Hoosier Uplands Economic Development Corporation General Information Technology Policy and Procedures

Revised 02/22/2024

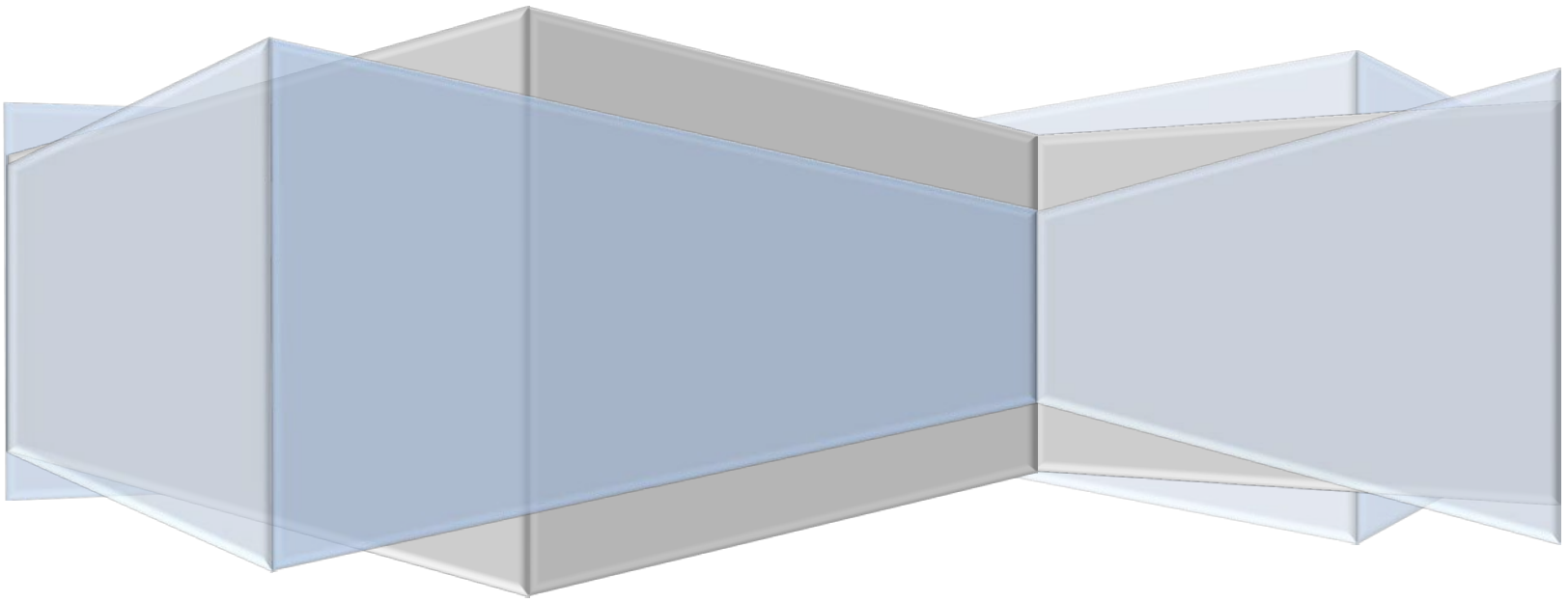

Table of Contents

1. General IT Usage Policy 2
2. General Workstation Use 6
3. Portable Workstation Use 9
4. Addendum to Corporate Computer Use (Passwords) 2/09/2023 12
5. Password Management 13
6. Procedures for Protection Against Malicious Software 15
7. Wireless Communication Policy 17
8. Router (Firewall) & Switch Policy 19
9. Disposal of Computer Hardware & Media 21
10. Cyber Security Best Practices & Procedures Training For HUEDC Staff 23
11. BYOD & Outside Entity Devices 25
12. Procedure to Account IT Assests & Media 27
13 . Incident Response & Reporting 28
14. Cyber Security Training for HUEDC Staff 28
15. Artificial Intelligence (AI) Usage & Security Policy (Addendum 2/22/24) 30

Hoosier Uplands Economic Development Agency
General IT Usage Policy

Purpose: This is the general HUEDC IT Usage Policy as per the personnel policies and procedures as dated 05/15/2020 The purpose of this procedure is to ensure the confidentiality, integrity, and availability of electronic protected client information.

Use of Corporation Computers, E-Mail System, and Internet Access

As computer and communications technological advances are made, we will have to remain vigilant regarding the integrity and proper use of those systems. Electronic mail ("E-mail") can greatly enhance the quality and efficiency of communication among employees and those we do business with and serve for our communities. However, e-mail can also be misused, with potentially serious consequences for both Hoosier Uplands and the e- mail user.
You should respect the rights and sensitivities of recipients and potential recipients or viewers, and should ensure that all e-mail messages reflect the professional image that Hoosier Uplands wishes to portray. It is expected that you will use common sense and good judgment when utilizing the e- mail and computer systems.

