Atria Institute of Technology
IT Security and Policies

Table of Contents

Data Security Policy

Purpose

This policy defines the guidelines for the security and confidentiality of data maintained by Atria Institute of Technology, both in paper and electronic form. This policy also informs each person who is entrusted to access student, employee and/or institutional data of their responsibilities with regards to confidentiality and safeguarding Atria Institute of Technology data.

Statement of Policy

All custodians and guardians of administrative data are expected to manage, access, and utilize the data in a manner that maintains and protects the security and confidentiality of that information. All notice to state & local regulations must be considered and adhered to when using or sharing personal or confidential information. Any notice of a breach of confidential information whether in paper or electronic form MUST be reported to the appropriate Head for the area involved immediately. Under no circumstances shall credit card numbers be stored or sent from college servers or desktops.

Definitions

There are two primary categories of data-handling and access defined in this policy - Data Custodians and Data Guardians.

Data Custodians

Data custodians function as gatekeepers for the data that is collected and maintained by individuals in their departments. Custodians are responsible for establishing access procedures for the administrative data available in their area and for approving access requests for that data. The table below indicates the administrative areas that maintain the college's primary data stores and the respective data custodians.

Administrative Areas	Data Custodian
Alumni and Development Data	
Financial Data	Senior Accounts Manager

Financial Aid Data	
Human Resources Data	
Information Technology Data	IT HEAD
Student Services Data	

Data Guardian
A data guardian is defined as anyone who, as a function of their position at Atria Institute of Technology, possesses or has access to Atria Institute of Technology's administrative data, either electronic or otherwise. Guardianship and its associated responsibilities apply to individuals who dispense or receive data.
Department heads are responsible for signing off on data access requests for employees under their supervision.

Scope
College employees, or others who are associated with the college, who request, use, possess, or have access to college's administrative data must agree to adhere to the protocols outlined in this policy. In addition, guardians, custodians and data users are prohibited from:

- Changing data about themselves or others except as required to fulfill one's assigned college duties or as authorized by a supervisor. (This does not apply to self-service applications that are designed to permit you to change one's own data).
- Using information to enable actions by which other individuals might obtain profit on personal grounds.
- Disclosing information about individuals without prior authorization by a supervisor.
- Engaging in what might be termed "administrative voyeurism" (reviewing information not required by job duties) unless authorized to conduct such analyses.
- Examples include tracking the pattern of salary raises, viewing a colleague's personal information, looking up for someone else's grades or viewing another colleague's work product when not authorized to do so.
- Circumventing the level of data access given to others by providing access that is broader than that available to them, unless authorized. For example, providing an extract file of employee salaries to someone who does not have security access to salary data is prohibited by this policy.
- Allowing unauthorized access to Atria Institute of Technology's administrative systems or data by sharing an individual's username and password.
- Engaging in any other action that violates the letter and spirit of this policy, either purposefully or accidentally.

Improper Guardianship

In assuming responsibility for the interpretation and use of college administrative data, guardians are expected to recognize the potential serious consequences of their improper guardianship. Improper maintenance, disposal, or release of college administrative data exposes the College to significant risk, including lawsuits, loss of employee and student trust, and loss of funding.
Guardians who are found in violation of this policy will be subject to institute's disciplinary processes and procedures including, but not limited to, those outlined in the AIT Student Handbook, and any applicable bargaining unit contracts. Illegal acts may also subject users to prosecution by local, and/or state authorities.

Policy Applies to College employees, or others who are associated with the College, who request, use, possess, or have access to college administrative data.

Exceptions This policy does not prevent the release of institutional data to external organizations or governmental agencies as required by legislation, Regulation, or other legal requirements.

Individuals Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology and General Counsel.

