

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY TABLE OF CONTENTS	Section 900

900	Information Security Policy
.5	Scope
.10	Roles and Responsibilities
.15	Access to Computers, Networks, and Systems
.20	Access Establishment Details
.21	Specialized Account Policies
.25	Emergency Access Establishment
.30	Specific Security Policy Requirements
905	Information Security Governance
.5	Scope
.10	Security-Related Policies and Procedures
.15	Information Security Council
.20	Coordinating Instructions
907	Information Technology Suite Security
.5	Office Suite Access
910	Application Development Security
.5	Scope
.10	Application Development Security Policy Summary
.15	Application Development Security Procedures
915	Data Backup and Storage
.5	Scope
.10	Data Backup Storage Practices
920	Data Center Access and Maintenance
.5	Scope
.10	Data Center Access and Maintenance Practices
.15	Unaccompanied 24 x 7 Access
.20	Unaccompanied Normal Working Hours Access
.25	Accompanied Access
.30	No Access
.35	Emergency Access Procedures
.40	Maintenance Recordkeeping
925	Incident Response and Reporting
.5	Scope
.10	Description and Definitions of Incidents
.15	Incident Response and Reporting Procedures Framework
.20	Incident Response and Reporting Procedures
930	Media Handling Policy
.5	Scope
.10	Server Policies and Principles
.15	Workstation-Specific Policies and Principles
935	Network Device Installation and Configuration Policy
.5	Scope
.10	Network Device Installation and Configuration

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY TABLE OF CONTENTS	Section 900

940	Remote Access
.5	Scope
.10	Remote Access Practices
945	E-Mail
.5	Scope
.10	Specific E-Mail Policy Guidelines
.15	Incident Response and Reporting
950	Passwords
.5	Scope
.10	Password Policy Procedures
.15	Technical Implementation
955	Internet and Web Access
.5	Scope
.10	Internet / Web Access Practices
960	Workstation Security
.5	Scope
.10	Workstation Security Practices
.15	Inventory Management
962	Portable/Removable Device Security
.5	Scope
.10	Portable/Removable Device Security Practices

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 900 – GENERAL INFORMATION SECURITY	Section 900

900 Information Security Policy

This document provides policy, direction, procedures, and guidance to ensure the security, confidentiality, integrity, and availability of electronic information and the automated systems that contain it.

Waukesha County shall provide only that access to computers, systems, and information that is required for that individual or agency to perform required tasks and duties. This policy includes both login access to computers, networks and servers, as well as physical access to workstations, systems, wiring closets, and data centers.

The overarching policy for information security is that everything that is not specifically permitted shall be denied. Access is granted or approved by the owner of the system or information, provided by employees of the Information Technology Division, and utilized by the employee or end-user for business purposes. Only authorized personnel are allowed to facilitate or provide access to systems. These include authorized employees of the Information Technology Division of DOA, or departmental employees who are authorized to create and administer application-level user IDs and passwords.

900.5 Scope

This policy applies to all automated resources, computers/computer systems, networks, hardware, software; and all information, data, applications, functions, files and resources located on Waukesha County networks, or within Waukesha County buildings. This policy applies to all County employees, elected officials, County Board and Commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

Anyone using the computing resources of or accessing information from or through Waukesha County systems or networks is required to abide by these procedures and guidelines. Failure to abide by the provisions of this document may result in disciplinary action up to and including termination of employment. Those not complying with these guidelines may also be subject to criminal prosecution or be held financially liable for damage to equipment, denial of needed resources, loss of data or harm or damage to an individual or entity caused by their action.

900.10 Roles and Responsibilities

- A. Waukesha County Government Waukesha County is the organizational entity that owns, secures and establishes policy for the security of all information, resources and facilities under its control, as well as for contractors, tenant organizations, and business partners. Policies may be based on a combination of law, administrative policy and commonly accepted business practices; and will be determined based on the best interests of Waukesha County Government and its constituents.
- B. Department/Division Heads Department/Division Heads are responsible for all electronic information in their areas, as well as all stored documents, and data archives. As such, they determine who will be allowed to access their information, consistent with their policies, and applicable laws and regulations. The Department/Division Head may delegate this authority to one other person in his or her organization, such as an Information Systems Coordinator, who may act or sign on his or her behalf. The final responsibility for establishing clear guidance for their data, and enforcing security policy lies with the Department/Division Head.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 900 – GENERAL INFORMATION SECURITY	Section 900

- C. Information Technology Division Information Technology Division houses, administers, and operates all servers, infrastructure and security equipment for Waukesha County agencies, unless special exceptions are granted. The I.T. Division is the custodian of the County's information resources and implements the policies set forth in this document. The Information Technology Division acts on behalf of Waukesha County Government, and Department/Division Heads to secure information, applications, systems and networks, to provide authorized access to approved personnel, and to monitor, detect, investigate and report on actual or suspected security breaches or incidents.
- D. End-Users/Employees Employees of Waukesha County, and others accessing County information or computer services, play a key role in maintaining the integrity and security of all of our automated systems. Each user of automated services is responsible to understand these rules and guidelines, to abide by them, as well as to identify and report issues and problems. Departments and employees are responsible for training interns, contractors, volunteers, etc. on the Security policies of the County.
- E. Affiliated Agencies These are departments or agencies who are members of or occupying space within the Waukesha County Government Campus area, but whose networking and/or computer support comes from an external entity. Examples of this are the Courts and District Attorney. Individuals in this category shall abide by these policies when utilizing county resources and networks, and should be familiar with and comply with the requirements of their networks when using those.
- F. Information Security Council This is an organization comprised of a member of the County Executive's Office, the Waukesha County Security Officer, the County Risk Manager, a representative of the Corporation Counsel, and invited Departmental representatives. The council will remain current on risks, threats and security issues and make recommendations to the County Executive on policies, actions, expenditures and strategies, which will mitigate or address those risks.
- G. Information Security Officer The Security Officer is responsible to oversee all aspects of the Information Security compliance effort. This includes creating and recommending policies, coordinating and leading security efforts, establishing training baselines, investigating issues and incidents, and continuously training on security and compliance related issues.
- H. Information Security Coordinator Each department will designate one individual to be their Security Coordinator. He or she will be appointed in writing and identified to the County Security Officer. This individual will be responsible for disseminating policy and guidance, providing or coordinating training, supporting the County Security Officer in monitoring and achieving compliance, notifying the Security Officer of actual or suspected incidents, and other duties as assigned.

900.15 Access to Computers, Networks, and Systems

Access to Waukesha County networks and systems is provided for the official use of Waukesha County employees, volunteers, contractors, affiliated government agencies and citizens. Access to County networks or systems is a privilege, not a right. Access can be suspended or removed for failing to comply with the provisions of this document. Some data or information that we process and store is protected by law. As such, in addition to administrative or disciplinary action, there may be legal, criminal or monetary penalties associated with non-compliance with this document or applicable laws and policies. Laws also provide stiff penalties for actual or attempted intrusion, destruction or defacement of information. These events, commonly known as hacking or cracking, carry fines and/or imprisonment.

Waukesha County Government hosts a considerable amount of data and information, and takes security very seriously. Access to information is a public trust and is to be protected with all prudence and diligence. The information systems we utilize are mission-critical devices that we depend on to conduct the business of the County and to support our citizens and residents

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 900 – GENERAL INFORMATION SECURITY	Section 900

as well as other governmental agencies. Good security policies and good policy enforcement are one way to ensure the highest possible availability of those resources and to prevent the accidental or intentional disclosure of information or damage to systems.