Data, information, messages, or communications that are transmitted or stored on our computer system, including e-mail, are Hoosier Uplands' records and property. We assume that everyone realizes that our system allows messages, once transmitted, to be printed, forwarded, or disclosed by the receiving party without the consent or knowledge of the original sender of the message. Therefore, employees should always use care in addressing any message to make sure that it is not inadvertently sent to the wrong party. This is not only important with regard to internal messages, but is equally important with respect to messages sent via the internet e-mail system. In addition, employees should operate within our public relations and code of conduct guidelines. All employees should bear in mind that the internal and external e-mail systems are to be used for business purposes only and that messages sent by the employees may be accessed by Hoosier Uplands in the ordinary course of its business at any time without notice. Employees are expressly prohibited from sending any messages or materials containing obscene, profane, lewd, derogatory, or otherwise potentially offensive language or images. The use of material containing racial, sexual, or similar comments or jokes is forbidden. Any employee who receives such e-mail should immediately report it to his or her Supervisor or the Director of Human Resources and not respond to it.

Access to the internet is a privilege that may be revoked by Hoosier Uplands at any time and for any reason. Hoosier Uplands reserves all rights to any material stored in files which are generally accessible to others and will remove any material which we, at our sole discretion, believe may be unlawful, obscene, pornographic, abusive, or otherwise objectionable.
Employees may not use Hoosier Uplands resources to obtain, view, download, or otherwise gain access to, distribute, or transmit such materials.
A number of websites exist today that make it easy to download music and video files from the internet However, many of these materials available for download are illegal duplications made available without permission of the copyright owner. Downloading and other duplication of copyrighted
materials are only legal with the permission of: (a) the actual copyright owner; or (b) a legitimate claim of "fair use." Therefore, it is our policy that music and/or video files may not be downloaded or otherwise copied from

the internet without the specific written approval of the Chief Executive Officer of Hoosier Uplands. When such downloads are authorized, we may check any downloaded files or software for viruses.

All employees must observe the following in accessing the internet:

The internet may be used only for Hoosier Uplands business. Examples of inappropriate internet uses include, but are not limited to, any traffic that violates State and/or Federal laws, any traffic that violates a copyright, trade secrets, or other intellectual property right, any traffic that is unethical in nature, the distribution of unsolicited advertising, propagation of computer worms and/or viruses, distribution of chain letters, attempts to make unauthorized entry to another network node, receipt or transmission of pornography, or use for recreational games. No employee should ever transmit confidential client or agency information over the internet or email unless there is verifiable security in place at the receiving agency.

Employees may not post opinions or statements in publicly accessible internet areas such as newsgroups and social media that are contrary to Hoosier Uplands' position, by using Hoosier Uplands equipment.

Employees may not attempt to access non-public internet sites unless they have received proper authorization from the site owner.

Employees may not misrepresent their identity in engaging in internet communications.

Employees may not disrupt the operation of Hoosier Uplands' equipment through abuse of or by vandalizing, damaging, or disabling the hardware or software.

1. Employees may not sell or purchase products from third parties via the internet without the specific approval of their supervisor. In addition, Hoosier Uplands' credit card numbers may not be transmitted over the internet unless the transmission is encrypted. As a general rule the use of operating system passwords are required on all staff computers & mobile devices (Laptops, Tablets, Agency Owned Smart Phones).

Passwords are required for access into individual software applications, network applications, and email are allowed upon the express permission of the Division Director and approval by the CEO.
The use of passwords must follow the following guidelines:

1. Passwords are recorded and given to the Division Director and or direct supervisor as soon as they are created or updated.

2. Upon request of the CEO or Division Director, IT Services will give access to accounts and or change account passwords on any HUEDC Staff

3. Division Directors will supply the IT Director with a list of computers and users and the corresponding credentials.

4. The department will update any changes to this list and send the revised copy to the IT Director. Access to any user account will be made available to the CEO upon request.

5. Passwords will be implemented and changed on a regular basis (*see password management*)

6. If a password change is required after a set amount of days by the software application, (as per HIPAA or Software Vendor regulations), the user must immediately notify their direct supervisor and or Division Director of the change.

7. The sharing of passwords with unauthorized users is prohibited.

8. Any employee, who leaves employment (voluntarily or involuntarily) without providing full access to any computer he or she was using, will forfeit any personal leave accrued at the time of separation. The willful and or premeditated act of disabling access and or damaging critical data information on an employer's computer by an employee (formerly or presently employed) is a criminal act and can be prosecuted.