Electronic Communication (Email) Policy

Purpose
Atria Institute of Technology has invested in its technology infrastructure to enhance its teaching and learning and to enable efficient business practices. All Atria Institute of Technology students, faculty, and staff have access to email as a communication tool and the academia portal for current news, events, personalized messages and teaching and learning activities. Atria Institute of Technology is committed to the optimum use of College wide electronic mail to enhance interpersonal communications, improve information exchange, and to reduce the use of paper and printed materials.
The purpose of this policy is to identify electronic mail as an official means of communication within Atria Institute of Technology and to define the responsibilities of Atria Institute of Technology students, faculty and staff related to electronic mail.

Statement of Policy
Atria Institute of Technology provides access to email and the academia portal for all students, faculty and staff. Email is an official method of communication at Atria Institute of Technology. Students, faculty and staff are held strictly responsible for the consequences of not reading College related communications sent to their official Atria Institute of Technology email address. Atria Institute of Technology students will also utilize the academia portal to post role specific messages and College related announcements.

Scope

Assignment of email addresses

Students and faculty are assigned a google username and password upon acceptance to a program or upon hire. Core faculty, Coordinators and staff are assigned a google username and password upon hire by Atria Institute of Technology, after being added to the Human Resource System. The official Atria Institute of Technology email address is:
Core Faculty/Staff - username@atria.eduStudent - username@visioneer.atria.edu

Educational Uses of Electronic communications
Faculty members may require the use of email, academia course tools, or other forms of electronic communication for course content delivery, class discussion, or synchronous chat. It is recommended that faculty specify these requirements in their course syllabus. Faculty may expect or require that students access academia and read notices sent to their official Atria Institute of Technology's provided email address.

Email forwarding
Students who forward their official Atria Institute of Technology emails to another email address (e.g., username@gmail.com) do so at their own risk. Atria Institute of Technology College cannot be held accountable or ensure the delivery of its official communications by external service providers. Forwarding email does not relieve the receiver from the responsibilities associated with electronic communications sent to their official Atria Institute of Technology email address. It cannot be stressed more strongly that students and faculty MUST use the email address provided by the college while they are associated with the College.

Responsible use of email

All use of email will be consistent with other Atria Institute of Technology policies and local and state law, including the Atria Institute of Technology's Policy on the Responsible Use of Information Technology.

Email is a tool provided by the College to complement traditional methods of communications and to improve education and administrative efficiency. All email users have a responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the college's e-mail system is confirmation that the user agrees to be bound by this policy. Violations of the policy may result in restriction of access to the College's email system and/or other appropriate disciplinary action.

The following should be observed when using any College email system:

> Conducting business for profit using College email and or other resources is prohibited. Incidental non-business personal use of e-mail is acceptable, but an expectation of privacy cannot be guaranteed due to the official nature of the email system; Using any email to send information that is classified as private or can be shown to contain personally identifiable information is prohibited. While the College will make every attempt to keep email messages secure, privacy is not guaranteed, and

users should have no general expectation of privacy in email messages sent through a College email system.

Under certain circumstances, it may be necessary for the Atria Institute of Technology IT staff or other appropriate College officials to access email files to investigate security or abuse incidents or violations of this or other college policies. Such access must be approved by CEO, Principal or General Counsel and will be on an as needed basis and any e-mail accessed will only be disclosed to those individuals with a need to know basis or as required by law.

Individuals are responsible for saving email messages as they deem appropriate. Due to limited resources the IT department has the right to restrict the amount of user storage on the College email system. Google email storage quotas are likewise controlled by Google. Users are asked to manage the volume of email in their account and are required, from time-to-time, to purge deleted or trashed emails. The College reserves the right to purge deleted emails in a users' account if space needs become critical.

When using email as an official means of communication, students, faculty, and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, students, faculty, and staff should not communicate anything via email that they would not be prepared to say publicly. Email may be accessed by the College for official purposes including but not limited to administrative need for official information, production in legal proceedings, information related to student records, information related to personnel records, etc.; however, such access must be approved by the account holder, CEO, Principal or General Counsel.

