes.
  • Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with the Limestone College Password Policy. Managing connectivity with partner networks can be handled different ways depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).
  • Any third party computer/laptop/tablet that is connected to the Limestone College systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage occurred to Limestone College in the event that an incident occurs.
  • Each third-party employee that has access to Limestone College sensitive information should be cleared to handle that information.
  • If applicable, an explanation of how Limestone College information will be handled and protected at the third party’s facility/site must be addressed.
  • Third-party employees must report all security incidents to the appropriate Limestone College personnel.
  • If third-party management is involved in Limestone College security incident management, the responsibilities and details must be specified in the contract.
  • The third party must follow all applicable change control procedures and processes.
  • All software used by the third party in providing service to Limestone College must be properly inventoried and licensed.
  • All third-party employees are required to comply with all applicable auditing regulations and Limestone College auditing requirements, including the auditing of the third-party’s work.
  • Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the appropriate Limestone College management.
• All third-party maintenance equipment on the Limestone College network that connects to the outside world via telephone lines, leased line, or the network will remain disabled except when in use for authorized maintenance.

• The third party’s major accomplishments must be documented and available to Limestone College management upon request. Documentation should include, but is not limited to events such as:
  • Personnel changes.
  • Password changes.
  • Project milestones.
  • Deliverables.
  • Arrival and departure times.

• Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to the Limestone College or destroyed within 24 hours. The third party will also provide written certification of that destruction within 24 hours. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by authorized Limestone College management.

• Limestone College will perform an impact analysis of other business-critical functions, once work has begun by the third party.

• Limestone College will eliminate third-party physical access to facilities after the contract has been completed or terminated. The following steps must be performed:
  • Remove third party authentication and all means of access to systems.
  • If needed, make sure that incoming e-mail is re-routed to an appropriate person.
  • Archive any third-party software configuration, and transfer ownership to designated internal staff.

End of Policy
Server Backup Policy

Introduction

Data is one of Limestone College’s most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on institution servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

What Is Backed Up

This policy refers to the backing up of data that resides on Limestone’s servers. Servers and the files on these servers that are covered by this policy include all servers that maintain critical network or college business data. The specific servers, data to be preserved, and backup procedures are maintained in a separate document, which is reviewed at least semiannually.

End-user files that are stored in their respective My Documents folder are maintained by a file server. When files are saved in the My Documents folder, they are backed up frequently. If a file restore is required, contact the Help Desk at extension 4357 (HELP). In the unlikely event that a computer crashes, the end-user files are easily accessible from other computers.

Backup Schedule

Backups are conducted manually and automatically.

The backup schedule for each server is to be designed to meet the following objectives:

- Backups are performed at scheduled times.
- A portion of the data is to reside offsite for disaster recovery (enough to perform an emergency restore).
- Backups may be accomplished via direct disk-to-disk copies and off-building/site network backups.

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it’s essential to regularly test one’s ability to restore data from its storage media.

- All tapes must be tested at least once every 3 months to ensure that the data they contain can be completely restored.

Data will be restored from a backup if:

- There is an intrusion or attack and significant amount of data is damaged.
- Files have been corrupted, deleted, or modified.
- Information must be accessed that is located on an archived backup.

In the event a data restore is desired or required, the following policy will be adhered to:

- In the event of data loss stored on a network server due to human error, the end user affected must contact the IT Department and request a data restore. The end user must provide the following information:
  - Name.
  - Contact information.
  - Name of file(s) and/or folder(s) affected.
- Last known location of files(s) and/or folder(s) affected.
- Extent and nature of data loss.
- Events leading to data loss, including last modified date and time (if known).
- Urgency of restore.

- Depending on the extent of data loss, the timing in the cycle will dictate whether the data backup is stored onsite or offsite. Data backup must be retrieved by the server administrator or pre-determined replacement. If the data backup is offsite and the restore is not urgent, then the end user affected may be required to wait up to 2 business days for a time- and cost-effective opportunity for the tape(s) to be retrieved.

- If the data loss was due to user error or a lack of adherence to procedure, then the end user responsible may be required to participate in a tutorial on effective data backup practices.

End of Policy
Devices on the Network

- **Non-Limestone IT network devices:**
  It is against Limestone IT policy for a user or an unauthorized IT support person to connect a network connectivity device (hub, switch, router or wireless access point) to "share" a single jack among multiple computers*.

  *Note that our IP phones have a port that supports the connection of the phone and a computer which is an acceptable and intended sharing of ports.

- **No DHCP servers:**
  To ensure network stability and security, it is prohibited for any user or unauthorized IT support person to run a local DHCP server (on a computer, printer, etc.) Devices that are (mis)configured to distribute IP address will be blocked from the network.

- **Disconnection of devices:**
  If a computer, printer or other network attached device is shown to be causing issues on the network due to misconfiguration or broken hardware or otherwise presents a security issue, if Limestone IT support cannot contact the responsible party the device in question will be disconnected from the network.

- **Rogue Wireless (Wi-Fi)**
  Only Limestone Network Services are authorized to deploy wireless access points. Please do not purchase your own. If Wi-Fi is a need or you are having access problems, please contact the Limestone help desk so that we may assist.

- **Wireless Printers:**
  Printers should be connected to a wired network port with a reserved DHCP address assigned. Wi-Fi enabled printers pose a risk to the existing Wi-Fi infrastructure by introducing interference and should have that feature disabled if present.