EDWARD WATERS UNIVERSITY

INFORMATION TECHNOLOGY PROCEDURAL MANUAL

EDWARD WATERS UNIVERSITY OTIS OFFICE OF TECHNOLOGY & INFORMATION SERVICES

OFFICE OF TECHNOLOGY & INFORMATION SERVICES (OTIS)

Rev. April 2024

Overview

This document serves as a rulebook and roadmap for successfully and properly utilizing the technology resources at Edward Waters University (EWU). Careful consideration should be taken to verify that one's actions fall within the authorized parameters for access, utilization, distribution, and modification of EWU's technology resources set forth within this document.

Any misuse, misappropriation, negligence, or deliberate disobedience concerning these policies and procedures will not be tolerated. It is up to each individual employee and affiliate of EWU to familiarize him/herself with the policies and procedures set forth herein prior to signing the agreement form at the end of this document.

It is the purpose of the EWU Office of Technology & Information Services (OTIS) to provide these procedures and standards in order to address potential situations and to provide steps to take during these situations. However, not all situations can ever be addressed so it is up to each individual employee and affiliate to use these procedures and standards for an example of what type of actions to take.

OTIS does encourage all EWU employees and associates to always err on the side of caution should a difficult situation present itself that is not discussed herein. If this should occur, the employee or associate of EWU can always contact OTIS to ask for assistance.

Contents

Overview 2
Acceptable Use 6
Overview 6
Procedure 6
Accessibility 9
Overview 9
Procedure 9
Auditing 10
Overview 10
Procedure 10
Backup 12
Overview 12
Procedure 12
Data Retention Procedure 17
Overview 17
Procedure 17
Electronic Communications Procedure 18
Overview 18
Procedure 18
Emergency Notification Procedure 20
Overview 20
Procedure 20
Encryption Procedure 21
Overview 21
Procedure 21
Enforcement Procedure 23
Overview 23
Procedure 23
Equipment Configuration Procedure 24
Overview 24
Procedure 24
Guest/Visitor Access and Technology Use Procedure 25
Overview 25
Procedure 25
Illegal File Sharing 26

Overview 26
Procedure 26
Information Sensitivity Procedure 28
Overview 28
Procedure 28
Password Procedure 31
Overview 31
Procedure 31
Physical Security Procedure 34
Overview 34
Procedure 34
Personally Identifiable Information Procedure 35
Overview 35
Procedure 35
Personal Technology Service Procedure 36
Overview 36
Procedure 36
Remote Access Procedure 38
Overview 38
Procedure 38
Student Rights and Responsibilities Procedure 39
Overview 39
Procedure 39
Vendor Access Procedure 40
Overview 40
Procedure 40
Wireless Communication Procedure 41
Overview 41
Procedure 41
Procedures 42
Emergency Operating Procedure 42
Equipment Ordering Procedure 44
Guest/Visitor Access Procedure 45
Incident Management Procedure 46
Vendor Access Procedure 47
Terms and Definitions 48

Disclaimer 53
Forms 54
Authorization of User Access Form 54
Equipment Transfer Form 55
Incident Report Form 56
Personal Technology Service Consent Form 57
Policies and Procedures Manual Compliance 58
Policies and Procedures Agreement Form 59
Non-Disclosure Agreement Form 60

Acceptable Use

Overview

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

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

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

Procedure

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

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

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

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

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

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

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

The following activities are strictly prohibited, with no exceptions:

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

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

Accessibility

Overview

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

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

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

Procedure

A reasonable attempt shall be made at all times to address the needs of our students and employees, particularly when those needs are due to an accessibility issue presented by a physical impairment or learning disability of some kind. The EWU OTIS shall make every effort to ensure that each and every student is presented with an equal or comparable learning environment regardless of the hurdle they may face.

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

Please note that advance notice of these needs is required and may change due to the request. For instance, additional software needs will take some time to produce an order and install the software so it will be unreasonable to expect a request such as this to have an immediate turnaround time.

Casting aside the general expectations above, the EWU OTIS cannot be held liable for issues surrounding software application issues, hardware failures, or the inability of employees or students to convey their respective needs in a reasonable amount of time to allow such software or hardware to be properly installed.