Approval and transmission of email containing essential college announcements to students, faculty, and/or staff must be obtained from the appropriate authority. Only the Office of Principal can authorize the sending of broadcast messages to a wide audience of students, faculty, and staff within the scope of their authority. IT will only send broadcast messages as they relate to maintenance issues or security concerns.

The following types of emails are explicitly prohibited:

- Emails that exchange proprietary information or other highly privileged, confidential or sensitive information.
- Emails that are considered advertisements, solicitations, chain letters, political communications and other unofficial, unsolicited email.

- Emails including sexual content, pornography, lewd or other highly inappropriate behavior when considering the official nature and purpose of the College email system.
- Emails that are in violation of any laws, including copyright laws, or institutional policies.
- Emails that knowingly transmit a message containing a computer virus.
- Emails that intentionally misrepresent the identity of the sender of an e-mail. Emails that use or attempt to use the accounts of others without their permission.

Policy Applies To

This policy applies to all students, faculty, and staff of the College and to all other users of information technology resources at Atria Institute of Technology. These users are responsible for reading, understanding, and complying with this policy.

Individuals Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology.

Personal Digital Assistant Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the use and support of Personal Digital Assistant devices (PDAs) that are common in the workplace and may be used by employees of Atria Institute of Technology College. This policy applies to, but is not limited to, all devices that fit the following device classifications:

Handhelds running the Apple OS, Android OS, Blackberry OS, Palm OS, Microsoft Windows CE, Pocket PC, Windows Mobile, Symbian, or Mobile Linux operating systems and others.
Mobile devices that are wireless or wired (i.e., connectible using the College wired or wireless network or by a wireless provider network such as Airtel, Reliance, or BSNL.
Smartphones that include PDA functionality.
Any third-party hardware, software, processes, or services used to provide connectivity to the above.

The policy applies to any PDA hardware and related software that could be used to access college resources, even if the equipment is not college sanctioned, owned, or supplied. The overriding goal of this policy is two-fold. The first goal is to protect Atria Institute of

Technology 's technology-based resources (such as College data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attacks that could result in loss of information, damage to critical applications, loss of revenue or damage to our public image. Therefore, all users employing PDA-based technology to access College technology resources should adhere to college-defined processes for doing so. See the Electronic Communication Policy and the Responsible Use Policy, (for examples). The second goal of this policy is to make clear the limits that the College places on user support for PDA devices.

Scope

This policy applies to all Atria Institute of Technology employees, including full-time and part-time staff, full and part time faculty, contractors, and other agents who utilize College-owned, personally owned, or publicly accessible PDA-based technology to access the College's data and networks via wired or wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at Atria Institute of Technology does not automatically guarantee the granting of these privileges.

Addition of new hardware, software, and/or related components to provide additional PDA-related connectivity within college facilities will be managed at the sole discretion of the Information Technology Department and the College.

Supported Technology

Currently Atria Institute of Technology does not provide support for employee-owned Cell Phones or PDAs. The Atria Institute of Technology's IT Department does not provide personal consulting to individual employees, it only restricts to assist an employee in their own attempt to connect a PDA device to a College IT resource. Such support is limited to availability of time and will often require the employee to perform upgrades, patches and revisions on their own.

Policy and Appropriate Use

It is the responsibility of any employee of Atria Institute of Technology who is connecting to the College's network via a PDA to ensure that all components of his/her connection remain as secure as his/her network access within the office. It is imperative that any wired (via sync cord, for example) or wireless connection, including, but not limited to PDA devices and service, used to conduct Atria Institute of Technology's business be utilized appropriately, responsibly, and ethically. Failure to act accordingly may result in immediate suspension of that user's account at the sole discretion of the IT Department. Based on this, the following rules should be observed:

1. Employees using PDAs and related software to connect to Atria Institute of Technology's technology infrastructure will, without exception, use secure remote access procedures. This will be enforced through public/private key passwords in accordance with Atria Institute of Technology's Responsible Use policy. Employees agree to never disclose their passwords to anyone, including family members if college work is conducted from home.