900.20 **Access Establishment Details**

- A. Access to systems is established through the use of the Login Request Form, which is posted on the Intranet. Special consideration should be given to ensure that each manager or supervisor is following the least privilege rule – that an individual should be given only that access required to perform his or her assigned tasks and responsibilities.
- B. Each user should have his or her own unique login account. That information is used for monitoring, determining acceptable use and securing our systems.
- C. To the extent possible, role-based access shall be used to provide consistent, least-privileges access to applications and systems. Departments shall be responsible for determining application access roles and requirements, and enforcing, monitoring, and managing them.
- D. Under no circumstances shall employees share, or be required to share login credentials, normally defined as the combination of both their user ID and password.
- E. If access to others' data is required, it shall be granted either by the use of a proxy function in the case of electronic mail, or by requesting access through the I.T. Division. Each department shall create internal controls for approval of such a request, such that the Information Technology staff is receiving requests from authorized individuals within departments. Unless otherwise specified, this will be considered to be the Department Head, or the I.S. Coordinator within that organization.
- F. Special consideration should be given when providing access to information that may be protected by rule or law.
- G. The Login Request form requires special training be provided for people accessing electronic Protected Health Information (ePHI). Care should be taken to ensure that managers and supervisors properly check and train employees prior to authorizing access to protected information.
- H. A review of all user IDs takes place at least annually through the IT Division. All system accounts will be reviewed for currency and applicability. Individuals, who have moved, departed or no longer require access will be removed from the system, or have their accounts appropriately modified.
- I. Contractors and support personnel may be issued IDs on County systems; however special care must be taken to be sure they are closely monitored, have access to only the systems that are required to support, and provided training and a copy of this security policy to read and review.
- J. Contractors and other non-County personnel will have an end-date established on the login request form. This date will be the expected ending date of the work or 365 days from the creation of the ID, whichever is less. If work ends earlier than anticipated or a contractor is released, the requesting department is responsible to ensure that the user ID is deactivated and removed from the system.
- K. Departments are required to inform I.T. of any changes in employee status which could impact on access levels. This includes, but is not limited to retirements and terminations, transfer, any personnel investigations or actions which may modify a particular user's access.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 900 – GENERAL INFORMATION SECURITY	Section 900

900.21 **Specialized Account Policies**

There are unique requirements governing the use of specialized accounts within County automated systems. Specialized accounts are those accounts, which are required for the proper functioning of systems, utilities or applications, **and** which have rights which exceed those of a standard user account. This definition includes, but is not limited to such account types as Administrator, Admin-equivalent, root, SA accounts, service accounts and super-users. While these account types are known by various names and aliases, the concept of higher-than-normal access is the distinguishing factor.

Such accounts provide extraordinarily high levels of access to varieties of systems. Used correctly, such access is vital to the correct operation of our applications and systems. At the same time, such accounts also add significant vulnerabilities and risk to the organization. They must be carefully configured, managed and administered to effectively balance both risk and benefit. The following policies will be strictly adhered to:

- A. Specialized accounts will be approved only when absolutely necessary, and the number of them will be kept to a minimum. They will only be provided to meet certain specific business needs or application requirements, and not because of being assigned to a particular organization or position.
- B. The only approval authorities for such accounts are the Infrastructure Administrator or his designated representative for systems, service or utility accounts, the Solutions Administrator for selected application and database accounts, and the proponent department application manager for application-specific access.
- C. Individuals having such access are prohibited from modifying other accounts to add access or from creating additional specialized accounts, unless such permission has been granted.
- D. Administrator-level accounts are to be used only for system or application administration. Personnel will not remain logged in under these accounts, or perform normal day-to-day functions with administrator-level accounts. Access should be temporary and designed to perform a specific function. When complete, the user should log out, and log back in with their normal county user ID. Under no circumstances should employees leave their desks while logged in with a specialized account. These will be logged off and workstations turned off after normal work hours.
- E. Generic accounts will not be used.
- F. A service account is a specific type of specialized access account. It is designed as an account which is specifically used to run applications or services on a host machine. Users should never log in through a service account to perform maintenance of any kind.
- G. Applications, scheduled tasks and services should never run under a named user account – standard or specialized. This will cause the application or service not to function when normal maintenance is performed or passwords are changed.
- H. Password Policies. If a service account is created, and not logged into, the password must be changed every 24 months. If a specialized account is or has ever been used for login, the password will be changed every 90 days, per our normal policy for all user IDs. Password complexity will be enforced.
- I. Credentials must never be shared.
- J. Extra care must be taken to secure and monitor access when contractors require specialized accounts. Contractors will provide background check information, and the county employee they are working with will closely monitor them. All contractor accounts require an expiration date 60 days from the date created. Extensions will be authorized based on business need, and each request will add a maximum of 60 days to the expiration date.
- K. Specialized access accounts will be suspended when not be used.
- L. Any exception to this rule must be approved in advance; and documented and justified.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 900 – GENERAL INFORMATION SECURITY	Section 900

900.25 Emergency Access Establishment

There are times when emergency access may be required, such as when a portion of a building becomes uninhabitable, or an entire section of a network becomes segregated from the County backbone. If that occurs, the following actions will be taken.

- A. The department will determine the extent of the problem or outage. The Help Desk will be notified.
- B. If immediate access is required, as in the case of emergency access to health information, or other mission-critical information, the department will attempt to locate habitable buildings or functional networks/systems, within its buildings and facilities. Critical operations will be transferred to functional facilities, as required.
- C. Departments will communicate any requirements for equipment and networking at alternate sites, by the fastest appropriate means to the Information Technology Division.
- D. If emergency operations require immediate access to systems, and if all areas within a department are inaccessible or non-functional, the department will call Information Technology at 262.548.7610, and page the Infrastructure Administrator or I.T. Division Manager. [After hours the Help Desk will page the I.T. Manager.] The I.T. Division will either provide a location to access systems (like a classroom or office area), or in the case of emergency, will escort an employee from the affected department into the data center to access needed information. This will be a temporary measure to meet legal and public safety obligations, and is only necessary when the core system is operational, and the data center is unaffected.
- E. If emergency access from an alternate location is required, the business continuity plan will be invoked if the outage goes beyond 4 hours.

Specific provisions of the County's policy on the acceptable use of technology are covered in Chapter 2, Section 700 – Information Technology Use Policy of the Waukesha County Administrative Policy & Procedure Manual. Implementation policies for various technological areas are appended to, and are a part of this Security Policy.

900.30 Specific Security Policy Requirements

In addition to all of the above listed provisions, the following sections are considered to be an integral part of the Waukesha County Security Policy:

- 905 - Security Policy Governance
- 910 - Application Development Security
- 915 - Data Backup and Storage
- 920 - Data Center Access and Maintenance
- 925 - Incident Response and Reporting
- 930 - Media Handling
- 935 - Network Device and Installation and Configuration
- 940 - Remote Access
- 945 - E-Mail
- 950 - Passwords
- 955 - Internet and Web Access
- 960 - Workstation Security
- 962 - Portable/Removable Device Security

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 905 – INFORMATION SECURITY GOVERNANCE	Section 900

905 Information Security Governance

This document describes the security governance and policy formation process within Waukesha County Government.

Information security is not the sole function of any department, group, or agency. Rather it is the result of the combined efforts of leadership to provide guidance and state intent, the Information Security Council to create policies and forward them for review and approval, a technical staff to implement the technical structures that support the policies, departmental directors, managers and supervisors to train, implement, and ensure compliance with the policies, and the human resources support necessary to provide enforcement and sanctions when policies are broken.

905.5 Scope

This policy applies to all automated resources, computers/computer systems, networks, hardware, software; and all information, data, applications, functions, files and resources located on Waukesha County networks, or within Waukesha County buildings. This policy applies to all County employees, elected officials, County Board and Commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

905.10 Security-Related Polices and Procedures

Policies are the heart of any compliance program. They form the baseline of organizational will and intent, as it pertains to Information Security. The County's security policies will be created by the Information Security Council, and approved by the County Executive's Office or his designated representative. Policies will be reviewed at least annually, or as often as may be required to respond to changes in laws, technology or other requirements.

905.15 Information Security Council

The Information Security Council:

- A. Will be comprised of the following permanent members: Security Officer, Risk Manager, Corporation Counsel representative, County Chief of Staff.
- B. Will be comprised of the following adjunct or advisory members: Director of Administration, Information Technology Manager.
- C. Will be comprised of the following invited members: No more than 4 Department Heads or their designated representatives, as invited by the permanent members.
- D. Will be chaired by the Information Security Officer who will prepare agenda items to support creation or modification of policy, training and information on recent threats and vulnerabilities, technical or programmatic initiatives to support and advance security at the County, other matters that may require the Council's attention or action.
- E. Will have meetings on a quarterly basis, or more often as needs arise.
- F. Will create and provide draft policies for approval to appropriate authorities within the County.
- G. Will receive guidance from County Leadership for security in general, and for specific areas of concern in the area of information security.
- H. Will recommend procedures for enforcement, training, investigations, monitoring, compliance, and any other areas that would provide benefit to County Leadership in the area of Information Security.
- I. Will act in a consultative or advisory capacity to County Leadership in all areas pertaining to Information Security.
- J. Will act as an advisory organization and information resource in the area of security to County departments

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 905 – INFORMATION SECURITY GOVERNANCE	Section 900

905.20 Coordinating Instructions

- A. The permanent members of the Council will determine a slate of departments to include as invited members. The sheer number of Departments make it impossible to include everyone. Participation will be based on willingness to participate, size of agency, applicability of subject material to their mission, and the ability to contribute to the mission of the Council.
- B. The Council itself is not an enforcement agency. It is advisory in nature.
- C. The Information Security Officer will set up room arrangements, collect agenda items, and make meeting notifications to participants.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 907 – INFORMATION TECHNOLOGY SUITE SECURITY	Section 900

907 **Information Technology Suite Security**

This document describes the security policies governing access to the I.T. Office area.