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

Auditing

Overview

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

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

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

Audits may be conducted to:

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

Procedure

This Procedure covers all computers, equipment, and communication devices owned or operated by EWU. This Procedure also covers any computers, equipment, and communications devices that are present on EWU premises, but which may not be owned or operated by Edward Waters University. The third-party audit group will not perform Denial of Service activities at any time during an audit.

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

The access involved in the scan may include:

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

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

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

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

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

Backup

Overview

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

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

Procedure

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

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

Specific information regarding backup restoration on an institutional scale can be found in the EWU OTIS's Disaster Recovery Plan (DRP) or the associated Backup Priority List (BPL). These deal with catastrophic recovery needs that affect multiple departments or the institution as a whole.

The hardware that the EWU OTIS uses consists of two Dell EqualLogic storage devices. One device is placed in the server area of the OTIS on the Edward Waters Campus to serve as a primary storage and backup device while the other is placed in the server area of the OTIS on the EWU Campus to serve as an off-site backup and replication device.

The primary device on-campus holds all data and backups and serves as the primary device for file access and immediate backup. The secondary, off-site device replicates all data from the on-campus device to create a stable off-site copy of the data and backups present on the on-campus device.

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

- Backups: These refer to snapshots taken of the file structure and database. These snapshots are essentially pointers to changes occurring within the storage device since the last scheduled snapshot. This greatly reduces the file storage requirements necessary to hold backups while still providing the same or superior level of backup capability found in other devices.

- Replication: This refers to the copying process of all data and associated backups from the primary backup device in the EWU Datacenter to the secondary backup device offsite, managed by SecureSI. During a replication, all data and backups are replicated so that a mirror copy is retained at the SecureSI Datacenter for off-site, backup capability should a disaster or other issues occur.

Regularly scheduled backups and replications shall be performed by the EWU OTIS using the following schedule:

Hourly Backups
- 7:00 a.m. – 10:00 p.m.
- Every day, every hour as noted herein, on the hour

Weekly Backups
- 10:30 p.m.
- Every Friday

Monthly Backups
- 11:59 p.m.
- Last day of each calendar month

Mid-Yearly backups
- 12:30 a.m.
- July 1

Yearly backups
- 12:30 a.m.
- January 1

Daily Replication
- 12:01 a.m.
- All data is replicated from the EWU Campus to an off-site datacenter managed by SecureSI.

At the beginning of each day, beginning at 7:00 a.m., backups will begin and continue each hour, on the hour, until 10:00 p.m. each evening.

Every Friday at 10:30 p.m., after the last hourly backup for that day, a weekly backup will be completed.

At the end of each month, on the last day of the month, a monthly backup will be completed at 11:59 p.m.

On July 1 of each year, at 12:30 a.m., a mid-yearly backup will be completed.

On January 1 of each year, at 12:30 a.m., a yearly backup will be completed.

At 12:01 a.m. every morning, all backups and data will be replicated from the EWU campus for off- site storage and secondary backup.

All backups are clearly labeled so as to distinguish one from another easily. At minimum, the following information is provided for each backup file:

- Time (CST) – e.g. 12:00:00 AM or 12:34:59 PM
- Date – e.g. 12/31/10 or 2/29/12
- Backup Type – e.g. Hourly or End of Year

Testing for data integrity will be performed at regularly scheduled intervals by the backup hardware but may also be performed manually at random times to verify the validity, accuracy, and authenticity of the backup. These random tests should total no less than six per year and it is recommended that these tests fall approximately two months apart, less if more than the minimum number of tests are used.

We encourage that backup tests be taken within one week of the completion of the yearly and mid- yearly backups with the remaining backups spaced throughout the remaining months of the year. If six are used, it should follow this testing schedule:

- Test 1 – January 1-7
- Test 2 – March 1-7
- Test 3 – May 1-7
- Test 4 – July 1-7
- Test 5 – September 1-7
- Test 6 – November 1-7

If more than six tests are used, then the schedule may be set at the discretion of the EWU OTIS , however, two of the tests must occur no later than one week after the yearly and mid- yearly backups are completed.