2. All PDAs that are used for college interests must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether they are in use and/or being carried. This includes, but is not limited to, power-on passwords. Any non-college owned computers used to synchronize with PDAs will have current antivirus software loaded. Antivirus signature files must be updated on a regular basis.

3. Passwords and other confidential data as defined by Atria Institute of Technology College are not to be stored on PDAs or their associated storage devices (such as SD and CF cards).

4. The Atria Institute of Technology College IT Department reserves the right to require students and employees to shut down any form of personally owned technology that has been determined to cause interference with the proper functioning of the College wireless technology.

5. Any PDA that is configured to access Atria Institute of Technology College resources via wireless or wired connectivity must adhere to the authentication requirements of the College, as found in the Data Security policy and the Responsible Use policy.

6. Employees, contractors, and temporary staff will make no modifications of any kind to college-owned and installed hardware or software without the express approval of the IT Department. This includes, but is not limited to, installation of PDA software on college-owned desktop or laptop computers, connection of sync cables and cradles to college-owned equipment and use of the College's wireless network bandwidth via these devices.

7. Employees, contractors, and temporary staff with Atria Institute of Technology College-sanctioned wireless-enabled PDAs must ensure that their computers and handheld devices are not connected to any other network while connected to Atria Institute of Technology College's network via remote access.

8. The PDA-based user agrees to immediately report to his/her manager and the IT Department any incident or suspected incidents of unauthorized access and/or disclosure of college resources, databases, networks, etc.

9. The PDA-based wireless access user also agrees to and accepts that his or her access and/or connection to Atria Institute of Technology College's networks may be monitored to

record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

10. The IT Department reserves the right to suspend without notice any access port to the network that puts the College's systems, data, users, and clients at risk.

Security

1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile device users must ensure all College data stored on the device is encrypted using strong encryption. See the Atria Institute of Technology College's Electronic Communication Policy for additional background. Please remember that email communications sent to and from PDAs and similar devices are insecure. Atria Institute of Technology College policies prohibit the sending and receiving of personally identifiable information by email. This includes employee data as well as student data. Employees must agree to never disclose their passwords to anyone, including family members if college work is conducted from home.

2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain college data. Any non-college computer used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by the IT Department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

3. Passwords and other confidential data as defined by the IT Department are not to be stored unencrypted on mobile devices.

4. Any mobile device that is being used to store Atria Institute of Technology College data must adhere to the authentication requirements of the College. In addition, all hardware security configurations (personal or College-owned) must be pre-approved by the IT Department before any enterprise data-carrying device can be connected to it.

5. The IT Department will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to disable or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Atria Institute of Technology College's Responsible Use policy.

6. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase College-specific data from such devices once their use is no longer required.

Help & Support

1. Atria Institute of Technology 's IT department will support its sanctioned hardware and software but is not responsible or accountable for conflicts or problems with personally owned PDA devices or other hardware and software.

2. The IT Department reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the College network.

3. The IT Department will make every attempt to assist users who wish to configure their PDA devices to provide access to the College's communications platform in a secure manner.

4. The IT Department will provide support (limited) to the College email communications application only. This includes email, calendar, and contacts.

5. The College cannot be held responsible for damage or loss of information on a personal PDA device when, at the request of the owner, it is being supported by a representative of the IT Department.

POLICY APPLIES TO

This policy applies to all students, faculty, and staff of the College and to all other users of information technology resources at Atria Institute of Technology. These users are responsible for reading, understanding, and complying with this policy.

Individual Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology

Remote Access Policy

Background for this Policy

Access to key information systems and services resident on the Atria Institute of Technology College network from the public Internet is a requirement for a significant portion of the Atria Institute of Technology College community. In the past, the College relied on a Virtual Private Network (VPN) to connect remote users directly to the College network. With

overhead and support for this type of technology solution running in the multiple thousands per year the College has sought out alternative solutions for this basic service.

While the College has not set a date to discontinue the VPN service it has established a service using LogMeIn's remote access "cloud based" solution to provide employees a way to access their secure desktops to perform most basic desktop functions.