Finally, to reiterate, the Agency supplied computer equipment is to be used exclusively for business-related reasons. It should be understood, in light of this policy, that playing games on computers is not authorized. If there are any questions as to whether a certain intended use of the computer equipment is appropriate, you should direct those questions to the Hoosier Uplands Director of Human Resources or the Chief Executive Officer. This policy is exceedingly important and, as is true of our other policies, any violation may result in discipline, up to and including termination, regardless of the date of discovery. Any known or suspected violations should be reported immediately to the appropriate Department Director, IT Services Director and or the Chief Executive Officer.

Hoosier Uplands Economic Development Agency
General Workstation Use Procedure

Purpose: The purpose of this procedure is to ensure the confidentiality, integrity, and availability of electronic protected client information by describing the appropriate use of all workstations that contain or that can access HUEDC's electronic protected client information.

1. Generally

Members of HUEDC's workforce should use workstations in compliance with this procedure. *In the case of HIPPA covered entities all policy and procedures are to follow the HIPPA policy and procedures for each entity.*

2. Enforcement

Violation of this Workstation Use Procedure is a sanctionable action under HUEDC's Policies for Protection of the Privacy and Security of Protected Information.

3. Policies

Members of HUEDC's workforce should use their workstations to access only the electronic protected health information which they have been authorized to access and to which they have been granted access. Furthermore, members of HUEDC's workforce should only use their laptop workstations to perform job related tasks.

a. Location

When placing a workstation or monitor in an office, the member of HUEDC's workforce should place the monitor so that it cannot be viewed from a vantage point outside of an employee's office or work area. Preferably, the monitor should be placed in a position where only the employee can view it. Workforce members should consider factors such as location of windows and doors and sightlines from these points.

b. Monitors

The Privacy and or Security Officer shall ensure that a device is placed on each workstation's monitor designed to prevent viewing the monitor from an angle.

4. E-Mail

Generally

The HU Email system has been implemented for the express use of sending work related information. Members of HUEDC's workforce should refrain from sending and or receiving personal e-mails using the HU Email

system. The sending and receiving of email containing any ePHI information must be encrypted either through the HU email encryption or an encryption system provided by the sender. The sending or receiving of ePHI that is not encrypted is strictly prohibited. *(For more info please refer to the HU Agency Policies and Procedures Handbook).*

a. Attachments

Members of HUEDC's workforce should not open e-mail and/or e-mail attachments that are received from unknown senders. E-mail from unknown sources should be deleted immediately. Attachments that may carry ePHI must go through an encryption system (*see HU Email policy above*).

b. Maintenance & Housekeeping

Staff members are responsible for maintain their HUEDC mailbox account. This includes cleaning and removal of non-critical email and or older email, which is no longer relevant to the user's job responsibilities. Staff needing older email archives should contact the IT Services department for options.

5. Internet Use

Internet access has been established for Hoosier Uplands business use only. Members of HUEDC's workforce are prohibited to access the Internet for personal use *(For more info please refer to the HU Agency Policies and Procedures Handbook).*

When accessing the Internet, members of HUEDC's workforce shall not visit websites that violate the law or that could be offensive to other members of HUEDC's workforce. Furthermore, members of HUEDC's workforce should not download files from the Internet to their workstations. HUEDC shall monitor all Internet traffic in order to ensure that members of its workforce comply with these policies.

6. Hosting a Website from a Workstation

Members of HUEDC's workforce shall not create web sites that are either hosted by HUEDC's computers or accessed through HUEDC's network.

7. Settings and Administration

All HUEDC Staff should have a comprehensive password in accordance to NIST standards.

The IT Dept. shall be responsible for configuring the workstation and for ensuring that users do not have administrative privileges and are not able to alter the settings on the workstation upon the discretion of IT Services.

.

8. Saving Files

Members of HUEDC's workforce shall not save files containing ePHI to their workstations. Instead, all files

shall be saved to the central application, central file folder, or cloud based application. The use of Flash USB storage is prohibited to backup only and should be encrypted and or password implemented.

9. Firewall

The IT Dept. Staff shall ensure that each workstation has a firewall installed. The IT Director shall configure the firewall according to the rules established by the Security Committee and IT department governing allowed and denied access. Furthermore, the firewall shall be configured to initiate when the workstation is started.

10. Virus Protection

The IT Dept. Staff shall ensure that each workstation has a software program installed designed to intercept, detect, and remove any malicious software The IT Dept. Staff also shall ensure that the software has all patches installed and has the most recent virus definitions.

