WAUPACA COUNTY INFORMATION TECHNOLOGY		
Issued: 1/3/12	**TECHNOLOGY USE POLICY**	Revised: 3/16/12; 5/9/2018

1.0 POLICY GOALS

1.1 The goal of this policy guide is to:

a. Support the mission of Waupaca County.
b. Protect confidential and proprietary information from unauthorized disclosure to third parties.
c. Prevent waste of Information Technology (IT) resources.
d. Reduce, and if possible eliminate, potential legal liability to employees and third parties.
e. Ensure the availability of IT resources to all County Departments.
f. Serve as a guide to Waupaca County employees and elected officials as to proper resource use; and to advise of consequences as a result of misuse.

1.2 This policy may be edited at any time. All edits will be approved by the Information Technology Committee. Users will be notified via email of changes after they are approved. The current policy will be posted at all times on the Waupaca County website: www.co.waupaca.wi.us.

1.3 This policy shall be utilized in conjunction with Waupaca County's Personnel and Procedures Manual, Section 7.07 Social Media. These policies are intended to be harmonized and reinforcing of one another.

2.0 ROLES AND RESPONSIBILITIES

2.1 Waupaca County

Waupaca County owns, manages and establishes policy for the security of all information and resources under its control.
To protect the integrity of the computer systems and to protect legitimate users from the effects of unauthorized or improper use of these technology resources, the County maintains the authority to do any or all of the following: to limit or restrict any employee's usage of the computing facilities; to inspect, copy, remove, or otherwise alter any data, file, or system resources that may undermine the proper use of that system; and any other steps deemed necessary to manage and protect the County's computer facilities. This authority may be exercised with or without notice to the employee; however, whenever possible, Information Technology personnel will consult with the department head or designee prior to taking action. The County disclaims responsibility for any loss or damage to data that results from its efforts to enforce these rules or from any changes, upgrades, or maintenance of the County Information Technology Resources.

2.2 Information Technology

Information Technology roles and responsibilities include, but are not limited to, the following:

a. Purchasing, maintaining, administering all Waupaca County business technology that work in conjunction with the County network, including mobile devices with the exception of smart phones, computers, laptops, e-mail, messaging systems, ShoreTel telephone system, servers, infrastructure components, security equipment, and so on.
b. Acting as the custodian of the County's information resources and implementing the policies and required training regarding information security, appropriate access and authorized use.
c. Acting on behalf of Waupaca County to secure information, applications, systems and networks; providing authorized access to approved personnel; and monitoring, detecting, investigating and reporting on actual or suspected security breaches or incidents.
d. Managing access to all Information Technology Resources, including network access.
e. Overseeing the destruction and/or recycling of resources in a safe and cost effective manner.

2.3 Departments

Department roles and responsibilities include, but are not limited to, the following:

a. Being the records custodian for all digital information in their areas, including stored documents and data archives. The Department Head or his/her designee shall determine access parameters, consistent with their policies and applicable laws. Department Heads are ultimately responsible for establishing clear guidance on data management and enforcing security policies. .
b. Determining application access roles and requirements and enforcing, monitoring, and managing them.
c. Ensuring that employees with access to Protected Health Information (PHI and ePHI), to confidential and proprietary information receive appropriate required training before authorizing access to this information.
d. Monitoring all Information Technology Resource usage by their employees to ensure it complies with all applicable laws and policies. To assist in this responsibility, departments may request reports detailing Internet and phone usage system reports that are maintained by Information Technology. Smart phone use and access is not monitored by Information Technology.
e. Creating policies for the permitted uses of removable media (for example, CDs or USBs) and monitoring employees for compliance.
f. Training interns, volunteers, contractors, and other business partners on the appropriate security and technology use policies.
g. Being compliant with records retention requirements in accordance with Wisconsin Public Records Law and other applicable state and federal laws.

2.4 Employees

All employees who are provided with access to Waupaca County electronic information are responsible for proper use of technology resources. Employees are responsible for:

a. Password protection and maintenance;
b. Critical data storage on secure network drives (M:\users, N:\department shares) and not on the local drive (C:);
c. Understanding and complying with all Federal and State laws and regulations and County and Department policies and procedures as they apply to information technology use, data security, and use of protected health information (PHI or ePHI) or other private information (PI);
d. Utilizing appropriate workstation physical security solutions;
e. Identifying and reporting technology use and/or security related problems and issues;
f. Utilizing appropriate destruction methods for obsolete removable media.