Purpose

The intent of this policy is to identify remote access methods and procedures that will insure a high level of security for Atria Institute of Technology's IT physical assets and data. These include network infrastructure, College servers, College workstations, Financial data, HR data, student information, other forms of personal information and other information necessary to support the academic mission and business functions of the College. The policy will define standard approved remote access methods for connecting to Atria Institute of Technology network resources by any/all authorized users. It will establish guidelines for managing and protecting information resources and services on the College LAN and enable the use of hardware, software and procedures for implementing the policy.

The policy's guiding philosophy is to keep Atria Institute of Technology's information within the institute's internal network. As such, this policy is designed to enable users' full remote access to authorized resources that are necessary to perform their jobs while minimizing the exposure of College IT resources to external threats. For example, copying or moving files that contain protected Atria Institute of Technology College information from a system on the College Local Area Network (LAN) to a remote workstation is prohibited. All policy decisions not explicitly outlined in the policy will be based on this philosophy.

This policy does not identify approved users or their authorization. It only identifies the method of access and authentication and defines the process for requesting access. Access privileges are granted by the Data Custodians, Principal Administrator, or Managers of a Business unit or application owners responsible for the information being accessed.

Scope

In order to provide a faster lighter weight method to gaining secure access to the College's business systems and services the IT department supports LogMeIn. LogMeIn is an authenticated "Cloud" based remote access service. The service is maintained and administered by the IT department and is available in two versions. One version provides full access to a user's desktop and allows the user the same control over services that they would have while seated at their work desk. There is no cost to the College for this version and therefore we will encourage users who need to use a remote access solution to adopt this version. The second version is similar to the free version with the additional capability

of transferring files bi-directionally between the remote computer and the user's work desktop. This expanded version is only available on an as needed basis. Both versions require supervisor approval.

POLICY APPLIES TO:

This policy applies to all faculty, and staff of Atria Institute of Technology who require remote access to the College network while away from their office. These users are responsible for reading, understanding, and complying with this policy.

Individuals Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology.

Information Technology Responsible Use Policy

Purpose

Atria Institute of Technology is an educational institution which encourages continuous learning, experimentation, and the development of the adult learner. The College is committed to respecting individual privacy and freedom while expecting everyone to act in a responsible, legal, ethical and efficient manner when using the College's information technology systems and resources. These systems are designed to encourage high-quality educational, professional career development and self-discovery activities.

The purpose of this policy is to define responsible and ethical behavior that guides faculty, student, and staff use of information technology resources at Atria Institute of Technology.

Statement of Policy

Atria Institute of Technology provides access to information technology resources for faculty, staff, students, and certain other users to support the College's mission and to conduct the business of the College. Every authorized user of information technology resource at Atria Institute of Technology is responsible for utilizing these resources in an efficient, ethical, and legal manner and in ways consistent with overall College policy.

Definitions:

Information technology includes but is not limited to desktop computers, workstations, network servers, mainframes computers, software, digital information and voice, video and data networks, including official College web pages on its portal, public website and social networking sites.

Scope

The following principles serve to guide the responsible use of information technology for all Atria Institute of Technology College users.

Respect the rights of others by complying with all College policies regarding sexual, racial and other forms of harassment, and by preserving the privacy of other individuals. For example, it is prohibited to send harassing messages via email or social networking or transmit or reveal personal or private information about individuals. Use computing facilities, accounts and data only when you have appropriate authorization and use them for approved purposes. For example, you should not use Atria Institute of Technology's information Technology resources to run a business or to access another individual's computer account.

Respect all pertinent licenses, contractual agreements, and copyrights. Use only legal versions of copyrighted software in compliance with vendor license requirements. For example, you should not post another individual's copyrighted material on your web page or install software with a single user license on multiple computers.

Preserve the integrity of computing systems, electronic data, and communications networks. For example, you should not modify settings on a desktop computer to make it unusable to others or excessively utilize networked resources, like music videos, that may overload Atria Institute of Technology College's network bandwidth.