Information Technology Division of the Department of Administration is a centralized IT facility located on the Waukesha County campus. Because of the scope of services provided, and the amount and type of information stored on County systems, the IT Offices are considered a secure area, which is generally closed to county employees, citizens and visitors alike. Those who do require access will be provided an appropriate badge or escorted at all time.

907.5 **Office/Suite Access**

Employees and contractors, requiring consistent and continuous access, and anyone else authorized by the IT Manager will be provided access by the issuance of a badge. The doors and exits, as well as the access hours will be authorized based on business need only. Such badges will be issued to the authorized individual, and remain in his or her position during the period of employment or need. There are no generic badges which will allow access to doors and exits. The badge remains the property of Waukesha County, and will be reported immediately if lost or stolen. This badge will be surrendered at termination, retirement, completion of work or consulting engagement or at the request of the IT Manager.

Visitors will sign into the visitors log and will be issued a visitors badge. This badge will be worn in plain view, and surrendered when the individual departs. Visitors will be escorted while in the office suite area. Visitor's badges will never allow for automated access to interior doors or building entrances/exits.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 910 – APPLICATION DEVELOPMENT/PROCUREMENT SECURITY	Section 900

910 Application Development/Procurement Security

The purpose of this document is to provide guidance to ensure that the development, configuration, and deployment of applications incorporates the best practices of information security and provides for the confidentiality, integrity, and availability of applications and information.

910.5 Scope

This policy applies to all applications in use at the County, accessed by the County, or containing County information.

910.10 Application Development/Procurement Security Policy Summary

Every application development or procurement effort shall include the goal of ensuring that information is appropriately protected, as well as the server resources on which the application will run. Additionally, each developer and analyst should become familiar with basic principles of secure application development in order to act as subject matter experts to selection boards and project groups.

910.15 Application Development/Procurement Security Procedures

- a. Security shall be considered throughout all phases of an application's lifecycle – from consideration/inception all the way through decommissioning and disposal.
- b. For in-house developed systems, the Solutions Administrator shall create a security profile which protects the information and the hardware resources.
- c. In addition to securing the information in the application, a system shall also protect the host operating system and hardware from attacks such as Trojan horses or buffer overflow.
- d. Vendors shall be asked to certify their systems' security during every bid or procurement action, and prior to the implementation of software enhancements, patches or fixes.
- e. Development/procurement activities shall conform to guidelines published by OWASP (Open Web Application Security Project), NIST (National Institute for Standards and Technology, and other pertinent standards documents.
- f. Special care shall be taken with financial systems, or systems housing particularly sensitive information which may be protected by law.
- g. Applications shall contain logging capability to provide appropriate controls for security compliance.
- h. Applications shall be tested for security before implementation.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 915 – DATA BACKUP AND STORAGE	Section 900

915 Data Backup and Storage

The purpose of this document is to establish policies and procedures for the consistent and correct backup of data in the County Data Centers. It is the policy of Waukesha County to perform systematic, and typically daily, backups of all data on our automated systems.

915.5 Scope

This policy applies to all systems housed within one of the designated County Data Centers and under the direct management of the Information Technology Division Staff. Systems that are owned and operated by departmental representatives, not housed in the Data Center, or not managed by our Information Technology staff will not be a part of this program.

915.10 Data Backup Storage Practices

- A. It shall be the mission of the Information Technology Division to maintain and operate the facilities and equipment necessary to do systematic, repetitive backups of all computer systems in the Data Center. These will generally be done on a daily basis, but the schedule may be modified to accommodate a more relaxed schedule for systems where data does not often change.
- B. Tape backups are intended for restoring accidentally deleted files and to recover servers from a business continuity event. **They are not designed as a record retention tool.** Tapes will not be stored beyond 12 months from their date created without written authorization of the IT Manager.
- C. Responsibility for the backup and restore functions lie with the Infrastructure Group of Information Technology Division. Backups will be scheduled and conducted on a daily basis. Restores are requested through the Help Desk, or may be scheduled in advance.
- D. As much as possible, a standardized backup architecture will be used within each technical family. Information Technology will prescribe how backups are to be conducted and the software and hardware, which will be required.
- E. Principal Administrators in each technology family are responsible to account for current, new, and retiring systems and adjust backups to meet the requirements of that particular system. Systems shall not be placed into production without backups being tested and certified
- F. Scheduled back up tape accountability and control:
 1. Tapes will enter and leave the data center in secured containers. Contents of the containers will be inventoried and boxes will be locked.
 2. All tape containers will be inventoried and signed for when custody is transferred.
 3. Tape containers will be transported by personnel from Records Management Division.
 4. Tapes will be rechecked just before closing and locking a box, and immediately upon opening a box. Any loss or variance will be reported to the manager immediately.
 5. Only County employees will handle tapes or tape containers. Background checks will be required for all those handling tape containers, and they will be a normal part of the pre-employment screening process for Information Technology staff.
 6. When outside the vault or Data Center, tape containers will not be left unattended.
 7. A verifiable chain of custody will be established with the handling and disposal of tapes. As a standard, we will know where they are, in whose custody, and shall be able to account for their whereabouts.
- G. Unscheduled or ad hoc backup tapes:
 1. Tapes may be created on an as needed basis to support project work. These tapes may be stored outside of the normal tape container, or in an employee's direct control or custody.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 915 – DATA BACKUP AND STORAGE	Section 900

2. When the tape is no longer needed, it shall be returned to the scratch tape pool, or destroyed appropriately.
- H. All tapes will be treated with the same level of security as the system that the information came from. Information, which is protected by law, regulation, privacy standards, policy or ordinance, will dictate how the tape is created, handled, secured and ultimately destroyed. In no case will a tape be handled with any less security than the information it contains. The entire tape shall have the classification of the highest sensitivity of information on any one of its files. Thus, if one file contains protected information, the entire tape requires that level of security.
- I. The authorized locations for tape and tape storage are:
1. Courthouse Data Center
 2. WCC Data Center
 3. Northview Data Center
 4. Waukesha County Records Management Storage Vault
- Tapes will be at these locations except while in transit, or when approved by a supervisor or manager.
- J. Tapes will not simply be thrown away. Tapes will be disposed of in accordance with the Media Disposal Policy.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 920 – DATA CENTER ACCESS & MAINTENANCE	Section 900

920 Data Center Access and Maintenance

The purpose of this document is to establish policies and procedures for providing access to the Waukesha County Data Centers

920.5 Scope

This policy applies to all County employees, elected officials, County Board and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers. Anyone accessing any of the County Data Centers shall be bound by this policy.

920.10 Data Center Access and Maintenance Practices

- A. It shall be the policy of Waukesha County Government that all Data Centers are secured, restricted areas. Access shall be granted to only those individuals who have a mission-essential business need and who have been appropriately cleared. County Data Centers contain information, which is sensitive, personal in nature, and in some cases, protected by law. Data Centers are not common workspaces. Traffic in the Data Centers shall be kept to a minimum.
- B. There shall be four categories of access under the provisions of this policy – Unaccompanied 24 X 7, Unaccompanied During Normal Work Hours, Accompanied Access Only, and No Access.
- C. In general, any access which is not specifically approved, is denied.
- D. Only the Manager of Information Technology Division and the Infrastructure Administrator have the authority to grant access. Badge requests requiring Data Center access will not be accepted from any other manager or employee.
- E. Unaccompanied badge access will be kept to the minimum required to perform mission-essential functions. It is not automatically granted as a part of being in a manager's position or a member of Information Technology. Any and all work possible will be done remotely from outside the Data Center.
- F. If an employee is allowed to provide access to those who require escort (Accompanied Access Only), that employee must remain in the room during their visit or stay, or place that person with another County employee having unaccompanied access authority. Employees providing access assume responsibility for the actions of those they allow into the Data Center and are responsible to clear them back out, ensuring that they have not removed items of equipment, media, or data.
- G. In general, badges to access the Data Center will not be provided to non-County employees. An exception to this rule is a badge that may be issued to a contractor for use during all or part of a day when supervised by a County employee.
- H. Badges are not transferable. It will be the manager or administrator's responsibility to retrieve and deactivate badges before an individual departs the organization.
- I. Badges must be secured by all employees. Employees are required to use only their personal badge, and have it secured at all times. Access is recorded, so a badge should not be shared with others. They will not be left lying on tabletops, under keyboards, or in unlocked drawers or cabinets.
- J. Actual or suspected loss of a badge will be reported immediately. Deactivation will occur at reporting time. At no time will a badge be left active while a search is taking place. Data Center badges generally also have access to outer doors, so it is critical to report suspected losses immediately.
- K. Special investigation requirements exist for unaccompanied off-hours access to the Courthouse and the WCC Data Center to comply with FBI and State Department of Justice requirements.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 920 – DATA CENTER ACCESS & MAINTENANCE	Section 900

- L. Evaluation of individuals having access will be continuous. If information is uncovered after access is approved, it may mean that access may be withdrawn depending on the circumstances.
- M. Our Data Center houses information which is covered under the provisions of the federal Health Insurance Portability and Accountability Act (HIPAA). The Information Technology Division of DOA is a Business Associate of the Hybrid Covered Entity of Waukesha County Government. Unaccompanied access shall require HIPAA training and the signing of the County Privacy Agreement.
- N. The Infrastructure Administrator will request reports, on a periodic basis, to review those who have accessed the Data Center. Facilities shall prepare these reports upon request or provide access to the Infrastructure Administrator.
- O. Special access rules will apply in case of emergency. They are described in paragraph 920.35 below.