11. Workstation Back-up

Members of HUEDC's workforce should ensure that any files that are necessary for them to perform their job are properly backed up on authorized media approved by IT Services.

12. System & Application Updates

All workstation (desktops, laptops & tablets) OS systems & application software are to be updated and patch with the latest general release. Automatic updates are to be turned on by IT Services. It is strongly suggested that all users keep their workstations powered on overnight with screen blanking enabled and reboot their system at least once a week or when requested by system or application. Workstations will have proper power protections installed in case of environmental power surges.

Hoosier Uplands Economic Development Corporation
Portable Workstation Use Procedure

Purpose: The purpose of this procedure is to ensure that the confidentiality, integrity, and availability of electronic protected health information by describing the appropriate use of all portable workstations that contain or that can access HUEDC's electronic protected information.

13. Generally

Members of HUEDC's workforce should use laptop workstations in compliance with this procedure. *Note: In the case of HIPPA covered entities all policy and procedures are to follow the HIPPA policy and procedures for each entity.*

14. Enforcement

Violations of this Portable Workstation Use Procedure may be punished according to HUEDC's policy for sanctions contained in HUEDC's Policies for Protection and Security of Protected Health Information, Section IV, I.

15. Procedures

Members of HUEDC's workforce should use their laptop workstations to access only the electronic protected health information which they have been authorized to access and to which they have been granted access. Furthermore, members of HUEDC's workforce should only use their laptop workstations to perform job related tasks.

16. Use of Workstation Away from Office

When away from HUEDC's office, members of HUEDC's workforce should ensure that, when in use, portable workstations are located so that unauthorized persons may not view electronic protected health information that appears on the monitor.

17. E-Mail

a. Generally

Members of HUEDC's workforce are allowed to access web based email systems only to send and receive personal e-mail from their laptop workstations.

b. Attachments

Members of HUEDC's workforce should not open e-mail and/or e-mail attachments that are received from unknown senders. E-mail from unknown sources should be deleted immediately.

18. Internet Use

a. When Away from HUEDC's Office

When a member of HUEDC's workforce is away from his or her workplace and needs to access the Internet with his or her laptop, they can use an available ligitimate internet hotspot (such as a hotel system or the facility in which they are visiting) or use a cellular hotspot if one has been assigned to you by the IT dept.

When accessing the Internet using a wireless connection, all ePHI must go through an encrypted system or secure VPN or secure WiFi platforms. No ePHI will be transmitted on any unsecure internet connection.

19. Personal Internet Use

No personal use

Members of HUEDC's workforce may only use their portable workstations to access the Internet in furtherance of their job duties. Portable workstations shall not be used to access the Internet for personal use.

20. Settings and Administration

The IT Dept. Staff shall ensure that each workstation requires a username and password to gain access. For workstations that are shared by members of HUEDC's workforce, each individual user shall have a unique username and password.

The IT Dept. Staff shall be responsible for configuring the workstation and for ensuring that users do not have administrative privileges and are not able to alter the settings on the workstation.

Each workstation should be configured to require a username and password to shutdown the screensaver. The screensaver should be configured to activate automatically after three (3) minutes. Additionally, the screensaver should be configured so that when the user leaves the computer unattended the user may start the screensaver immediately.

21. Saving Files

Members of HUEDC's workforce may save files containing EPHI to their portable workstations. However, all such files shall be saved to the network application or file server folder assigned whenever the workforce member returns to the office .

22. Firewall

The IT Dept. Staff shall ensure that each portable workstation has a firewall installed. The IT Dept. Staff shall configure the firewall according to the rules established by the Security Committee and IT department governing allowed and denied access. Furthermore, the firewall shall be configured to initiate when the workstation is started.

23. Virus Protection

The IT Dept. Staff shall ensure that each workstation has a software program installed that is designed to intercept, detect, and remove any malicious software. The employee who has been assigned the laptop shall also ensure that the anti-virus software has all current patches installed and has the most recent virus definitions. Any issues or error messages pertaining to the anti-virus or firewall systems should be reported to the HU IT Dept. immediately.

24. Workstation Back-up

Members of HUEDC's workforce who are away from HUEDC's office with their portable workstation should make duplicate retrievable copies of all files and electronic protected health information at the end of each business day while away. Immediately upon returning, a complete back-up should be performed in accordance with HUEDC's back-up policies and procedures.

Hoosier Uplands Economic Development Corporation (2/09/2023)
Addendum to Corporate Computer Use Policy

Subject: Password usage policy on corporate computers & software accounts

Purpose: This addendum is a clarification and reminder of the Hoosier Uplands corporate policy concerning the use of passwords on agency owned computers & devices. All HUEDC devices will implement OS system and application passwords according to NIST standards

The only exceptions to this rule fall under the following conditions:

1) Computers that have been deemed by their Division Director & IT Director to fall under the federal HIPAA regulations.

