Computer, Network & Data Use Policy

Employee Information Technology Policy

Purpose

Upshur County must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios.

Principles

Upshur County shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

General

a. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.

b. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.

c. Records of user access may be used to provide evidence for security incident investigations.

e. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

Access Control Authorization

a. Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by Gilmer Computer Tech.

b. Passwords are managed by Gilmer Computer Tech.

c. Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

Network Access

a. All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.

b. All staff and contractors who have remote access to Upshur County networks shall be authenticated using the VPN authentication mechanism only.

c. Segregation of networks shall be implemented as recommended by Upshur County network security research. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.

User Responsibilities

a. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.

b. All users must keep their workplace clear of any sensitive or confidential information when they leave.

c. All users must keep their passwords confidential and not share them.

Application and Information Access

a. All County staff and contractors shall be granted access to the data and applications required for their job roles.

b. All County staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from Department Head.

c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

Access to Confidential, Restricted information

a. Access to data classified as ‘Confidential’ or ‘Restricted’ shall be limited to authorized persons whose job responsibilities require it, as determined by the Computer, Network & Data Use Policy or Department Head.

b. The responsibility to implement access restrictions lies with Gilmer Computer Tech.

Reporting Requirements

a. Daily incident reports shall be produced and handled within the IT Security department or the incident response team.

b. Weekly reports detailing incidents shall be produced by the IT Security department and sent to the IT manager or director.

c. High-priority incidents discovered by the IT Security department shall be immediately escalated; the IT manager should be contacted as soon as possible.

d. The IT Security department shall also product a monthly report showing the number of IT security incidents and the percentage that were resolved.

Data Breach Response Policy

Background

This policy mandates that any individual who suspects that a theft, breach or exposure of Upshur County Protected data or Upshur County Sensitive data has occurred must immediately provide a description of what occurred via e-mail to openticket@geekyourpc.com or by calling (903) 680-5086. This e-mail address & phone number are monitored by Gilmer Computer Tech. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of Upshur County. Any agreements with vendors will contain language similar that protects the fund.

As soon as a theft, data breach or exposure containing Upshur County Protected data or Upshur County Sensitive data is identified, the process of removing all access to that resource will begin.

Gilmer Computer Tech will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT staff – Gilmer Computer Tech
- County Judge
- Finance (if applicable)
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by Gilmer Computer Tech

The above will be in charge of deciding how & when to communicate the breach to: a) internal employees, b) the public, and c) those directly affected. Anyone outside of this team found in violation of communication about incident may be subject to disciplinary actions. See Section below "Enforcement"

IT Risk Analysis

The security official and Management Teams conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of DATA held by the covered entity.

IT Breach Tracking

It is Gilmer Computer Tech policy to maintain a detailed log of every breach of unsecured DATA reported or detected. This can be from Malware, Spyware, or virus infections, or direct system access from unauthorized individuals.

Breaches are immediately reported to Gilmer Computer Tech for the appropriate action

Procedure

In the event of a breach, the user that identifies the breach:

1. Send email to openticket@geekyourpc.com with the information:

   a. A description of what exactly happened—the circumstances surrounding the breach

   b. The date of the breach

   c. The date of the discovery

   d. A description of all types of information involved in the breach

   e. A description of what types of notifications were made

   f. h. Details of steps taken to resolve the situation and make corrective action/mitigation

2. A log (ticket placed in the ticketing system by Gilmer Computer Tech) must be maintained that contains the information.

3. The user will then contact their supervisor to notify them of the incident.

Termination Procedures

A staff member's authorization to use information resources and to access DATA ends upon termination of employment.

Procedures

1. HR department Open ticket with Help Desk (email: openticket@geekyourpc.com)

   a. Employee name

   b. c. Any special requests (i.e. do not erase email or forward email to another user)

2. IT:

   a. Change Active Directory user account password

   b. Disable Active Directory User Account

3. IT / Internal practice Admin:

    a. Disable application specific accounts

Company Shared Files

Each defined role also grants or denies access to specific shared files on the network.

Procedure

To request system access:

1. Submit email to openticket@geekyourpc.com or call (903) 680-5086

    a. Individual or Group Name

    b. Data requested access to

2. Gilmer Computer Tech will add users to the appropriate group for accessing the requested share

3. Department head will validate access with user

Protection from Malicious Software (Anti-Virus Software)

Anti-virus software is installed on all computer workstations and servers to protect Upshur County and its information from attack by malicious software such as computer viruses, worms, and Trojan horses.

Employees are responsible for reporting all viruses detected by anti- virus software. Gilmer Computer Tech will confirm that the viruses have been successfully removed from the affected machines.

Employees with access to the Internet should not open email messages and email attachments from unknown senders.

Email is also protected by a third-party cloud service to scan and clean email before it arrives in the user mailbox.

Staff members cannot disable anti-virus software and must immediately take action to report virus infections and remove viruses from affected machines when the anti-virus software identifies an infection.

All workstations and servers are connected to a centralized management console that alerts IT of outbreaks, infections, lack of updates, etc.

Clean Desk Policy

Overview

This policy applies to all Upshur County employees, elected officials and affiliates.

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the work day.
4. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
5. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
6. Upon disposal Restricted and/or Sensitive documents should be shredded
7. Whiteboards containing Restricted and/or Sensitive information should be erased.
8. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
9. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Access Authorization

Staff members receive authorization to access DATA and to use Upshur County workstations, conduct transactions, and run software applications based on their job responsibilities and qualifications. Authorization enables staff members to use the information resources.

Staff members should not access information for other staff members who lack appropriate authorization.

Procedures

Only authorized staff members are allowed to use workstations (computer terminals, personal computers, and other devices) that can access Upshur County.

a. A unique user ID and password are required to use Upshur County information system.
b. New staff members receive security training as part of their orientation.

c. Contractors and consultants receive training and/or information on the security policies and procedures.

All users must use their individual Network User accounts and passwords when logging on to Upshur County information system. Passwords should not be written down or disclosed to other members of the staff, friends, family, or anyone else.

A staff member may not use another staff member's user name and password to access Upshur County information system. Staff members may not give their passwords to other staff members.

Automatic Screen Locks

All workstations are configured to log users off within 2 minutes of inactivity. After being automatically logged off, a user must re-enter his or her user name and password to resume the interrupted activity.

Users may not disable this automatic logoff feature.

Procedure

1. An Active Directory Group Policy is in place that automatically locks user screens after 2 minutes of inactivity.
2. Users are trained to lock their desktop when walking away for any amount of time.

Enforcement

Any Upshur County personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

Computer, Network & Data Use Policy

Upshur County, TX

Your signature below indicates that you have read, understand, and agree with the Computer, Network & Data Use Policy

Signature: ____

Department: ____

Printed Name: ____

County Email: ____

Please note: A copy of this Computer, Network and Data Use Policy will also be emailed to you at the email above.

To be signed and kept on file at the Upshur County IT building