920.15 Unaccompanied 24 X 7 Access

- A. This level of access will be granted to the least possible number of employees. Employees in this category should be full-time and have completed an advanced background check. The employee shall have exhibited a level of trust and confidence, which would justify this level of access.
- B. Access will be established by obtaining permission and filling out a badge access request form.
- C. Unaccompanied access authorization does not automatically grant permission for that individual to escort or admit others to the Data Center. A clear mission requirement will exist.
- D. Only Infrastructure technical staff is allowed to authorize the delivery or removal of equipment in or out of the Data Center. No items will be brought in or taken out without Infrastructure Administrator's knowledge and permission.
- E. Unaccompanied access implies consent to search the person or belongings if such a search is required to ensure the confidentiality, integrity, or availability of information or systems.
- F. By entering the Data Center, individuals accept responsibility to monitor activities and report things that may look wrong or out of place. It is everyone's responsibility to recognize those others who are in the room and to try to verify the identities of unrecognized individuals.
- G. Facilities personnel have badges and access codes for unaccompanied 24 X 7 access. This access should be used only in the case of a page, alarm or emergency. All such access should be reported to the Facilities Manager, who should log the information. Facilities personnel are not allowed to access County systems from within the data center. (For example, they may not check their Email from a workstation within the data center.)

920.20 Unaccompanied Normal Working Hours Access

- A. This level of access will be granted to provide unaccompanied badge access to the Data Center between the hours of 7:30 a.m. and 5:00 p.m., Monday through Friday, excluding County Holidays.
- B. This level of access will be granted to the least possible number of employees and contractors. Employees in this category should be full-time and have completed an advanced background check. The employee shall have exhibited a level of trust and confidence, which would justify this level of access.
- C. Access will be established by obtaining permission and filling out a badge access request form.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 920 – DATA CENTER ACCESS & MAINTENANCE	Section 900

- D. Unaccompanied access authorization does not automatically grant permission for that individual to escort or admit others to the Data Center. A clear mission requirement will exist.
- E. Only Infrastructure technical staff is allowed to authorize the delivery or removal of equipment in or out of the Data Center. No items will be brought in or taken out without Infrastructure's knowledge and permission.
- F. Unaccompanied access implies consent to search the person or belongings if such a search is required to ensure the confidentiality, integrity, or availability of information or systems.
- G. By entering the Data Center, individuals accept responsibility to monitor activities and report things that may look wrong or out of place. It is their responsibility to recognize those others who are in the room and to try to verify the identities of those they are not sure of.
- H. Employees granted access at this level are expected to leave the Data Center by 5 p.m. each workday.

920.25 Accompanied Access

- A. Those with Accompanied Access will be allowed access to the Data Center, only with those who are appropriately badged for Unaccompanied Access and who are authorized to admit others.
- B. Access at this level will be granted on an ad hoc basis as project requirements dictate. .
- C. Employees acting as escorts must remain in the Data Center during the visit or stay and be in a position to observe what is done. Escorts assume responsibility for the actions of those they allow into the Data Center and are responsible to clear them back out, ensuring that they have not removed items of equipment, media, or data.

920.30 No Access

- A. Everyone who is not otherwise cleared, and has a business need for entering the facility, is in this category.
- B. An individual may also be moved into this category as a result of an unfavorable personnel action, investigation information, or as a result of criminal activity. When that occurs, the IT Manager will be notified, and Facilities will be contacted immediately to change the badge access programming. If access is required as a part of the individual's work requirements, they may have to be terminated as a result of losing access to the Data Center.
- C. Employee or contractor status does not imply access authority. Each individual will be evaluated on a case-by-case basis before being moved from the "No Access" category.

920.35 Emergency Access Procedures

- A. In the event of fire, natural disaster, chemical spill, or any other event which would render any data center uninhabitable, the building will be evacuated immediately. If damage could be caused to the systems, the Infrastructure Administrator will make the decision to affect an Emergency Power Off (EPO) cutting electricity to all systems.
- B. Emergency personnel – fire, police, and/or the Waukesha County Sheriff's Department will generally control access to the site during the entire course of the emergency. Only the site commander or senior emergency staff member on site may authorize access to the building and the Data Center.
- C. Once access is granted, the IT Manager, Infrastructure Administrator or the senior I.T. person on site will enter first, to make an initial assessment of the condition of the Data Center and equipment.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 920 – DATA CENTER ACCESS & MAINTENANCE	Section 900

- D. If conditions keep the site habitable, systems will be allowed to remain running, and Infrastructure personnel will access the data center to make an assessment and take appropriate remedial action.
- E. If the site can be accessed, but is not habitable, personnel will be called into the data center to begin a process of an orderly shutdown, and begin removing equipment, racks, etc. that are functional or may be repairable. Priority will be given to the safety of personnel, and to evacuating as much equipment as possible to a safe indoor location, or a safe and guarded outdoor location, until it can be moved to a better location. Precise procedures and instructions will depend on the nature and extent of the emergency. The senior I.T. staff member on site will direct the effort, and work with other agencies to secure help to move and transport equipment.
- F. Movement, repair and restoring of service will be prioritized in accordance with the business continuity plan.
- G. System, tapes and networking devices will be secured in accordance with the level of security of the information that remains.
- H. If the building is structurally dangerous, the minimum personnel necessary may be allowed into the Data Center to retrieve as much as can be safely removed.

920.40 Maintenance Recordkeeping

- A. Any maintenance work done on the physical structure, walls, doors, utilities, or locks of the Data center will be approved by the Infrastructure Administrator.
- B. All work done will be documented.
- C. All workers will be cleared by the Infrastructure Administrator prior to entry to and will be escorted into the Data Center.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 925 – INCIDENT RESPONSE AND REPORTING	Section 900

925 Incident Response and Reporting

The purpose of this document is to establish policies and procedures for responding to information and network security incidents in Waukesha County.

It is the intention of Waukesha County to adhere to a standardized procedure of responding to security incidents, investigating these events, documenting the results of those investigations, and taking appropriate action to meet operational and legal requirements for addressing the incident. The County shall maintain preventative measures to avoid any reasonably anticipated events that would compromise the confidentiality, integrity, or availability of data stored on the County network or County owned devices. It is also the intent of this policy that each investigation contains recommendations and courses of action that will lessen the likelihood of a recurrence whenever possible.

925.5 Scope

This policy applies to all actual or suspected security incidents on Waukesha County networks, including attacks emanating from outside the County, business partner connections, wireless and remote access, or the theft or unauthorized removal of media, data, storage devices, disks or CDs. This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

925.10 Description and Definitions of Incidents**A. Denial of Service**

Denial of service attacks are those incidents which cause network or information resources to abnormally terminate operations, degrade operation, or be disrupted or interdicted to the point where they cannot efficiently perform their intended function. This can be caused by a targeted attack from one or more internal or external sources, a server crash or network failure either by intentional attack or a natural occurrence, or a denial of physical access to a facility or devices. Such an event could affect critical systems used throughout the County is would need to be addressed immediately and investigated.

B. Malicious Code

Any worms, Trojan horses, rootkits, or viruses brought into the County network intentionally or unintentionally have the potential to attack and destroy data quickly, or to compromise the confidentiality and integrity of our information. Such an event would require immediate attention.

C. Unauthorized Access

Anyone gaining access without authorization to the County network or County owned media, devices, or servers would be classified as a violation of policy and a security incident. This incident would require immediate attention and coordination between multiple departments.