2) Those computers deemed to have confidential information that need a more comprehensive password scheme, that has the prior approval of the Chief Executive Officer.

The use of passwords must follow the following guidelines:

1) Passwords are recorded and given to the Division Director and or direct supervisor as soon as they are created or updated.

2) Upon request of the CEO or Division Director, computer users will provide the current password.

3) Division Directors will supply the IT Director with a list of computers and users Division directors will notify IT Services when a user has a change in their employment status or job position that requires an account change.

4) The department will update any changes to this list and send the revised copy to the IT Director. A copy of this list will be made available to the CEO upon request.

5) If a password change is required after a set amount of days by the software application, (as per HIPAA or Software Vendor regulations), the user must immediately change their passwords as directed.

6) The sharing of passwords with unauthorized users is prohibited.
7) Any employee, who leaves employment (voluntarily or involuntarily) without providing full access to any computer he or she was using, will forfeit any personal leave accrued at the time of separation. The willful and or premeditated act of disabling access and or damaging critical data information on an employer's computer by an employee (formerly or presently employed) is a criminal act and can be prosecuted.

Hoosier Uplands Economic Development Corporation
Password Management Procedure

Purpose: This procedure is designed to ensure that if passwords are maintained in a manner that reduces the risk of unauthorized entry into HUEDC's information systems. Note: *This policy does not apply to departments that are deemed to be HIPPA covered entities. Those departments will follow the policy and guidelines laid out in their departmental HIPAA policy and guidelines.*

Responsible Party: The Department Directors along with the IT Services Department shall be responsible for ensuring that this procedure is followed by members of HUEDC's workforce.

25. Password Requirements

a. HUEDC's information systems shall use passwords to authenticate individual users. Each user will be assigned a unique password. A password must be at least eleven (11) characters long. A password may not have any part of the user or login name. Random character passwords are encouraged. A password must have at least one (1) alpha numeric, one (1) numeric and one (1) special characters (!@#$%&).

The IT Director shall configure HUEDC's information systems to only accept passwords that meet the above criteria.

The IT Dept. Staff shall assign each user a password when the user's account is created. The workforce member's supervisor shall provide the password to the user by document or email if applicable. The user shall be required to change the password. At that time, the workforce member will notify their direct supervisor and the security officer who will then document the change.

26. Password Expiration and Renewal

a. Password Expiration

Password be changed every 120 days from the date of creation (unless a shorter time period is required by HIPPA covered entities). After that time, the user shall choose a new password in accordance to complexity rules.

27. Safeguarding Passwords

Users shall not write passwords down anywhere around their workstations. Users shall not share passwords with other users.

Users should never disclose their passwords in an email.

HUEDC Procedure for Protection Against Malicious Software

Purpose: The purpose of this procedure is to ensure that HUEDC's information systems are protected against malicious software.

28. Anti Virus Software

The IT Dept. staff shall ensure that all HUEDC workstations have a software program installed that is capable of detecting and removing malicious software. This software shall be configured to automatically scan all e-mail attachments, removable media, and any other files downloaded onto the workstation or any electronic media connected to the workstation.

The IT Dept. staff shall ensure that this software is regularly updated, has the most current virus definitions, and has the most current patches installed. The IT Dept. shall ensure that the auto update feature of the anti-virus software is enabled and will make periodic check to make sure it has been updated and is in good working order.

In the event of a malicious computer virus outbreak in the agency the following procedures will be implemented.

1) Isolation and disconnection of any and all computers infected by either hardware or software means to be determined by IT Services.

2) Lockdown and isolations of all servers until scanned.

3) Use of centralized antivirus software to load latest virus definitions and fixes and distribute through the network.

4) Perform a security evaluation after the initial outbreak has been contained and infected system have been cleaned.

29. Internet Firewall

The IT Dept. Staff shall ensure that HUEDC has a firewall program or appliance installed between the Internet and its local area network. This firewall shall be configured to allow members of HUEDC's workforce to use the Internet in conformance with HUEDC's polices and procedures on Internet usage, but should prevent unauthorized access to HUEDC's network from the Internet. The exact configuration of the firewall will be determined by the IT Director and documented in the network configuration files located in the IT Director's office.