Respect and adhere to all applicable local and state laws. For example, it is prohibited to use Atria Institute of Technology 's information technology resources to attack computers on another network by launching viruses, worms, or other forms of attack.

Privacy

While the College values and respects the privacy of its staff, faculty, students, and other users, the intrinsic nature of electronic records places limits on the extent to which the College can guarantee a user's privacy. Despite security protocols, communications over the Internet—and across the College's local campus network—can be vulnerable to interception and alteration. Consequently, the College cannot assure that absolute privacy can be maintained for data that resides on the College network or on storage media.

Out of respect for personal privacy, the College does not routinely examine the contents of data or files in user accounts. However, on occasion, circumstances may require an examination of a user's files to maintain system security, to administer or maintain system integrity, to access necessary College information or in response to legal mandates. In such cases, authorized personnel may examine a user's data without notice. Authorized personnel

are those specifically entrusted and approved by the College (needs CEO or Principal level or General Counsel approval) to conduct such examinations.

Some data are subject to strict access restrictions, such as library patron records and data protected by the Family Educational Rights and Privacy Act (FERPA). The library, and other departments that administer confidential data may enforce more stringent access policies.

Personal Use

Personal use is defined as the non-academic, non-administrative use of Atria Institute of Technology's IT systems. Such use is solely discretionary; it neither serves an essential employment function nor is it related to academic discourse. Data that result from personal use are "personal data."

Personal use of Atria Institute of Technology's IT resources is secondary to performing essential College functions using such resources. If personal use of College IT resources interferes with or causes disruptions to the essential functions of the College performed by IT, then authorized personnel may curtail such use.

Passwords and User IDs

System accounts, passwords, and user IDs play an important role in protecting the files and privacy of all users. Because users are responsible for all uses made of their accounts, users must take exceptional care to prevent unauthorized use of their accounts. This includes changing passwords regularly and disabling "automatic" log-ins.

In most cases, it is inappropriate—and perhaps dangerous—to allow another person to use another user's network credentials or email account. In some cases, a user's data is vulnerable to alteration or deletion. In others, the validity of a user's credentials could be compromised. Alternatively, if criminal activity can be traced to a user's account, the person to whom the account is assigned may be held accountable. The College, therefore, reserves the right to restrict or prohibit password sharing.

In addition, the College reserves the right to implement and enforce password maintenance procedures, including detecting and disabling "weak" passwords and implementing password "aging" mechanisms. Weak passwords are those that may be easily "cracked," guessed, or discovered, such as a user's birth date or name. Password aging refers to a process that requires users to change passwords at predetermined intervals.

Data Storage and Back-ups

The College maintains a centralized repository of data stored in user accounts on the College network. This includes all the data that a user creates and saves on the College's network storage devices. It also includes saved email messages, attachments, files, and folders.

The College reserves the right to restrict the amount of network storage available for users. This includes the prerogative to impose quotas on the number and/or size of stored files. The Director of IT, after conferring with the College Leadership, can regulate the availability of central network storage to which each user is entitled.

Data files are routinely backed up on a daily, weekly, monthly, and/or yearly basis. These back-ups facilitate the restoration of college data that have been lost, altered, or damaged. The College will not routinely retrieve backed-up personal data. Users, therefore, are encouraged to maintain independent back-ups of their important personal data, including email messages. Atria Institute of Technology College disclaims any responsibility for maintaining or providing access to backups of a user's personal data.

For data backed up by the IT department, retrieval or restoration is at the discretion of the Director and/or the College Leadership.

Security

The College implements appropriate "industry-standard" practices concerning the security of the College's IT resources. These methods are designed to protect against unauthorized access, intrusion, or damage to the availability, access, or integrity of the College's IT systems. However, due primarily to the nature of security threats and the remote possibility of a breach of security, the College warrants neither a user's privacy nor the integrity of data stored on the College network.