Testing shall consist of one or more of the following methods of data validation and verification of accuracy and authenticity:

- **Random Dummy File Restoration:** Six to twelve dummy files are inserted on the file server at random locations. Afterwards, we will intentionally delete these dummy files. Then, recovery will be tested to verify data is being restored properly. If this verifies the data is being restored properly, the test is completed and the dummy file may be removed.
- **Random Actual File Restoration:** Recovery of a six to twelve actual random files located on the server. Comparisons will then be made with current versions of the same files to verify content and accuracy of restoration process. If the comparisons verify that the recovery was successful, then the test is completed.
- **Random File Location Verification:** Movement of a single dummy file to various locations on the file server. Initially the file is inserted onto the file server and backups are tested to verify the file exists in backups at the initial location. If this is confirmed, then the file is moved on the file server to a second location and backups are tested yet again to verify that the file is in the

second location. Once this is confirmed, the file is moved for a third time and backups are once again tested to verify the file exists in the new location. If this is confirmed then the test is completed and the dummy file may be removed. Backups are working correctly and file contents and locations are being updated appropriately.

- **Miscellaneous:** Other tests may be used at the discretion of the EWU OTIS with only one restriction: they may not interfere with access or otherwise cause any data loss on the file server.

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

- Re-routing primary traffic from backup and storage device at the EWU Datacenter to accompanying device(s) at the SecureSI Datacenter or vice-versa
- Physically transporting one device to another location
- Copying all files or a subset of files from the backup equipment to the file server
- Via the testing process described in this document
- Utilizing the EWU OTIS 's Disaster Recovery Plan
- Utilizing the EWU OTIS 's Backup Priority List
- Other methods, approved by the EWU OTIS , that do not interfere with access or otherwise cause any data loss on the file server

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

If these issues prevent backups from occurring, then the off-site backup device, managed by SecureSI will be transferred to primary backup duties and a secondary device should be purchased and then placed on-site at the EWU Datacenter to regain primary functionality.

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

- Hourly Backup
  - Copies on file: 16 per day, 112 total
  - 7 days worth of data at hourly intervals

- Weekly Backup
  - Copies on file: 12 total
  - 12 weeks (approx. 3 months) worth of data at weekly intervals

- Monthly Backup
  - Copies on file: 3 per month, 36 total
  - 36 months (approx. 3 years) worth of data at monthly intervals

- Mid-Yearly Backup

  - Copies on file: 3 total
  - 3 years worth of data at yearly (mid-year) intervals

- Yearly Backup
  - Copies on file: 3 total
  - 3 years worth of data at yearly (end-of-year) intervals

- Daily Replication
  - Copies on file: 32 total
  - 32 days worth of exact copies of existing data and backups replicated off-site in daily intervals

Online log files are retained consisting of information for each backup or replication process, hardware/software errors, access issues, or other critical errors involving the backup hardware. These entries are also emailed to the EWU Backup email account for verification and notification.

Data Retention Procedure

Overview

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

Procedure

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

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

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

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

Electronic Communications Procedure

Overview

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

- Email
- VoIP
- Videoconferencing
- Digital Signage

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

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

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

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

Procedure

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

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

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

Electronic communication from a EWU resource…

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

Emergency Notification Procedure

Overview

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

Procedure

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

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

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

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

- Chief Information Officer
- Director of Information Technology
- Director of Campus Safety & Security
- Director of Marketing, Communications & University Relations
- Vice President for Student Success & Engagement
- Vice President for Institutional Advancement, Development, Marketing & Communications
- EWU CERT Team Lead

Encryption Procedure

Overview

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

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

Procedure

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

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

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the EWU OTIS . Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

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

- Never leave any PC unattended that contains confidential EWU data or a method to access confidential EWU data.
- If you must leave a PC unattended that contains confidential information (i.e. in an open office or a conference room), only do so if proper encryption has been enabled and the PC has been powered off for no less than 5 minutes.
- Never authenticate the encryption on a PC which contains confidential EWU data or a method to access confidential EWU data and leave it unattended, allow a non-EWU user to utilize the device, or permit the device to be copied in any way.

- Never disable or bypass the encryption on a PC which contains confidential EWU data or a method to access confidential EWU data.

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

Enforcement Procedure

Overview

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

Procedure

All policies herein are applicable to any and all users of technology resources at EWU.

If it is found that any individual, department, or external entity disobeys the policies and procedures set forth within this document, whether knowingly or unknowingly, then the enforcement of such Procedure may include, but may not be limited to:

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

Equipment Configuration Procedure

Overview

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

Procedure

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

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

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

For more details on procedures required to place an order for technology equipment, please see the Equipment Ordering Procedures included in this document for detailed instructions.