30. Other Procedures

a. E-mail

Members of HUEDC's workforce shall not open e-mail attachments that are part of e-mail that originated from an unknown source. The e-mail shall be deleted immediately upon receipt. (*See Cyber Security Training Section)*

b. Downloading Software from the Internet

Members of HUEDC's workforce shall not install software on their workstations. Furthermore, members of HUEDC's workforce shall not download software or other files from the Internet. In the event an employee believes a piece of software, whether from the Internet or elsewhere, or a file from the Internet is necessary for the employee to do his or her job, the employee shall obtain the approval of the IT Director prior to downloading any files or installing any software. The IT Director shall review the request and, if appropriate, shall download and install the software for the person requesting the software.

The IT Dept. shall implement procedures governing the appropriate handling of e-mail and e-mail attachments and other procedures regarding downloading files from the Internet. These procedures shall be designed to prevent employees from inadvertently introducing malicious software into HUEDC's environment and to prevent the propagation of malicious software due to employee failure to follow HUEDC's policies and procedures. These procedures shall be detailed in HUEDC's Workstation Use Procedure. (*See Cyber Security Training Section)*

Hoosier Uplands Economic Development Corporation
Wireless Communication Policy

1. **Purpose:** This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a HUEDC network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the IT Services Team are approved for connectivity to a HUEDC network.

   Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an

2. Standard

General Requirements

All wireless infrastructure devices that connect to a HUEDC network or provide access to HUEDC Confidential, HUEDC Highly Confidential, or HUEDC Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from HUEDC production device SSID.
- Broadcast of lab device SSID must be disabled.

Wireless Device Requirements

All wireless infrastructure devices that provide direct access to a HUEDC network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 12 characters) on the wireless client and the wireless access point
- Disable public broadcast of SSID
- Change the default SSID name
- Change the default login and password
- All external wireless devices that are NOT the property of HUEDC will only be allowed to access the guest WiFi only unless spacifically authoried by the CEO and or IT Services. Unauthorized domain access is prohibited.

\

3. Policy Compliance

Compliance Measurement

The IT Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Services Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Hoosier Uplands Economic Development Corporation
Router and Switch Security Policy

.

Purpose: This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity.

Policy: Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.

2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

3. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services
    d. UDP small services
    e. All source routing and switching
    f. All web services running on router
    g. Discovery protocol on Internet connected interfaces
    h. Telnet, FTP, and HTTP services
    i. Auto-configuration

4. The following services should be disabled unless a business justification is provided:
    a. Discovery protocol and other discovery protocols
    b. Dynamic trunking
    c. Scripting environments, such as the TCL shell

5. The following services must be configured:
    a. Password-encryption
    b. NTP configured to a corporate standard source

6. All routing updates shall be done using secure routing updates.

7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

9. Access control lists for transiting the device are to be added as business needs arise.

10. The router must be included in the corporate enterprise management system with a designated point of contact.

11. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging
    c.
    d. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    e. Router console and modem access must be restricted by additional security controls

Policy Compliance

Compliance Measurement
The IT Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT Services team in advance.

Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Hoosier Uplands Economic Development Corporation
Procedure for Disposal of Computer Hardware

Purpose: The purpose of this procedure is to ensure the confidentiality of HUEDC's electronic protected health information is maintained even when computer hardware or storage media are discarded.

Procedure: Electronic protected health information shall be removed from computer hardware and other electronic media in the following manners:

30. Computer Hardware

Option 1 - Reformat Hard Drive and Re-Install Software

The IT Dept. Staff shall ensure that all computer hardware containing electronic protected health information is reformatted. This option is only to be used if the unit in question is being redeployed to another member or division of HUEDC. The IT Dept. Staff shall then reinstall any operating system or other software that was originally installed on the computer's hard drive or any other software that was purchased by HUEDC.

Option 2 - Wipe Hard Drive Prior to Disposal of a Unit Being Taken Out of Service

The IT Dept. Staff shall, prior to reformatting the hard drive, ensure that all electronic media containing electronic protected health information have had the files deleted using a program that rewrites information over the used sectors of the disk. In the case of a program that will rewrite over a sector a number of times chosen by the user, The IT Dept. Staff shall ensure that at least three (3) rewrites are performed.

If the computer is to be donated or sold, after the wipe is completed, the IT Dept. staff shall remove the hard drive from the unit and physically destroy it before disposal.

31. Other Electronic Media

a. Disposing of External Hard Drives, Floppy Disks, Zip Disks, and Other Removable Magnetic Storage Media

b. Disposing of CD-ROMS and Other Non-Rewritable Forms of Optical Storage.

In some situations, HUEDC stores electronic protected health information to write once compact disc media. When HUEDC determines it is appropriate to dispose of these compact discs, the IT Dept. staff shall ensure that the discs are rendered physically unusable prior to disposal.