Copyright, Trademark, and Domain Names

Users must comply with all copyright, trademark, and other intellectual property laws. In general, permission is necessary for a user to reproduce materials, such as video, music, images, or text. To "reproduce" in this context includes downloading and saving a digital copy to a hard drive, floppy, or other storage media. Photocopying copyrighted materials without authorization is also prohibited. Certain exceptions apply, such as "Fair Use."

In addition, users must generally obtain permission from the copyright owner to prepare derivative works, including modifying existing works. Copyright law also prohibits the distribution, display, or performance of works created by another without a proper release.

The College possesses trademark rights in certain symbols and phrases such as images of the College logo and the words "Atria Institute of Technology College." Unauthorized use of these trademarks is not permitted.

Additionally, the College owns certain Internet domain names. These include atria.edu, acme.atria.edu and other such domain names. Registration of domain names incorporating or referencing College trademarks is prohibited without the approval of the College Leadership.

Compliance and Enforcement

All users of the College's IT resources must abide by these policies. Users not wishing to agree to and comply with this policy will be denied use of or access to Atria Institute of Technology's IT resources.

College community users who intentionally violate these policies are subject to disciplinary action by the College consistent with established College due process. At the discretion of the Director of IT alleged violations of this policy may be referred to the Executive Leadership or College disciplinary body. In addition, the Director of Human Resources may investigate regarding the alleged infraction. Violators may also be liable for civil damages and/or criminal prosecution, if applicable.

Guest users of publicly available College IT resources are also subject to the terms of this policy. While explicit acceptance of this policy is not required for guests to access these limited IT resources, guests are accountable for their actions while using College IT resources. Guests who violate this policy will be asked to cease use and may be barred from further access. If a guest user violates state, or local law while using College IT resources, the Director of IT may report this activity to the General Counsel.

Members of the Atria Institute of Technology community who believe they have witnessed or been a victim of a violation of this policy should notify or file a complaint with the appropriate office as follows:

Students should report suspected violations to the respective HoDs. Faculty members should report suspected violations to the Principal/Provost of Academic Affairs. Staff members should report suspected violations to their department head who may report the problem to the Director of Human Resources. Reports of suspected unauthorized use or misuse of Atria Institute of Technology information technology resources will be investigated pursuant to standard College procedures.

Information technology users who are found in violation of this policy will be subject to Atria Institute of Technology's disciplinary processes and procedures including, but not limited to,

those outlined in the Student Handbook, the Atria Institute of Technology policies, and any applicable bargaining unit contracts. Privileges to use Atria Institute of Technology's information technology resources may be revoked. Illegal acts may also subject users to prosecution by local and/or state authorities.

POLICY APPLIES TO:

This policy applies to all students, faculty, and staff of the College and to all other users of information technology resources at Atria Institute of Technology. These users are

responsible for reading, understanding, and complying with this policy.

Individuals Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology.

Technology Renewal Policy

Purpose

The purpose of the Atria Institute of Technology College Technology Renewal Policy is to ensure a sustainable technology infrastructure to support the learning environment and to enable efficient business practices. In addition, support resources and lost productivity from downtime will be reduced with the use of newer equipment.

Technology equipment covered under the plan includes:

- Faculty and staff computers
- Lab and classroom computers
- Shared departmental or lab/classroom laser printers
- Centralized servers
- Network electronics including routers and switches
- Classroom technology including video projectors, white boards, and videoconferencing equipment

Technology equipment not covered under the plan includes:

- Computers purchased from grant funds and used by grant funded programs
- Reassigned computers and printers that are below the campus standard for support

Core faculty, and staff computers will be replaced or upgraded on a 4-year cycle, budget permitting. Each faculty or staff member will be allocated a single machine (laptop or

desktop) with some exceptions. Non-critical machines (e.g., student workers) will be replaced from available recycled inventory. Computers will be replaced based on the age of the machine, oldest replaced first. Principal and department heads will be allowed to determine which faculty or staff member receives the newer machine.