Guest/Visitor Access and Technology Use Procedure

Overview

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

Procedure

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

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

Internal Access may include:

- Wireless VLANs (i.e. EWUwireless, EWUguest)
- Wired VLANs (i.e. housing, guest)
- Singular or multiple file access
- System access such as Moodle, ID Card System, etc.

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

To obtain guest/visitor access users should contact the EWU OTIS with their requested system access requirements using the attached Authorization of User Access form.

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

Illegal File Sharing

Overview

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

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

Procedure

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

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

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

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

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

Educause – Legal Sources of Online Content

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

- iTunes
- Amazon: Books/Newspapers, Video, Music, Games
- Hulu Plus
- Rhapsody

- CinemaNow
- Zune: Music, Video
- Napster
- MP3
- AmieStreet
- GameTap
- OnLive
- Netflix
- Walmart MP3 Downloads
- Blockbuster On Demand
- eMusic
- Mindawn
- GameFly

Free services

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

Information Sensitivity Procedure

Overview

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

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

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

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

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

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

Procedure

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

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

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

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

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

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

- Most Sensitive
  - Description: Operational, personnel, financial, source code, & technical information integral to the security of the institution.
  - Access: Only those individuals (EWU employees and associates) designated with approved access and signed non-disclosure agreements.
  - Distribution internal to EWU: Approved electronic file transmission methods.
  - Distribution external to EWU: Approved electronic file transmission methods to recipients within EWU. Strong encryption is highly recommended.
  - Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored on a physically secured computer.
  - Disposal/Destruction: A necessity. Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention Procedure and federal and state retention guidelines should be observed for original copies.

Password Procedure

Overview

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

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

Procedure

All passwords will meet the following criteria:

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

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

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password or a subset of the password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software
- The words "EWU", "edward waters",“university” or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

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

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

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

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

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to a supervisor.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers.
- Don’t reveal a password to vendors.
- In short, don’t reveal a password to ANYONE.
- Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger, Internet Explorer, Firefox, Thunderbird).
- Do not write passwords down and store them anywhere in your office.

- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without proper encryption.
- Change passwords at least once every three months.

Other items to remember:

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

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

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

Physical Security Procedure

Overview

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

Procedure

All areas will be classified into two categories:

- Office
- Restricted

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

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

- Switch closets
- Server rooms
- Telecommunications rooms
- EWU OTIS storage areas

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

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

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

All EWU OTIS restricted and office locations should contain the following recommended security mechanisms:

- Reinforced steel doors and frames
- Keyed deadbolt locks
- ID card access
- Steel bars over windows

Personally Identifiable Information Procedure

Overview

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

Procedure

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

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

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

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

Personal Technology Service Procedure

Overview

This Procedure will set forth the rules and regulations which will determine how the EWU OTIS personnel are to perform work on personally-owned employee or student technology products.

The EWU OTIS does not service technology equipment for individuals who are not EWU employees or students.

Procedure

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

This Procedure will set forth the rules, regulations, and guidelines for which the EWU OTISpersonnel may provide services for personally-owned technology equipment and/or projects outside of normal work hours.

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

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

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

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

- Personal technology work may be performed during regular business hours, only if such work does not directly interfere or delay the normal operations or job duties of the EWU OTIS employee.
- No on-site work. All equipment must be brought to the EWU OTISfor a preliminary diagnosis and troubleshooting.
- No parts purchases. All parts to be installed must be purchased by the user.

- No illegal software. Only legally licensed software may be installed.
- No work without proper authorization signature on consent form.

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

Edward Waters University cannot be held responsible for any work done after hours by EWU OTIS personnel on any personal technology equipment. All work provided is not warranted or guaranteed. By signing the Personal Technology Service Procedure Consent Form, you agree to these terms and conditions and waive any damages which may occur due to any work on your personal technology equipment. All work is done and once completed is left as is and no standing warranty or guarantee is implied.

Remote Access Procedure

Overview

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

Procedure

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

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

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

Student Rights and Responsibilities Procedure

Overview

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

Procedure

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

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

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

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

Vendor Access Procedure

Overview

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

Procedure

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

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

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

At all times, the vendor shall…

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

Wireless Communication Procedure

Overview

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

At present, this Procedure allows access to the EWU wireless network via any data communication device containing the hardware required to connect. Connecting to the EWU wireless network does not grant a user access to the internal networking infrastructure or any internal information of EWU, only external access to the internet. Utilizing EWU's wireless network for access to the internal network and/or information requires additional software that must be obtained through the EWU OTIS .