D. Inappropriate Usage

An individual who accesses systems, networks or data without full compliance with all policies violates the County Acceptable Use Policy. Examples include, but are not limited to the access of inappropriate web sites, using the County E-Mail system for inappropriate, non-work related materials, abusing systems or using them for unintended purposes, using workstations, or using servers or other devices to attempt to monitor, detect passwords, probe systems or networks, or other such hacking or cracking activities. This type of incident may be less critical, but does require prompt response.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 925 – INCIDENT RESPONSE AND REPORTING	Section 900

- E. Mixed or Blended Attack
It is possible that an incident would be comprised of multiple categories of incidents. The relative severity of a blended attack will be determined based on the information gathered at the time of the attack or detection.

925.15 Incident Response and Reporting Procedures Framework

Incident Response and Reporting Activities generally fall within these major categories.¹

- A. Preparation and Prevention
The process of creating a policy severity index and reporting structure for incidents, and creating a security posture which may prevent incidents from occurring.
- B. Detection and Analysis
The steps involved in identifying an incident, providing immediate notification to appropriate parties, analyzing the available information, assembling the incident response team participants, creating an action plan, gathering data and/or evidence, and determining extent of access or damage.
- C. Containment, Eradication and Recovery
The processes involved with stopping the spread of the incident or problem, cleaning affected systems, recovering data, involving law enforcement agencies (if appropriate), finalizing the collection of logs and data, and returning systems or networks to a fully operational condition.
- D. Post-Incident Activities
Determining root causes, creating final reports, notifying affected individuals, complying with all legal requirements for notifications and documentation, determining corrective actions, and ensuring that those corrective actions become a part of the preparation and prevention process are all requirements of the Post-Incident Activities category.

925.20 Incident Response and Reporting Procedures

- A. Preparation and Prevention Phase:
1. The County will have a standing, on-call team of incident first-responders. This team will be comprised of the County Chief of Staff, the Risk Manager, the Security Officer, a member of HR, a member of Corporation Counsel, and the applicable Privacy Official.
 2. A notification system will be designed so that employees may report security incidents through a variety of methods. They will include electronic mail, in writing, by telephone, or in person. At least one of these methods will provide an anonymous method of notification. These methods will be included in the new employee orientation and training.
 3. Technical measures will be taken, consistent with budgeting and personnel levels, to monitor and prevent security events as are reasonably appropriate.
- B. Detection and Analysis Phase:
1. Upon notification of a security event, the Security Officer will take immediate steps to assess the validity of the information, and extent of the potential breach or incident.
 2. The Security Officer will determine the level of investigation and reporting that may be required, and make immediate notifications to appropriate individuals. This may be up to and including all members of the team.
 3. The County will adhere to a policy of flexible response, such that minor events can be handled and cleared quickly, with minimal involvement, but that more serious matters involve more team members. Depending on the severity, a determination will be made as to who needs to actively participate in the investigation. The investigating

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 925 – INCIDENT RESPONSE AND REPORTING	Section 900

personnel will create a work plan, determining the scope of the effort, and specific objectives.

4. Staff will be included as necessary to assess systems or networks, complete any required investigation items in the time frame allotted. In the event that specialized expertise is required or criminal activity may be involved, contractor or law enforcement resources may be called upon, respectively.
5. Human Resources will be notified so that an investigation can be done pursuant to the provisions of the Sanctions Policy.
6. It is the policy of Waukesha County that there will be no punishment 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.

C. Containment, Eradication, and Recovery Phase:

1. Priority will go to identifying the scope of the incident or attack, and containing its spread.
2. Every attempt will be made to retain and collect evidence, which could be useful to the investigation.
3. Systems beyond the initial scope of the report may need to be examined to determine the number of devices involved.
4. No system will be left on line until we determine that it is not harmful to networks or other systems.
5. Recovery will proceed as quickly as possible, without compromising security or unnecessarily exposing other systems to compromise or damage.

D. Post-Incident Activities Phase:

1. An incident report identification number will be assigned to each incident, regardless of severity. It will be assigned in an 8-digit format. In general, the format will be XXXX-YYYY, where XXXX is the Julian date when the report was submitted or discovery was made, and YYYY is a sequence number beginning at 0001, and incrementing by 1 for each event reported that day. For example, the first event on January 1, 2005 would carry an incident number of 5001-0001.
2. An Incident Report form will be started, creating a diary of events as they transpire. All documents, reports, logs, written summaries of interviews, files, etc. will become a part of the official record of the investigation. This information will be protected from public disclosure as permissible by law. A sample copy of the report is attached.
3. The Incident Response Team will continue to meet or discuss the investigation to determine whether the work plan needs to be expanded or modified.
4. Investigation will continue until all work plan requirements have been met or it has been determined that the data is unavailable.
5. Once data collection is complete, the Security Officer in coordination with Corporation Counsel will determine reporting and notification requirements.
6. Whenever possible reports will include, the proximate causes, and recommended corrective actions.

¹ “Computer Security Incident Handling Guide”, page 3-1, National Institute of Standards and Technology, Jan 2004, Gaithersburg, MD.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 930 – MEDIA HANDLING	Section 900

930 Media Handling Policy

The purpose of this document is to establish policies and procedures for the consistent and correct handling of removable and non-removable media for Waukesha County automated systems.

It shall be the mission of Waukesha County Government and all its employees to provide for the security (confidentiality, integrity, availability) of all information systems and resources. Storage, on both removable and non-removable media is a fundamental part of our systems and infrastructure. Appropriate handling, storage, security and destruction of these media are essential and required. In general, all media will be protected and secured in accordance with the highest level of information stored in any one of its files. Thus, if a single file on a drive contains protected information, the entire drive must be protected. Media will be physically protected from harm or loss whether or not it is installed or inserted into a target device, workstation or server. It will not be lying about in unprotected or public access locations. This policy will be reviewed annually.

930.5 Scope

This policy applies to all systems owned by, or connected to Waukesha County computers or networks. Remote systems are also included, such that equipment in remote locations, employees who are working from home, contractors, and business-to-business partners may also be covered within the scope of this policy.

930.10 Server Policies and Principles

- A. Servers will generally not be re-commissioned for other uses until an evaluation is completed to determine that residual data requiring special security considerations have been deleted.
- B. No media will be disposed of, without being erased, degaussed/or and destroyed first. The objective of such cleaning and/or destruction shall be to ensure that the data that was written to that device is no longer retrievable or readable by any recovery mechanism. In general, this requirement goes far beyond simply erasing the files, or formatting the drive. Additional steps or tools must be used to ensure that data is not available to those not authorized to access it.
- C. Servers will never leave any Data Center with drives in them unless it is being relocated to another data center, intact. The following procedures will take place:
 1. When a server is deactivated, the drives will be removed first, and taken directly to the office of the Infrastructure Administrator.
 2. Once the drives have been removed from the room, the server may be removed and disposed of or placed in storage as appropriate.
 3. The drives will be degaussed. This process involves running the drives through a professional quality degausser.
 4. After drives are degaussed, they will be physically destroyed, and pieces may be thrown away.
- D. The following procedures will take place in order to dispose of tapes:
 1. Tapes will be degaussed, using a professional quality degausser.
 2. The tape will then be pulled or removed from its case, reel or carrier.
 3. It will finally be cut up into short, random-length pieces, and the pieces disposed of in multiple trash containers over a several day period of time.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 930 – MEDIA HANDLING	Section 900

- E. Removable USB drives will not be allowed to be used with our server fleet, and use in the Data Center should be avoided.
- F. Manufacturers' CDs may simply be thrown away. CDs or DVDs with County data should be erased if possible, or destroyed by breaking; and, if they contained compliance type data (financial information, health information, payroll, juvenile), they should be shredded.
- G. If sensitive data is copied to a portable, removable media, the movement of that media will be accounted for and tracked. The individual responsible for creating the data onto the removable media is responsible for its care until destruction can be certified.
- H. Upon destruction of all media, a Certificate of Destruction form will be completed. A copy of the form may be obtained from IT.

930.15 Workstation-Specific Policies and Principles

- A. Workstation media must also be protected and potentially erased or destroyed when the device or media is decommissioned.
- B. Workstations may be reused, elsewhere in the County. In this event, the device will be reconstructed or re-imaged, essentially destroying the data on the drive.
- C. If a drive is damaged, but still under warranty, every attempt is made to run the Autoclave program, at level 3, against the device. The electronics are then returned to the vendor and the media are physically destroyed.
- D. If a drive is operative and the system is being disposed of, the Autoclave program will be run at level three, and the physical media will be destroyed with a hammer and then disposed of. A Waukesha County computer forensic investigator has certified that data cannot be retrieved from an intact drive after Autoclave has been run at level 3.
- E. There is no outright prohibition against using removable devices like USB drives or writeable CDs or DVDs. Extreme care must be exercised, since they are smaller and easier to lose. The entire medium takes on the classification and restrictions of the highest level of information on that medium. Thus, if there are 1000 files on a USB flash drive, and only one has HIPAA data, the entire device must be treated as if it had HIPAA data on it. All users must protect removable devices and secure them. Any loss or theft will be reported immediately.
- F. The county reserves the right to implement special provisions restricting the use of non-county devices or mandating security and encryption for such devices.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 935 – NETWORK DEVICE INSTALLATION & CONFIGURATION	Section 900

935 Network Device Installation and Configuration Policy

The purpose of this policy is to describe how networking devices and equipment will be installed, configured, maintained and secured at Waukesha County.