32. Disposing of Rewritable Optical Media

In some situations, HUEDC stores electronic protected health information to rewritable compact disc media. When HUEDC determines that it is appropriate to dispose of these rewritable discs, the IT Dept. staff shall

ensure that the discs are erased. This shall be done by using the appropriate software to return the CD-RW to a pristine state. Simply deleting the table of contents is not sufficient.

33. Disposing of Flash Drive Media

In some situations, HUEDC stores electronic protected health information to flash drive media. When HUEDC determines that it is appropriate to dispose of these flash drives, the IT Dept. staff shall ensure that the drives are erased. This shall be done by using the appropriate software to return the flash drive to a pristine state. Simply deleting the table of contents is not sufficient.

Hoosier Uplands Economic Development Corporation Cyber Security Best Practices & Procedures Training For HUEDC Staff (2/9/2023)

1. All HUEDC staff will be required to complete all cyber security training assigned by IT services. These trainings will be made available online via the provided training curriculum.

2. Directors will be responsible that all staff comply with these training requirements IT services will provide a detailed report on user training status.

3. IT services will record and keep all staff training along with the creation and removal of staff accounts and all pertinent training data.

TESTING & SIMULATIONS

4. IT services will implement cyber security simulations and scenarios on a regular basis and report these findings to the division directors, administrative staff and CEO upon request.

5. Staff who are deemed to be at particular risk will be required to receive additional trainings and resources as needed.

6. Staff will be given sufficient time to complete the required training. Staff will also be given reminders and a set timeframe for completion.

7. IT services will make available additional training and other resources to all HUEDC staff. These may or may not be mandatory but are highly recommended. IT Services will notify all staff when these training sessions are available via email and or verbal communications.

COMPLIANCE & EXEMPTIONS

8. Failure to complete required training in the set timeframe will be reported to the division director and administrative services. Disciplinary action may be taken upon the discretion of the division director, administrative staff and or CEO.

9. IT Services will assist in any staff person who is unable to access training material or needs additional assistance with the material content. HUEDC staff will not be penalized for non-compliance if access or material is unavailable. HUEDC staff will be exempt from training requirement if it is deemed that their job position does not require them to have any cyber footprint in the HUEDC domain to be determined by their division director administrative staff and or CEO.

HUEDC:BYOD (Bring Your Own Device) & Outside Entity Device Policy

Purpose: HUEDC grants its employees the privilege of using smartphones and tablets of their choosing at work for their convenience. HUEDC reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below. This policy is intended to protect the security and integrity of HUEDC's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. HUEDC employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Note: HUEDC departments that fall under the HIPPA guidelines should follow the policies set forth by their departmental HIPPA acceptable use policy.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of HUEDC.
- The company defines acceptable personal use on company time as reasonable and limited personal communication.
- Devices' camera and/or video capabilities are/are not disabled while on-site.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Harass others
    - Engage in outside business activities
    - Etc.
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc. as per the permission of their department director and or executive director. Employee will register their device with IT services
- HUEDC has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
- Client and or general public devices are expressly forbidden on any HUEDC infrastructure network (wired or wireless)
- Client and or general public storage devices (such as flash drives, USB hard drives, ect.) are expressly forbidden to be used on any device owned by HUEDC
- Outside business entities (such as state officials, auditors, resellers etc.) are allowed limited access by permission of department directors, executive director and CEO.

Devices and Support

- Smartphones including iPhone, Android, and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Security

- In order to prevent unauthorized access, devices connected to the HUEDC network and or email system it is required that the device be password protected and or bio security features are enabled depending on the features of the device and a strong password is required to access the company network.
- It is also recommended that the device should lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees' access to company data is limited based on user profiles defined by IT Services and automatically enforced.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- HUEDC reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Hoosier Uplands Economic Development Corporation
Procedure to Account for
Computer Hardware and Electronic Media

Purpose: This procedure is designed to ensure that HUEDC keeps an accurate record of the computer hardware within its work environment.

HUEDC's IT department shall perform an inventory to determine what computer hardware and electronic media is maintained by each of HUEDC's departments. This inventory shall be recorded on HUEDC's Initial Department Accounting of Computer Hardware and Electronic Media Form. This inventory shall be provided to the IT Director who shall maintain the master inventory.

After the initial inventory, the IT Director/IT Dept. shall provide an inventory update whenever a move of equipment occurs, new equipment is added, or old equipment is removed. This update shall be recorded on HUEDC's Department Hardware and Electronic Media Inventory Update Form and submitted to the division director and security officer. The IT Director shall then update the master inventory list based upon the information provided in the update form.

Hoosier Uplands Aging Division
Incident Response and Reporting Procedure

Purpose: The goal of this procedure is to ensure that HUEDC responds to security incidents and or physical disasters in an appropriate manner.