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

Procedure

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

All wireless data communication devices connected with EWU's wireless network that require access to EWU's internal network and/or information will be required to utilize specific software and/or access credentials obtained through the EWU OTIS to do so.

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

Procedures

Emergency Operating Procedure

In the event of an emergency, normal operating procedures should be restored as quickly as possible. Due to the small size of our department, it is beneficial that all employees learn laterally to allow for greater ability to maintain operations should any individual employee be unavailable. The steps below will indicate how operations should continue in the event of an emergency directly affecting the EWU OTIS .

1. Assess situation and determine if any personnel impact to the EWU OTIS exists. If so, go to step 2. If not, go to step 3.
2. Given any personnel impact below, the following options are available to ensure OTIS operations can continue in an emergency. If the OTIS suffers the loss of any of the following employees, the available options are:

    a. Director of Information Technology
        i. Responsibilities will defer to the President or designee until a suitable appointment can be made.
    b. Network Administrator
        i. Responsibilities will defer to the Director.
        ii. Interim assistance can be performed by SecureSI Tier II or Tier III Support or another suitable vendor to facilitate network management.
        iii. Network management is more specialized than workstation management so vendor assistance will most likely be a necessity.
    c. Desktop Administrator
        i. Responsibilities will be shared between remaining personnel.
        ii. Emergency/Interim hiring may be required.
    d. Helpdesk Administrator
        i. Responsibilities will be shared between remaining personnel.
        ii. Emergency/Interim hiring may be required.
    e. Student Helpdesk Technicians (5)
        i. Responsibilities will defer to the Helpdesk Administrator.
        ii. Emergency/Interim hiring may be required.
    f. Distance Education Administrator
        i. Responsibilities will defer to the Director.
        ii. Emergency/Interim hiring may be required.
    g. Programmer
        i. Responsibilities will defer to the Director.
        ii. Interim assistance can be performed by EWU OTIS or SecureSI to assist.
        iii. Emergency/Interim hiring may be required.
    h. Departmental catastrophe (3+ users unavailable to perform duties)

i. Responsibilities will defer to the President or designee until emergency hiring can be finalized.
ii. If necessary, assistance may be obtained from other institutions and/or vendors:
    1. SecureSI
    2. Networking: Intellicom or Skybox

i. NOTE: Emergency approval for costs associated with assistance will need to be obtained under any scenario.

3. Determine if any equipment loss has occurred. If so, proceed to step 4. If not, proceed to step 5.
4. Determine what resources are affected and bring them back up as soon as possible:
    a. Network and connectivity equipment
    b. Mission critical services (group drives, ID card system, etc.)
    c. Non-mission critical services (security cameras, wireless infrastructure, residence hall connectivity, etc.)
5. Once all connectivity and resources have been restored, normal operations can now resume.

NOTE: Please see the EWU OTIS 's detailed Disaster Recovery Plan for detailed information regarding disaster scenarios and specific planning information.

Equipment Ordering Procedure

This document is to serve as a set of guidelines for all EWU Faculty and Staff who choose to order computing equipment.

1. Contact the EWU OTIS to obtain a quote and or information regarding the equipment you wish to purchase.
2. Submit your order requisition.
3. Your order will be routed through the appropriate approving channels, including the EWU OTIS, since it is a technology equipment purchase.
4. Once your order has been approved, you may check the progress via Colleague.
5. When your equipment arrives, the Mailroom may notify you to pick up the equipment. Otherwise, the EWU OTIS will retrieve your equipment and configure it, if necessary, prior to delivering it to you.

   NOTE: All technology orders must be received by the EWU OTIS before it can be released to the purchaser. This is to ensure that the proper software is installed and all equipment is properly tagged and placed in inventory.

Guest/Visitor Access Procedure

This procedure will indicate how guests and visitors to campus should obtain access to EWU's technology resources.

1. Obtain contact information from user needing access:
    a. Name
    b. Phone
    c. Email
2. Fill out the enclosed Authorization of User Access Form.
3. Submit the form to the EWU OTIS .
4. Access will be created as soon as possible. Confirmation will be sent to requesting employee once access has been created.