All lab and classroom upgrades and renovations will first be classified by the Instructional Technology Team before a design is created. Labs and classrooms will also be classified and declared under a 2, 3, or 4-year replacement cycle. Those on the 4-year cycle will receive recycled machines from the 2- or 3-year facilities. A primary goal of this process is to have the same equipment in each facility to provide consistency for students and faculty and to minimize maintenance time. Priority for the replacement cycle classifications will be given to shared facilities, usage statistics, and application requirements.

A pool of computers from this process will be reserved annually to accompany new faculty and staff positions.

Technology equipment that is covered under the plan is not to be purchased from departmental Computers and/or printers that are replaced through the renewal process are returned to IT. IT then reassigns the machines or disposes of them through the campus disposal process. Computers and printers that are below the campus standard for support will only be reassigned for special circumstances. Those that are reassigned to new purposes will not be considered in the renewal process.

A list of hardware covered under this plan will be maintained within IT.

Individuals Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology

Wireless Network Use Policy

Purpose

Atria Institute of Technology provides wireless networking services in public spaces on each campus to enable the convenience of mobile network connectivity. This service allows members of the College community to access the campus wide network from wireless devices or portable computers where coverage is available. The radio frequency airspace of the College serves as the transport medium for this technology. Some wireless devices do not confirm to frequency standards and can cause interference to wireless service which may prevent College users from obtaining or maintaining network connectivity.

The purpose of this policy and related procedures is to define responsibilities for the management and use of the wireless network and associated radio frequency airspace to

provide a reliable wireless network to the College community, to manage other uses of the wireless spectrum and to insure security across the Atria Institute of Technology network.

Scope

The Department of Information Technology (IT) will regulate and manage all wireless access points and the radio frequency bands used by wireless technology to ensure fair and efficient allocation and to minimize collision, interference, unauthorized intrusion and failure of the wireless network.

DEFINITIONS

Access Point (AP)

A hardware device that acts as a communication hub for users of a wireless device to connect to a wired network. APs are important for providing heightened wireless security and for extending the physical range of service to which a wireless user has access.

Wireless device

The end user system or device that accesses the wireless network for data communications purposes. This is normally a portable computer or personal digital assistant (PDA) containing an appropriate wireless network interface card (NIC)

PROCEDURES

Security

Users should assume that data transmitted over the wireless network is NOT secure.

Access Points

Only access points provided and installed by the IT Department or approved for installation by IT are permitted on the College network. IT reserves the right to disconnect and remove any access point not installed and configured by IT personnel or specifically covered by prior written agreement and/or arrangement with IT. In cases where the device is being used for specific academic or research applications IT will work with faculty to determine how the wireless devices may be used while maintaining required security and without causing interference. Any person found responsible for the installation of unauthorized access points may be submitted to the appropriate college authority for disciplinary action.

All access points shall be installed and configured in such a way as to comply with all security features of the wireless network, including restrictions to provide connections only to those users who are authorized to access the Atria Institute of Technology College network.

Other Wireless Devices

Unapproved wireless devices, such as portable phones and other devices with two-way radios may interfere with the operation of the College wireless network. If the IT department receives a report of interference and determines that a non-approved wireless device is causing interference the College will ask the owner of the device to discontinue its use.

Authorized Use

Only users affiliated with Atria Institute of Technology are authorized to use wireless networking on campus. IT may implement or alter data encryption and authentication security measures at any time with the proper notification to the community. These measures must be followed by all users to provide security for Atria Institute of Technology network users and electronic resources. These measures require the use of specific wireless network products and are designed to meet emerging wireless encryption and security standards. These measures may include other authentication mechanisms including authorization by username and password.

POLICY APPLIES TO:

This policy applies to all students, faculty, and staff of Atria Institute of Technology and to all other users of the Atria Institute of Technology wireless network. These users are responsible for reading, understanding, and complying with this policy.

Individuals Responsible for Revision and Implementation: CEO, Principal and Administration and Director of Information Technology.