Networking devices, servers and ancillary equipment provide the backbone infrastructure on which all our data moves. As such, it provides extraordinarily high exposure and vulnerabilities in the area of information security. Intrusions, breaches, or mis-configured or improperly installed equipment can immediately impact on operations, security or both. Special precautions must be followed to ensure the confidentiality, integrity and availability of our information, networks and systems.

935.5 Scope

This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

935.10 Network Device Installation and Configuration**A. Switches and Routers**

1. Switches, routers and other connectivity equipment will be procured based on the County architectural standard.
2. Only the Infrastructure Group of Information Technology Division will specify, procure, configure and install network connectivity devices.
3. All such devices will be secured in locked closets or facilities, and protected from intrusion and tampering.
4. Wires will be color coded to distinguish standard LAN connections from specialized VLANs or unsecured connections.
5. Administrative access will be provided to the least number of personnel, and only those having a direct need for access at this level.

B. Firewalls, Intrusion Detection Sensors, Network Probes

1. This is a very specialized classification of equipment that requires special handling.
2. These will be deployed only with the approval of the County Security Officer.
3. Log file data requires special protection to ensure that results of security investigations, issues, or incidents are not released inappropriately.
4. Only authorized personnel will review and report on firewall and probe data.
5. Details of firewall, and security devices type, software versions, and configuration data will not be disclosed without the permission of the Security Officer.
6. Administrative access to security devices will be provided to the least number of personnel, and only those having a direct need for access at this level.
7. All changes will be evaluated and tested both before and after moving them to production. Unanticipated consequences which may weaken security will be sufficient cause to return the device to the last known good configuration.
8. Firewall and router rule sets, and access control lists will be reviewed at least quarterly.
9. All firewalls and security devices will be designed to generally allow access from higher level security interfaces to lower level. They will be designed to restrict higher security interfaces from all other traffic unless it has been specifically allowed, and technically implemented. Medium security interfaces, such as the DMZ will be egress filtered such that unintended traffic will not be allowed to exit the network.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 935 – NETWORK DEVICE INSTALLATION & CONFIGURATION	Section 900

- C. Servers and Hosts
1. All servers and hosts will be installed and secured in an authorized County data center.
 2. Administrative access will be provided to the least number of personnel, and only those having a direct need for access at this level.
 3. All hosts will be secured in accordance with industry best practices for security hardening. Non-essential services will be removed or deactivated. Access to the host will be the minimum necessary for an individual to perform their assigned tasks or duties.
 4. Servers will have industry standard anti-virus software installed, and configured for frequent and periodic update.
 5. For availability requirements, backups will be conducted in accordance with the Data Backup and Storage Policy.
 6. Servers will be monitored and reviewed for unauthorized activity. Incidents will be reported to the Security Officer immediately.
- D. Wireless Networking and Devices. By its very nature, wireless networking is less secure than traditionally cabled networks. Technology has provided simple and inexpensive ways to clandestinely connect to or monitor the functions of wireless networks or devices, and in some cases to be able to illegally capture information and data, utilize networked resources for their own unauthorized purposes, or disrupt the operation of wireless networks or devices. Waukesha County will take special steps in the deployment and security of wireless networks and equipment.
1. Wireless equipment will only be installed by authorized employees of the Information Technology Division. While such equipment is readily available and quite inexpensive in the general marketplace, employees may not simply purchase devices or bring them in from home, and plug them into County networks.
 2. Wireless access points will not be connected directly to our internal networks. They will be connected to lower security networks. Access to internal networks from wireless access points will use a VPN client for encryption and authentication.
 3. Devices using wireless connections should be protected with personal firewall software.
- E. Special Security Consideration for Classrooms, Meeting Rooms and other Public or Unattended/Unsupervised Areas. Such areas will follow the same security architecture and engineering guidelines as wireless – that the connection will be outside the secured County network infrastructure. Access to secured networks, from common areas will require a VPN client. This provision does not apply to interior conference rooms inside of office areas.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 940 – REMOTE ACCESS	Section 900

940 Remote Access

The purpose of this policy is to provide guidance on security and use of Waukesha County systems from a remote location.

The County provides the capability to remotely access our networks and systems for several business-related purposes. This capability makes it possible for the County to allow people to work from home or from official travel locations, to allow for business-to-business connections to support missions and support requirements, and to allow for the access or exchange of information with individuals or other governmental agencies.

940.5 Scope

This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

940.10 Remote Access Practices

These measures will be followed and enforced for remote access users:

- A. Remote access is defined as connections to County networks and or systems from outside of a County building or campus location. This includes, but is not limited to dial-up from home or other location, client-based VPN, router-based VPN, or access to an application through the Internet.
- B. Access will be established through the use of a login request form. For business-to-business connections, a County employee must certify the requirement and need for remote access.
- C. All access will be authenticated. Each user will establish a userid and password for security and logging purposes.
- D. Remote access capabilities will not be engineered or installed by anyone outside of the Infrastructure group of Information Technology Division. Under no circumstances will modems be directly attached to workstations, or will devices such as workstations or laptops be plugged into phone lines at the County. The County does monitor and audit for such devices, and disciplinary action will be taken if unauthorized devices are found.
- E. Employees who are accessing networks from home, or using a laptop system from a remote location will ensure that these systems contain adequate and updated anti-virus protection. If a personal workstation appears to be virus infected or is behaving unpredictably, it should not be used to access County systems until it has been checked and issues have been addressed.
- F. Under no circumstances should family members be allowed to access a workstation or County networks. Passwords should not be saved in dialers or programs on workstations such that another family member could access the system without the employee's knowledge. Family members are not allowed to use County connections to surf the web, collect Email or use networks or systems for any reason.
- G. County systems and networks are monitored. There should be no presumption of privacy.
- H. Contractor or business-to-business connections will be provided on an as-needed basis only. Accounts will be activated for the minimum practical duration, and inactivated when not in use. Businesses desiring connections should complete a remote access networking agreement as a part of the contracting process. A sample is attached.
- I. Waukesha County Acceptable Use policies govern individuals utilizing remote access.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 945 – E-MAIL	Section 900

945 E-Mail

The purpose of this policy is to provide guidance on the security and use of electronic mail.

Unless special measures are taken, E-Mail is not to be considered a secured medium of communication. The protocol and technical standards by which E-Mail is transmitted do not provide any requirement for encryption or security. Everyone must assume that any E-Mail could be intercepted or detected in transmission, and therefore, opened and read. Additionally, our systems are subject to the State's Open Records Provisions, thereby making it impossible to protect against the lawful disclosure of the contents of some E-Mail messages.

All E-Mail users must assume that the recipient could forward the message to other persons or accounts, without the sender's knowledge or consent. E-Mail can be copied, printed, stored and retrieved, all without the sender's authorization. It may be best stated that you should send nothing in an E-mail that you would not want to see in tomorrow's newspaper.

Additionally, the County stores information that is not publicly available. Such information should not be inadvertently released by placing it into E-Mail. There are strict rules and guidelines for some types of information. We are subject to laws protecting things like juvenile or health care records, personal financial information, and other types of highly sensitive information. Individual users should know and understand the laws and policies for each type of information they may want to send in E-Mail.

945.05 Scope

This policy applies to all County employees, elected officials, County Boards and commission members, interns, contractors, affiliated or tenant agencies, business partners and volunteers who have access to County email systems. This policy applies to all E-Mail accounts, on any platform under the administration and control of Waukesha County Government.