Incident Management Procedure

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

1. Determine scope of incident.
2. Fill out attached Incident Management Form.
3. Ensure supervisor of employee that reported or caused incident has been notified.
4. Submit form to Director of Information Technology.
5. Administration will be notified of incident.
6. Resolution will be drafted given incident scope and individuals involved.

Vendor Access Procedure

If any vendor requires access to technology resources, please follow these steps:

1. Submit Authorization of User Access Form to EWU OTIS .
2. EWU OTIS will evaluate request and grant access based upon need and policies.
3. Vendor access will be created to comply with existing policies.
4. Requesting employees will receive email once appropriate access has been created

Terms and Definitions

Appropriate Measures

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

Approved Electronic File Transmission Methods

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

Approved Electronic Mail

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

Approved Encrypted Email and Files

Techniques include the use of AES and others. Please contact the EWU OTIS for further information.

Asymmetric Cryptosystem

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

Chain email or letter

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

Information System Resources

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

Information Technology Systems

The technology department responsible for managing EWU's computing resources.

Configuration of EWU-to-Third Party Connections

Connections shall be set up to allow third parties requiring access to the EWU campuses, networks, data, etc. These connections will be setup in order to allow minimum access so that third-party

entities will only see what they need to see, nothing more. This involves setting up access, applications, and network configurations to allow access to only what is necessary.

Domain Name System

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

Email

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

Encryption

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

Encryption Key

A software key used to gain access to encrypted data.

Expunge

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

Forwarded email

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

Individual Access Controls

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

Insecure Internet Links

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

Internet

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

Internet Protocol

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

Local Area Network

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

One Time Password Authentication

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

Personal Computer

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

Physical Security

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

Private Link

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

Proprietary Encryption

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

Public Link

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

Secure Internet Links

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

Sensitive information

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

Symmetric Cryptosystem

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

Unauthorized Disclosure

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

User Authentication (Local)

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

User Authentication (Network)

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

Virtual Private Network

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

Virus Warning

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

Wide Area Network

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

Disclaimer

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

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

Forms

Authorization of User Access Form

User requesting access: _____

Name: _____ CWID: _____

Email Address: _____

Cell Phone: _____

Employee making request: _____

Name: _____

Email Address: _____

Title: _____

Type of access needed: _____

System: _____ Duration: _____

System: _____ Duration: _____

System: _____ Duration: _____

System: _____ Duration: _____

System: _____ Duration: _____

Special Requirements: _____

_____

_____

_____

EWU OTIS Personnel Use Only: _____

Receiving Employee: _____ Date: _____

Access Created? Yes – No – Other: _____ Date: _____

Details: _____

_____

Equipment Transfer Form

User receiving equipment: _____

Name: _____ Company: _____

Email Address: _____

Cell Phone: _____

Employee transferring equipment: _____

Name: _____ Date: _____

Email Address: _____

Title: _____

Equipment being transferred: _____

Item 1: _____ Serial #: _____ EWU #: _____

Item 2: _____ Serial #: _____ EWU #: _____

Item 3: _____ Serial #: _____ EWU #: _____

Item 4: _____ Serial #: _____ EWU #: _____

Item 5: _____ Serial #: _____ EWU #: _____

Item 6: _____ Serial #: _____ EWU #: _____

Item 7: _____ Serial #: _____ EWU #: _____

Item 8: _____ Serial #: _____ EWU #: _____

Item 9: _____ Serial #: _____ EWU #: _____

Item 10: _____ Serial #: _____ EWU #: _____

Special Requirements/Notes: _____

_____

EWU OTIS Personnel Use Only: _____

Receiving Employee: _____ Date Received: _____

Details: _____

_____

Incident Report Form

User Causing/Experiencing Incident: _____

Name: _____ Incident Date: _____

Email Address: _____

Cell Phone: _____

Incident Details: _____

_____

_____

_____

_____

_____

_____

_____

_____

Special Requirements/Notes: _____

_____

_____

EWU OTIS Personnel Use Only: _____

Receiving Employee: _____ Date Received: _____

Details: _____

_____

Additional Steps Needed: _____

_____

_____

_____

Personal Technology Service Consent Form

By signing this form, I understand that the EWU OTIS is not liable for any loss of information that may occur during the service of my technology equipment. I also understand that I waive my right to file any complaints, either formally or informally, should such issues arise.