Each responsibility is more fully described in subsequent sections.

3.0 GENERAL PROVISIONS

This section outlines general provisions regarding information technology use that apply to all types of Information Technology Resources. Additional provisions relating to specific types of Information Technology Resources may be found in other sections of this policy.

3.1 Business Use Only

The County's Information Technology Resources are designed for County business use only.

3.2 Personal Use of Information Technology Resources

The County recognizes that an employee may occasionally use Information Technology Resources for personal use. All such use must occur outside of the employee's normal work hours, must not interfere with the use of equipment for County purposes and must not promote activities for political purposes or financial gain. All such activity must not contain virus, spyware, malware or related risks.

3.3 Acceptable Use of Information Technology Resources

Acceptable use is lawful, ethical, reflects honesty and shows restraint and good judgment. The primary purpose for using the County's information technology resources is to perform the governmental functions of the County, including but not limited to:

a. Communicating with and providing service to clients and members of the public.
b. Conducting the business of the County Department.
c. Communicating with other employees for work-related purposes.
d. Gathering information relevant to job duties or to expand skills and expertise.

3.4 Inappropriate Use of Information Technology Resources

Employees are prohibited from engaging in the following activities, with the exception of those activities required in the fulfillment of an individual's job responsibilities, for which s/he has received prior approval from a direct supervisor:

a. Accessing resources or altering data without explicit management authorization.
b. Engaging in illegal activity as defined by State and Federal law and local ordinance.
c. Using the Internet for gambling or gaming or engaging in commercial activity.
d. Promoting personal, political, religious or private causes, positions or activities, or working on behalf of organizations that have no professional or business affiliation with Waupaca County.
e. Transmitting, creating, viewing, installing, downloading, and/or copying of threatening, abusive, obscene, lewd, profane or harassing material.
f. Transmitting or viewing materials with intent to demean any person's age, disability, gender, race, national origin or sexual orientation.
g. Viewing, reading or accessing any sexually explicit sites or materials that are in any way sexually revealing, sexually suggestive, sexually demeaning or pornographic.
h. Intentionally preventing or attempting to prevent the disclosure of your identity with the intent to frighten, intimidate, threaten, abuse or harass another person.
i. Unauthorized or improper transmittal of material that is confidential to the County, or is otherwise protected by law.
j. Intentionally introducing a computer virus.
k. Interception or alteration of network packets or disabling or interfering with the County network or county-installed software.
l. Attempt to evade, disable, or bypass any security provisions of systems on the network, including use of another's USER ID or Password.
m. Allowing non-authorized individuals to access or use Information Technology Resources.
n. Installation of hardware on resource without prior consent of Information Technology

Department.

o. Streaming media for listening to music, playing games, or watching videos or movies on the County network is prohibited unless for a job-related purpose. Employees may use the Waupaca County unsecure WiFi to stream **music only** during the employee's breaks or lunch or during work time with Supervisor approval as long as the music streaming does not take place on County owned technology equipment and does not impact or interfere with the business of Waupaca County. Streaming of video content over the unsecure WiFi is prohibited and includes sites like YouTube, Crackle, Dish Anywhere, and so on.

Inappropriate use as described above specifically includes an employee's use of the Internet on County Information Technology Resources and an employee's use of E-mail communications.

3.5 Ethics Conflicts
Information Technology Resources may not be used for purposes prohibited by the County Ethics Code, Code of Ordinances Chapter 2.

3.6 Authorization of Use
Employees are to be provided access to County Information Technology Resources only if authorized by the appropriate department head or designee. Employees should be granted the minimum level of access to networks, information, and technology required to perform their job responsibilities. All access that is not specifically permitted is denied.

3.7 County Access
The County reserves, and intends to exercise its right, as is reasonably necessary, to search, review, audit, monitor, intercept or access an employee's use of the Information Technology Resources provided to him/her.

3.8 Privacy
Employees should not have an expectation of privacy regarding the use of Information Technology Resources of any kind regardless of the assignment or creation of passwords and/or access codes.

3.9 Work Product
All work products created through the use of information technology resources are the property of Waupaca County. Any materials developed, composed, sent, or received, using County-provided Information Technology Resources are, and will, remain the property of the County.

3.10 Copyrighted Materials
Duplicating or distributing copyrighted material without the express written consent of the owner is against the law and is prohibited.

3.10 Federal, State, Local Laws and Regulations
Usage of Waupaca County Information Technology Resources shall not violate applicable federal, state, and local laws and regulations.