945.10 Specific E-Mail Policy Guidelines.

- A. A special, encrypted E-Mail system (Securemail.waukeshacounty.gov) exists, which may be used to pass sensitive information such as ePHI outside of the County. To learn more about this capability, contact your department head or IS Coordinator.
- B. E-Mail is not a secured media, except inside the County's Exchange/Outlook environment. Any E-Mail that can be sent out of the Exchange/Outlook system to locations outside of Waukesha County should be considered non-secure unless you have been informed otherwise.
- C. The use of the County E-Mail system should be restricted for business purposes only. However, the County understands that employees occasionally need to use E-Mail for personal reasons. Employees are required to keep this usage to a minimum and should attempt to use other alternatives for personal E-Mail. Excessive or inappropriate use of the County E-Mail system for personal use is prohibited and may lead to disciplinary action.
- D. No individual should E-Mail sensitive, personal or private information.
- E. Never send E-Mail that is obscene, harassing, sexually oriented, or clearly unwanted by the receiver.
- F. Exercise discipline in the choice of words and any emotions displayed in the document.
- G. There are special laws and rules requiring our compliance. It is especially important for Departments to understand these and to train their people appropriately.
- H. In general, E-Mail is subject to applicable privacy, security, and records retention laws and guidelines, as are appropriate, for the information that a particular message contains. The employee and their Department will ensure that E-Mail is being appropriately

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 945 – E-MAIL	Section 900

secured and retained. It is important to remember that you may be creating a government document simply by creating and sending an E-Mail.

- I. E-Mail is subject to monitoring or inspection by the managers and leaders of Waukesha County. Employees should have no expectation of privacy on County E-Mail systems.
- J. Every E-Mail bears the host name of the sending agency. All E-Mails sent from Waukesha County reflect on our organization.
- K. Employees should not open unusual looking or unexpected E-Mail. Often, E-mail is used for illegal purposes or contains computer viruses.
- L. Employees should never respond to E-Mail requesting personal or banking information, or requesting user IDs or passwords. If there is doubt as to the authenticity of an E-Mail, or of what it is asking a person to do, they should contact their manager immediately for assistance.
- M. E-Mails can be traced back to their sender. Employees will be held personally responsible for E-Mails they send. Protect your password and understand the rules concerning the information contained in your E-Mail.
- N. Autoforward rules should never be set up to forward Email from your County Outlook mailbox to a personal or non-county Email account.

945.15 Incident Response and Reporting.

Certain incidents must be reported to your manager or the Security Officer. They are as follows:

- A. Unauthorized release of information in an E-Mail, whether intentional or accidental.
- B. Receipt of any E-Mail containing information that is protected from disclosure (such as health care information), or E-Mail that looks to be illegal or contains sexually explicit, hate-group related or otherwise illegal material.
- C. Suspicion that your password has been disclosed or that someone may have been using your E-Mail account.
- D. Any E-Mail that triggers your anti-virus software.
- E. Any individual who asks you for your password, or to use your account to review the contents of your E-mail.

Report Incidents by calling 970-4757, or by sending E-Mail to infosec@waukeshacounty.gov

Chapter 2 – Information Technology		
Issued: 6/2/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 950 – PASSWORDS	Section 900

950 Passwords

The purpose of this policy is to establish and maintain standard parameters for passwords used in Waukesha County.

At present, the combination of Login IDs and passwords are considered to be adequate and acceptable security measures for all of our systems. The fundamental philosophy of this policy is to ensure that the passwords we use on our systems are 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 Waukesha County Government.

950.05 Scope.

This policy pertains to all systems in use at Waukesha County Government. This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers. It includes but is not limited to workstations, servers, routing and switching equipment, and accounts on other devices.

950.10 Password Policy Procedures

These measures will be followed and enforced on our systems where possible:

- A. Passwords will be a minimum of 8 characters in length.
- B. Passwords will be changed every 90 days.
- C. Passwords may not be reused for 6 generations.
- D. The password shall not be something that is easily guessed, such as the name of a pet, a child or other family member, or any part of a person's name or their login ID. The password "password" is not acceptable, nor is a simple series of numbers like "12345678".
- E. Passwords should not be standard dictionary words that can be acquired or cracked with automated password cracking programs and brute force dictionary attacks.
- F. Passwords must contain at least one number or special character that is not at the beginning or the end of the password.
- G. Password will not be asked of, or given to others. If someone requests an individual's password, it should be reported to the Security Officer immediately.

950.15 Technical Implementation

- A. Passwords will not be written down and stored on or near computer equipment.
- B. Passwords will never be stored in any application or system in a readable format.
- C. Passwords will not be stored in database tables unless encrypted and not available to any account except the root, system, or administrator.
- D. Passwords will not be stored in scripts, or programs.
- E. Passwords and password files may not be copied or transmitted across any means of communication in clear text.
- F. It is the responsibility of technical staff, including systems administrators, developers, and support personnel to ensure that systems are designed and implemented that do not compromise the security of Login IDs or passwords, or inappropriately embed credentials and rights within stored procedures which may be readable.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 955 – INTERNET AND WEB ACCESS	Section 900

955 Internet and Web Access

This document provides policy, direction, procedures and guidance for the security of information systems and Internet resources for Waukesha County Government.

Access to the Internet from County workstations is provided to allow County employees access to critical information, access to applications residing outside the County, and to make employees more productive in their jobs. This access is provided for official use only, and should be based on the needs of the person or position.

955.05 Scope

This policy pertains to all systems in use at Waukesha County Government. This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers. It includes but is not limited to all workstations, servers, laptops, wireless devices, and other equipment allowed access to the public Internet.

955.10 Internet/Web Access Practices

- A. It is the responsibility of each Internet user to ensure that they are in compliance with all applicable laws and County policies, including computer security, virus detection, and access to questionable sites and/or material.
- B. Internet access is expected to be used for work related purposes only. Employees are encouraged to optimize their use of Internet resources to perform work-related research, in order to make them more knowledgeable or efficient. During non-work hours, the Internet may be accessed for acceptable personal use. For more information, refer to the Information Technology Use Policy.
- C. Streaming media should only be used for official or training purposes. The Internet should not be used to listen to radio or TV broadcasts for entertainment.
- D. Instant messaging is not allowed, except for that which is provided by Microsoft Communicator.
- E. Access to the Internet is not provided to all employees. It will be granted based on business need by a manager or supervisor through the use of the login request form.
- F. Internet access requires authentication through the firewall. This practice ensures that only authorized employees may access the Internet.
- G. Directors, managers and supervisors shall monitor Internet usage among their employees to ensure it complies with this policy.
- H. Under no circumstances is Internet access to be used to support another business or enterprise that the employee participates in off-hours.
- I. Under no circumstances will the Internet be used to access lewd, objectionable, pornographic, sexually explicit, or illegal materials, or sites that are sponsored by or contain materials regarding discrimination, hate groups, or gambling. The only exception to this rule is when such access is used to perform official investigations, required in the course of one's work, and approved at the Department Director level.
- J. The Internet shall not be used to transact business via personal (non-County) credit card unless that personal card is being used to transact County business. An example of this might be to purchase plane tickets or guarantee a hotel room for official travel. County credit cards (also called P-Cards) may be used online, to book airfare and seminar registration for the official use of the County, but except as noted above a personal debit or credit card may not be used to purchase any items using any County workstation or network connection.
- K. Internet access from County-owned workstations can be traced back to us at the County. It is to be used responsibly at all times.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 955 – INTERNET AND WEB ACCESS	Section 900

- L. Internet access is both filtered and logged. The County records and can report on the activity generated from a particular workstation. Such reports may be requested by managers and may form the basis for investigations or disciplinary action.
- M. Employees are to exercise caution when prompted to enter information, which will identify them, or the networking architecture of the County. If there is any question as to the legitimacy of the site or of the information requested, the employee should seek assistance from the Help Desk before proceeding. Employees accept all risk when entering person, medical, or financial information of any kind on external websites.
- N. Employees should not download programs or plug-ins from the Internet unless authorized to do so by IT. Such actions could download harmful programs, such as viruses or worms onto their system, or violate licensing and copyright laws.
- O. File downloads are permissible. Things like *.pdf files, Word Documents, research materials, etc. are permissible for download. All downloaded files should be checked for viruses. Employees shall take no actions that may disable the County-installed anti-virus systems.
- P. The Internet should not be used to attack, or test the security of other systems. This includes, but is not limited to the use of tools designed to sweep or detect devices on other networks, attempt to login to a system without permission or authorization, copy or plant information on another site, run a large number of pings or connection requests, or attempt to access non-public or unauthorized parts of a host or a site.
- Q. Violations of this policy may lead to administrative, disciplinary and in some cases, criminal action.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 960 – WORKSTATION SECURITY	Section 900

960 Workstation Security

This document provides policy, direction, procedures and guidance for the installation, positioning and security of workstation systems for Waukesha County Government.

The County will implement policies and procedures to keep end point systems (defined as desktop, laptop, and handheld computers, as well as printers) physically secure and accessed only by authorized users. That which is not specifically permitted is prohibited. Any variation from these procedures must be approved in advance. Special care must be taken to protect information that is considered particularly sensitive. Examples of this include, but are not limited to: Protected Health Information (PHI), financial information, or information that is protected by law.