Note: Along with the following procedures IT Services will follow the procedures and guidelines set aside in the HUEDC Disaster Recovery Procedures (DRP) manual. HUEDC departments that fall under the HIPPA guidelines should follow the policies set forth by their departmental HIPPA incident response policy.

34. Preparation

a. The Security Officer/ IT Director shall ensure that the security of HUEDC's information systems is maintained at a reasonable and appropriate level.

b. Because training is important to ensure that procedures are followed, Security Officer shall ensure that HUEDC's security training program includes training employees on how to report and respond to a security incident.

c. Incident simulations will be performed on an annual basis.

35. Detection

a. The Division Director and or Deputy Directors shall be the central point of contact for incident reporting. When a member of HUEDC's workforce determines that a security incident has occurred, or detects evidence that a security incident may be imminent, that person shall notify the Division Director and or Deputy Directors. The Division Director will then notify the IT Director/IT Dept. who shall then implement HUEDC's Incident Response and Reporting Procedure.

36. Analysis

Upon detection of a security incident, the IT Dept. shall immediately begin efforts to determine the nature, scope, and source of the incident. The IT Director shall also endeavor to determine the potential harm from the incident including information at risk and the level of risk presented. At this point the CEO and or proper Administrative staff will be notified of the incident and any potential risk to other computers.

37. Containment

a. The IT Director shall work with department heads to determine parameters for containment. These parameters shall be used by the IT Director/IT Dept. to determine when to begin containment procedures. Once the IT Director/IT Dept. has determined the nature and scope of the incident, this information shall be used, in conjunction with the containment parameters, to determine an appropriate containment strategy and when that strategy should be implemented.

b. Once the IT Director/IT Dept. determines that containment shall begin, the IT Director/IT Dept. shall immediately take steps to isolate those systems that have been affected or compromised by the incident from the rest of HUEDC's information systems.

c. The affected or compromised systems shall remain isolated until the incident is resolved.

38. Eradication

Upon the identification of a security incident, the IT Director/IT Dept. shall begin eradication procedures as soon as possible.

39. Recovery

a. After the IT Director/IT Dept. is certain that the security incident has been resolved, the IT Director shall investigate whether data was lost or altered during the incident. If the IT Director determines that data was lost or damaged, the IT Director shall determine the extent of loss or alteration to data and shall restore lost or damaged information.

b. IT Director/IT Dept shall take steps to mitigate the harm from the security incident by following HUEDC's mitigation procedures.

The IT Director shall document the occurrence of the security incident. This documentation shall include; date of the incident, extent of the incident, duration of the incident, response to the incident, and any other pertinent information that he or she determines is necessary for future reference or any reporting require.

ARTIFICIAL INTELLIGENCE USAGE AND DATA SECURITY POLICY
(February 23, 2024)

This document outlines HUEDC's policy on the use of generative AI platforms such as ChatGPT, Google Bard, or other similar AI platforms using "large language models" (LLMs) for work tasks of any kind.

Protecting Sensitive Information
The purpose of this policy is to ensure that private, confidential, proprietary, trade secrets, or otherwise sensitive information is not intentionally or inadvertently transmitted to such platforms or related third parties.

Authorization from the CEO, Department Directors & IT Services Directors
Before using generative AI, employees must obtain explicit, documented authorization from the CEO and Department Directors in consultation with the Information Technology Services Directors.

Considerations for authorizing use of Generative AI
The decision to authorize an employee's use of generative AI will be based upon the following considerations, and the decision may be withdrawn at any time:

1. The nature of the task, the role of the requesting employee, and the sensitivity of the information that the employee regularly accesses.

2. Whether the employee has, or is willing to undergo training on the appropriate use and risks of using generative AI platforms.

3. Whether the employee clearly understands the nature of the information he will be using, including whether the information is private, confidential, proprietary, a trade secret, or otherwise sensitive.

4. Whether the employee has clearly defined the tasks and developed a thoughtful approach to drafting prompts.

5. Whether the intended use is likely to yield helpful results while avoiding the disclosure of confidential information, proprietary data, trade secrets, or otherwise sensitive information.

6. Whether the requesting employee is the only person who intends to use the AI generative platform.

7. Whether there are procedures in place for the employee's supervisor to regularly review the employee's prompt and the result history he receives.

Policy Violations

The unauthorized use of generative AI may result in the employee losing permission to use generative AI or further disciplinary action, up to and including immediate termination of employment.

Any known or suspected violation of the guidelines and requirements outlined in this document, even if inadvertent, must be reported immediately to the employee's supervisor.