3.11 Electronic Documents as Public Record
All electronic documents, including E-mail, may be considered a public record, and as such, may be open to public inspection upon request.

3.12 Administration and Enforcement of this Policy

Administration and enforcement of the provisions contained herein shall be the responsibility of the employee's immediate supervisor and, in turn, the Department Head. The guidelines regarding information security and technology use shall be considered work rules and enforced accordingly by Department Heads. Department Heads will promptly notify IT that any identified non-compliance with this policy has been corrected.

4.0 E-MAIL USE

The following items apply specifically to the use of E-Mail on Waupaca County systems:

4.1 Security and Confidentiality

a. E-Mail is not a secured media, except inside the County's E-Mail system. Any E-Mail that can be sent out of the County's E-Mail system to locations outside of Waupaca County should be considered non-secure.
b. E-Mail can be manually encrypted by the employee by typing ZIXSECURE (all one word) in the subject line. Encryption is the best practice in keeping content of E-Mail from being intercepted by third parties.
c. E-Mail is subject to applicable privacy, security, and records retention laws and guidelines for the information that a particular message contains. As such, E-Mail records must be appropriately secured and retained.
d. No employee should E-Mail sensitive, personal or private information, unless it is authorized and sent by approved methods.

4.2 Network Safety

a. Employees should not open unusual looking or unexpected E-Mail or click on links embedded within an E-mail that is unknown to the employee. E-Mail is often used by others for illegal purposes and may contain computer viruses.
b. County E-mail account addresses should not be used as contact addresses for solicitations, chat rooms, blogs or subscriptions not related to County business.
c. If an employee has any doubt about the authenticity of an E-Mail, or about what the E-Mail is requesting, the employee should notify their supervisor immediately, contact the sender to make sure the E-mail was sent with a legitimate purpose, and not open any attachments or click on website links contained in the E-mail until contact is made with the suspected sender.

4.3 Storage

a. Large attachments (over 3Mb) should be saved to another storage media and deleted from the email system.
b. Large attachments, such as newsletters, should not be sent to multiple user groups via the County E-mail system. A link to the county website where the information may be found is the best practice for information sharing.

4.4 Privacy and Ownership

a. Employees should have no expectation of privacy for E-mails sent or received through the County's network.
b. If an employee accesses an outside E-mail or text messaging account through county technology resources, the content of the information transmitted across the network is the property of the County regardless of the time of day the access is performed or if the device is remote (ex.: County laptop but using an outside network to access the information).

5.0 PASSWORDS

Computer passwords should be of sufficient strength so as not to be easily cracked or broken by unauthorized individuals, and to ensure the safety of the information and networks within Waupaca County. The Information Technology Department will establish and communicate specific requirements for password content.

5.1 The following items apply specifically to password use:
a. Each user should have his/her own unique login account.
b. Passwords should not be written down and stored on or near computer equipment.
c. Passwords should never be stored in clear view.

5.2 Under no circumstances shall employees share, or be required to share, login credentials, normally defined as the combination of both the employee's user ID and password. In the event that the Information Technology Department needs an employee's password, the Department will assist the employee in changing to a new password after the required service is completed.

6.0 PHYSICAL SECURITY

Employees are responsible for maintaining the physical security of their desktop workstations, portable computing devices, and removable media and paper documents by restricting and controlling physical access to these items. This can be accomplished by utilizing one or more of the following physical security solutions:

6.1 Monitors should generally be kept from the plain view of anyone who does not have the appropriate security access or clearance to information that may be displayed. Make sure that monitors cannot be viewed through outside windows, from public hallways, from public reception areas, or by reflection off of other objects. Utilize a special shade or polarizing monitor filter, when necessary.

6.2 Printers should be kept in protected areas to keep sensitive information from being disclosed inappropriately. Printed materials from any source should be kept secure, away from viewing, and out of public reach.

6.3 Best practice is the use of an automatic screensaver that is password protected and which activates after a set period of inactivity.

6.4 Removable media will have the same security requirements as the highest sensitivity of information on that device, and should be stored, secured, and destroyed as such.

7.0 SECURITY AND CONFIDENTIALITY OF ELECTRONIC PRIVATE INFORMATION

Employees are required to comply with state and federal laws and regulations, and County and Department procedures and policies regarding the use and security of electronic protected health information (ePHI), and proprietary, sensitive, personal, or confidential information, all of which is herein after referred to as Private Information (PI). Failure to comply will result in discipline up to and including termination of employment. In addition, the employee may be subject to civil and/or criminal penalties.