The EWU OTIS will do everything we can to ensure your data is retained; however, issues may occur that cause data loss beyond the control of the EWU OTIS, such as equipment failure, virus activity, data corruption, or pre-existing data loss prior to arrival on-site.

I understand that this service is provided free of charge and that I will be liable for any and all additional hardware costs if needed. I also understand that no warranty or guarantee is provided once services are rendered and that my only recourse is to return the equipment for additional service if needed.

By signing below, I understand the above statements and agree to the terms and conditions as described within this form and the associated Personal Technology Service Procedure.

Please Print:

Name: _____ EWUID: _____

Email Address: _____

Home Phone: _____ Cell Phone: _____

Login credentials for equipment: _____

_____

Detailed Description of Problem: _____

_____

_____

Student Signature: _____

EWU OTIS Personnel Use Only: _____

Receiving Employee: _____ Record Added to Spreadsheet? Yes – No

Date Received by Employee: _____ Problem Resolved? Yes – No

Date Returned to Student: _____

Policies and Procedures Manual Compliance

The forms following this page are required for every employee upon successfully reading and agreeing to the policies and procedures set forth within this document. All other forms mentioned earlier within this document may be used as needed during daily activities and as required for performing job duties.

A copy of these two forms shall be retained by the EWU Office of Human Resources and Administrative Services at all times to ensure all employees have signed and agreed to the policies and procedures included herein.

An employee's signature on a previous version of this policies and procedures manual does not exclude any user from being required to abide by any new or updated policies or procedures. Any signature, by any employee, upon first being hired is transferable to subsequent iterations of this document from henceforth so that all current employees shall not be required to re-sign these documents.

Upon successful approval of changes, a copy shall be made available for all employees so that any current employee may view new policies and procedures and/or any changes to current policies and procedures. If any employee disagrees with any Procedure, procedure, or change included herein, he/she may voice this complaint to Administration. However, it is important to note that since agreement with this document is stringent upon employment, any employee who does not agree to this document and sign these required forms, will effectively resign from his/her position effective immediately and all technology access will be revoked.

Employees may obtain a current copy of this document from the Human Resources or OTISat any time.

Policies and Procedures Agreement Form

I certify, by signing below, that I have read and understand the policies and procedures contained in this document.

Also, by signing below, I agree to abide by the aforementioned policies and procedures having known and understood the consequences outlined within this document.

Please print.

Name: _____ Date: _____

Title: _____

Signature: _____

Non-Disclosure Agreement Form

The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that guarantees the confidentiality of a student record. As an employee of Edward Waters University, it is important for you to familiarize yourself with some of the basic provisions of FERPA to insure that you do not violate federal law. You should not only use student information cautiously but you should also observe these same requirements for EWU employee and associate information as well. Considering this, the two following general guidelines should be observed at all times.

You must **not**, under any circumstances, release to any individual any information about a EWU student, employee, associate, vendor, etc. unless your position specifically requires you to do so. You must refer any requests for information to your supervisor to ensure that you do not potentially violate FERPA.

You should **not** acquire any student, employee, associate, vendor, etc. information that you do not need to perform your job. Also, you should **not** exchange any information that you may have learned while performing your normal job duties. A minor disclosure of information (i.e., telling a student of someone's class schedule or informing someone of a student's grades) may be a violation and could result in penalties including termination from employment.

I certify, by signing below, that I have read and understand my responsibilities stated under the Family Educational Rights and Privacy Act Non-Disclosure Agreement. Also, by signing below, I agree to abide by the aforementioned agreement, having known and understood the consequences outlined above.

Please print.

Name: _____ Date: _____

Title: _____

Signature: _____

For more information on FERPA, please refer to the FERPA website at: http://www.ed.gov/Procedure/gen/guid/fpco/ferpa/index.html

EWU
EDWARD WATERS
UNIVERSITY
EDWARD WATERS UNIVERSITY
OTIS
OFFICE OF TECHNOLOGY & INFORMATION SERVICES

EWU
EDWARD WATERS
UNIVERSITY
EDWARD WATERS UNIVERSITY
OTIS
OFFICE OF TECHNOLOGY & INFORMATION SERVICES