960.05 Scope

This policy pertains to all systems in use at Waukesha County Government. This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers. It includes but is not limited to all workstations, laptops, or palm systems, whether wired or wireless.

960.10 Workstation Security Practices

- A. It is the responsibility of Waukesha County Government, and Department Heads, in coordination with the County Risk Manager, the Sheriff's Department, and the Department of Public Works to determine the access and security requirements for each building, and office area. The policy is to provide for adequate security and safety of personnel, access by the public to needed goods and services, confidentiality, availability and integrity of all information, adequate protection for County assets, the safety and protection of citizens, and to create a clean, efficient and productive work environment.
- B. Physical safeguards for end point equipment will be provided by using one or more of the following, as needed to achieve the above listed goals: counters and partitions, locked doors, card access or combination key access systems, camera monitoring, and/or alarmed entrances.
- C. There will be some cases in which end point equipment will be accessible to the general public. In general, the following rules will apply:
 1. The equipment will be in an office suite or building, which can be locked or secured after normal business hours.
 2. The equipment will be monitored to ensure that it is not removed or intentionally damaged while accessible to the public.
 3. The equipment will be technically locked down so that a member of the public cannot access our internal secured networks.
- D. For all cases, other than computers designated for public use, security will be provided by restricting and controlling physical access to offices and desktop systems, and by properly positioning and protecting systems such that information cannot easily be read or obtained.
- E. Monitors should generally be kept from the plain view of anyone who does not have the appropriate access or clearance to information that may be displayed. Site surveys should be conducted by each department to check for unauthorized viewing from the following sources:
 1. Through outside windows
 2. From public hallways
 3. From public reception areas
 4. Reflection off of other objects

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 960 – WORKSTATION SECURITY	Section 900

- F. This may be addressed by turning the monitor away from counter areas, or by installing a special shade or polarizing monitor filter. This is especially critical where compliance-related information, which may be protected by law, may be displayed.
- G. Keyboard, mouse, and other components should be kept far enough away from the public, so that they cannot be tampered with or stolen.
- H. Printers should also be kept in protected areas to keep sensitive information from being disclosed inappropriately.
- I. Printed materials from any source should be kept secure and away from viewing and out of public reach.
- J. The County will use standards that support workstation security. These include, but are not limited to:
 1. Utilization of either Windows XP or V7 operating systems, appropriately patched.
 2. Utilization of a locked down configuration – that each user will not have local administrator rights on his or her workstation.
 3. Utilization of an automatic screen saver that is password protected. Such screen savers will automatically activate after 15 minutes of inactivity.
 4. Exceptions to the lock out policies will be personally approved by Department Directors.
 4. Users or departments will take no action that disables the use or prolongs the time frame of such security measures.
 5. A standard warning message will be displayed on each system at start time. This message will inform each user that they are subject to applicable security rules, and may be monitored. An example is attached.
- K. The County considers workstations as a sensitive item – subject to accountability controls, and inventory tracking. Workstations will be appropriately tagged and accounted for, when entering the inventory, tracked throughout their lifecycle, and appropriately removed from inventory and destroyed.
- L. Removable media will have the same security requirements as the highest sensitivity of information on that device. They should be stored and secured as such.
- M. County employees should never modify their own systems, install hardware or software, or bring in personally owned software or devices. All software and hardware should be procured, and installed by County IT.
- N. All media storage devices will be destroyed in accordance with the Media Disposal Policy. They may not simply be discarded in the trash.

960.15 Inventory Management

Waukesha County tracks all hardware used in the county in the Information Technology (IT) Hardware Assets Tracking System (HATS). The IT Division and corresponding department share responsibility in maintaining all hardware assets in HATS (hardware type, ID tag number, machine name/printer name, user ID, serial number, location, projected year of replacement, fund cycle, pricing, and obsolete assets). Designated department personnel have continuous access to HATS to make adds/changes/deletes to records with their respective departments.

Refer to the Purchasing Division section 1920, Methods of Disposal, Disposal of Surplus/Obsolete Fixed Assets, and the IT Media Handling policies that establish procedures for the consistent and correct disposal and handling of removable and non-removable media for Waukesha County automated systems.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 960 – WORKSTATION SECURITY	Section 900

962 Portable/Removable Device Security

This section provides policy, direction, procedures and guidance for portable computing devices for Waukesha County Government.

Smaller, more portable devices provide greater risk to county information and networks. By their very nature, such devices are intended to be mobile and lightweight, making them easier to steal or misplace. Special care must be exercised both in granting such authority to employees, and monitoring their use.

962.05 Scope

This policy pertains to all portable devices/systems in use at Waukesha County Government or connecting to Waukesha County networks from remote locations. This policy applies to all County employees, elected officials, County Boards and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers. It includes but is not limited to all laptops, hand-held, notebook, smart-phones, CDs, DVDs, USB storage device or any other such system on which data can be accessed or stored, whether wired or wireless.

962.10 Portable/Removable Device Security Practices**A. General.**

1. It is the responsibility of Department Heads, Managers or Supervisors to determine the need and grant access for out-of-office computing, and if allowed, to provide appropriate training and oversight to ensure that data remains secure.
2. Employees are responsible to ensure that all information and devices remain protected, regardless of the location they might be working from, and to take reasonable safeguards to protect hardware, devices or information from theft, destruction or unauthorized release.
3. All policies which apply to the protection, care and security of information or technology assets apply regardless of location.
4. Portable devices should be secured and protected so as to avoid theft or unauthorized use. As far as is practical, the device should be under the observation and control of the employee, and should not be stored or left unattended. If the device must be temporarily kept in an automobile, it should be placed in a trunk, covered or hidden from sight and the vehicle should be locked and secured. Whenever practical, the device should be brought into a home or hotel room, under the direct observation or control of the employee during the overnight hours.
5. Employees should not use portable devices while operating a motor vehicle.
6. Any loss of hardware or suspected loss or compromise of data will be reported to a supervisor or manager immediately.

B. Laptop or Notebook Systems.

1. Laptop or Notebook systems, with installed applications provide a wealth of information to unauthorized individuals. Special care must be taken to ensure the device remains secure and under the control of county personnel.
2. Care will be taken to ensure that data is not copied or stored to the local hard drive. An exception to this policy would be that it may be permissible if the entire hard drive is encrypted.
3. Laptops connecting to the internet through an unsecured wireless connection face special risks. Employees must ensure that the windows firewall remains on, to ensure their system is not compromised.

C. SmartPhones, or iPhones.

1. Handheld devices which can receive Email, browse the Internet, and sometimes run applications are generally referred to as SmartPhones. These typically fall into three major categories: Windows Mobile, Blackberry, or Apple iPhone technologies.

Chapter 2 – Information Technology		
Issued: 8/3/2005 Revised: 3/20/2010	INFORMATION SECURITY POLICY 960 – WORKSTATION SECURITY	Section 900

2. The county only supports Windows Mobile devices procured through our mobile phone contract. On a best-effort basis, the IT Division may have the resources necessary to assist users of personally-owned devices in accessing County Email.
 3. The County does not support custom applications of any kind on handheld devices at the present time. IT will assist in the initial setup and activating Email and Calendaring only.
 4. Individuals may choose to utilize their personal smartphone or handheld device to perform business related functions. They do so, totally at their own risk. The County assumes no liability for claims of damage resulting from such use.
 5. No County data should be stored on non-County owned devices.
 6. In order to connect to County Email systems, each user must allow automated policies to be pushed out to your handheld device.
 7. Handheld devices should not open directly to a user interface screen. There should be a PIN or password set to provide security.
 8. If a device is lost, it must be reported to IT immediately. A “remote wipe” will be done to erase the contents of the device upon next activation.
- D. Memory or Storage Devices. Because of the decreasing size and increasing capacity of small and/or portable USB devices, extra caution must be taken to ensure that County information is protected to the fullest extent of all laws, policies and guidelines. This includes but is not limited to CDs, DVDs, thumb drive/memory stick type devices, iPods or other devices onto which it is possible to copy information or files, flash cards, and portable hard drives,
1. Employees should check with their supervisor or manager and obtain permission before using portable memory or storage devices.
 2. The entire device takes on the security requirements of the most secure data it contains. If only one file contains information requiring special security, the entire device must be secured to that level.
 3. Any device containing information that is protected by law or policy must be encrypted in accordance with County guidelines and standards.
 4. Devices must be encrypted with County-standard encryption. Use of departmentally procured or personal encryption software is not permitted.
 5. If a device is lost, it must be immediately reported.
 6. If such portable media is used at all, an accurate inventory of the files and information it contains must be created and kept current.
 7. If a device is lost, it must be reported to IT immediately.