Each Department Head or his/her designee is responsible for permitting authorizations to ePHI and PI to identified individual employee use in the performance of her/his job duties. Each Department Head or her/his designee shall train all employees under her/his supervision regarding acceptable use and disclosure of this type of electronic private information.

7.1 HIPAA Security Policies and Procedures

Employees who have access to electronic protected health information (ePHI) have the responsibility to follow all documented HIPAA security and privacy practices, procedures, and policies provided by Waupaca County. Employees must keep desktop computers, and all portable computers, physically secure and prevent them from being accessed by unauthorized users. Employees must keep ePHI data from being read by or distributed to unauthorized users. Failure to comply with all HIPAA requirements will also result in an employee being subject to employee discipline, up to and including termination. In addition, the employee may be subject to civil and/or criminal penalties.

7.2 Security of Private Information (PI) and Confidential Information

Waupaca County is responsible for providing employees with the means to keep PI and confidential information secure.

Employees shall keep this information safe, private, and unavailable to employees and non-employees who have no business need to access it. This may be accomplished by:

a. Utilizing all appropriate workstation physical security as described above.
b. Logging out or locking the workstation before leaving the computer unattended.
c. By applying all Waupaca County PI, security and privacy policies and practices learned through training.
d. By logging off and powering down all computer workstations at the end of each workday.
e. Printed materials should be kept secure in transit and at rest and locked up when the office space is vacant.

7.3 Destruction of Obsolete Removable Media Containing PI

Subject to applicable record retention laws and schedules, employees will use the removable media destruction and elimination devices and processes made available by Waupaca County Information Technology to destroy all obsolete removable media containing PI or other information requiring protection.

7.4 Security of Criminal Justice Information Systems (CJIS)

Users that come in contact with Criminal Justice Information are required to abide by any CJIS policies and procedures, including state and federal regulations and Department policies.

8.0 NETWORK COMPUTER HARDWARE / SOFTWARE USE

8.1 Attachment of Equipment or Other Devices

Prior approval from IT must be obtained before any equipment is attached to the County network or to a County computer.

Information Technology may, upon request and demonstrated need, permit, enable, and support remote network access for job-related purposes. See further detail in Section 9 below.

8.2 Alterations of Computer Hardware

County-owned technology equipment must not be altered in any way for any purpose.

8.3 Unauthorized Software

Use of unauthorized software may degrade the performance of the County's systems, create security risks, reduce employee productivity, and expose the County to copyright liability.

a. Users are prohibited from installing any applications, plug ins, and so on, on their County workstation without prior approval from IT.

b. IT will immediately remove any unauthorized software in use, when encountered, unless the software has a legitimate business purpose for the user, is appropriately licensed, and approved by the user's supervisor. IT will work with the Department Head or her/his designee to address any legitimate business need prior to removal.
c. Use of all software must be in compliance with the manufacturer's license agreement and cannot be copied to multiple computers unless permitted by the license agreement.

8.4 Compliance with Software Copyright Laws

Use of computer software is subject to Federal copyright laws. Copying and using software without explicit permission from the copyright owner constitutes copyright infringement. Employees who willfully and knowingly infringe a software copyright by making, acquiring, installing, downloading, or using unauthorized copies of computer software will be subject to discipline up to and including termination of employment. In addition, the employee may be subject to civil and/or criminal penalties.

8.5 Use of State-Provided Computers and Software

Employees who are assigned to use a State-provided PC or who utilize software provided by the State are required to comply with all provisions of this policy in addition to any technology, internet or e-mail use policy implemented by the State. Misuse of the technology provided by the State may result in discipline up to and including termination of employment. In addition, the employee may be subject to civil and/or criminal penalties.

8.6 Disposal of Obsolete Hardware and Software

Information Technology is solely responsible for the proper disposal of all County-owned software and hardware. Departments should contact the Information Technology Department for proper disposal.

9.0 MOBILE DEVICES

9.1 Definition: A mobile device is any device used to access County's information technology resources from outside of the County's secure facilities or via any network connection other than County's private, secure network facilities.

9.2 Approval

a. Mobile access to the County's information technology system must be reviewed and approved by Information Technology for a legitimate business need and upon recommendation of the appropriate Department Head.
b. Information Technology will have final say on which device is purchased and what software will go onto that device.
c. Only Information Technology Department approved devices will connect directly to the County network.

9.3 Appropriate Use of County-owned Devices

a. The appropriate use and inappropriate use policies discussed above also apply to mobile devices.
b. Personal use of county-owned devices is discouraged. Occasional personal use is acceptable provided no additional costs are incurred by the County, use is authorized by Department Head, and use does not violate the terms of this or other related County policies, and the personal use does not lead to the introduction of virus, spyware, malware type infections.
c. Mobile devices should not be used while driving or operating equipment.

9.4 Security

a. Mobile devices must be properly secured at all times to prevent theft, loss and/or unauthorized access.
b. Passwords and applicable security safeguards must be utilized.
c. Avoid any use which may compromise device security.

9.5 Work-related Use of Employee-Owned Devices

a. A personal mobile device used for County government business may subject the entire device to Wisconsin's Public Records Law. Any information stored on the device is subject to review by the County or other government officials in response to a public records request and for the purpose of completing an investigation.
b. If a personal mobile device is approved by IT and the user's Department Head for use for work-related purposes, the County reserves the right to install software for security and support a remote wipe of the device whenever necessary to ensure the safety of the County's IT system; track device use and location; remotely lock out access; and compel production of the device for public records requests or other legal obligations related to information accessed by or stored to the device.
c. If a personal mobile device is used for work-related purposes, the County will not be responsible for damage or malfunction; additional provider services charges or costs incurred by work-related activities; loss of information stored on the device; and support or repair of the device.

9.6 Loss or Theft of Mobile Device

a. Loss or Theft of any mobile device (county-owned or personal) used to access the County's information technology resources must be reported immediately to Information Technology.
b. Upon notice of loss or theft, IT will remotely lock the device, attempt to determine the location of the device, work with the owner to locate the device, and issue the command to remotely wipe the device if it cannot be located.

10.0 TELEPHONE USE

10.1 Information Technology is responsible for the maintenance, software and equipment related to the Shoretel landline phone system.

10.2 Use of county-owned smartphones will be in accordance with individual Department policies.

10.3 Any smartphone used by a County employee to conduct government business will subject all data contained on the device and data collected by the service provider about the device subject to Wisconsin's public records law.

11.0 INCIDENT REPORTING

Employees have a responsibility to report any actual or suspected information or network security incidents to the appropriate responsible party. There will be no discipline or adverse action for the good-faith reporting of security issues, problems, or incidents. Sanctions as outlined in the HIPAA Sanctions Policy will not apply to disclosures by employees who are whistleblowers or crime victims.

11.1 Types of Incidents Which Should Be Reported:

The following types of incidents are examples of situations that should be reported as a possible security incident:

a. Unauthorized release of information in an E-Mail, whether intentional or accidental.
b. Unauthorized receipt of any E-Mail containing information that is protected from disclosure (such as health care information).
c. Receipt of E-Mail that looks to be illegal or contains sexually explicit, hate-group related, or otherwise illegal material.
d. Suspicion that your password has been disclosed or that someone may have been using one of your login credentials or accounts.
e. Receipt of any E-Mail that triggers anti-virus software.
f. Any individual who asks you for your password, or to use your account to review the contents of your E-Mail.
g. Computer attacks coming from outside the County, or any suspected virus, worm, or other malicious code.
h. Theft or unauthorized removal of media, data, storage devices, disks, CDs or USBs.
i. Unauthorized access to the County's computer system(s) by a third party.
j. Inappropriate use of the County's Information Technology Resources. Examples include, but are not limited to, access of inappropriate websites; using County systems for inappropriate, non-work related materials; abusing County systems or using them for unintended purposes; using workstations, servers, or other devices to attempt to monitor, detect passwords, probe systems or networks, or other such hacking/cracking activities.

11.2 Incident Reporting Procedures and Response

Employees must report incidents to either her/his Department Head or to the Information Technology Department. Information Technology will investigate all reported incidents. If the report alleges misuse or improper disclosure of ePHI, PHI and/or Private Information, Human Resources will participate in the investigation.

11.3 Sanctions

At the conclusion of an incident investigation, the Information Technology Director will provide written documentation of the incident, his/her conclusion regarding the allegations, and provide information regarding the severity of the incident, the degree of non-compliance with this policy, and the effect on County business operations. The Information Technology Director will provide the report to Human Resources and cooperate in any disciplinary actions taken regarding the incident.

11.4 Waupaca County Compliance Guide for HIPAA Sanctions can be found on Waupaca County's website: www.co.waupaca.wi.us.