


| | | | | | |
|---|-------------------------------------|--------------------------------------|-----------------------------------|--------------------|--|
|  | WASHTENAW COUNTY POLICY | GENERAL OPERATIONS - VOLUME I | | | |
| TITLE: Security for E-Government Initiatives | RESOLUTION NUMBER 01-0232 | SUPERCEDE: | EFFECTIVE DATE 10/17/01 | PAGE OF 1 6 | |

I. APPLICATION:

This policy shall govern the County's security for any E-Government Initiative.

II. INTENT:

It is the intent of the Board of Commissioners to provide guidelines for the security and integrity of the information obtained and contained on it's website and any E-Government initiative.


III. GENERAL POLICIES

- I. The sensitivity level of all E-Government systems will be determined based on the sensitivity of the data processed or the importance of the system to mission accomplishment. All systems must include security controls that reflect the true importance of the information processed on the system and/or the government investment embodied in the components of the E-Government system. The sensitivity level of all Washtenaw County E-Government systems will be identified in one of the following categories:

- (1) Secure Systems contain information, which requires protection against unauthorized disclosure
- (2) Sensitive Systems include those that require some degree of protection for confidentiality, integrity or availability.
- (3) Non-Sensitive Systems contain only public data, which has no protection required for confidentiality, and the services of the County can be accomplished without the system.

Password Standard

All Secure Systems will be protected by personal passwords selected by users. These passwords must contain **at least** six characters with the combination of ~~four~~ **four** alphabetical letters and ~~two~~ **two** numeric digits. No password will be given over the phone or listed on the web site but shall always be sent to the original e-mail of the user in highest secured format.

| | | | | | |
|---|------------------------------------|---|-------------------|---|----------------------------------|
|  | WASHTENAW COUNTY POLICY | GENERAL OPERATIONS - VOLUME I | | | |
| TITLE: Security for E-Government Initiatives | | RESOLUTION NUMBER 01-0232 | SUPERCEDE: | EFFECTIVE DATE 10/17/01 | PAGE OF 2 6 |

Verification Review

An E-Government Security verification review will be conducted on all E-Government systems by an evaluation team under the direction of the Washtenaw County Information & Technology Services Department (ITS). The purpose of the E-Government security verification review is to provide a level of review and evaluation, independent of the system owner, that will verify that adequate and appropriate levels of protection are being provided for the individual systems, based on their unique protection requirements.


Incidents and Violations

All Washtenaw County departments will establish and implement, with the assistance of the Washtenaw County ITS, a process and procedures to minimize the risk associated with violations of E-Government security, and to ensure timely detection and reporting of actual or suspected incidents or violations. An E-Government security incident is any event, suspected event, or vulnerability that could pose a threat to the integrity, availability, or confidentiality of Washtenaw County systems, applications or data. Incidents may result in the possession of unauthorized knowledge, the wrongful disclosure of information, the unauthorized alteration or destruction of data or systems and violation of federal or state laws. If such violations are detected or suspected, they are to be reported immediately to the Washtenaw County ITS Customer Support.

Malicious Software

ITS and all Washtenaw County departments will comply with County Internet and E-mail Policies and Procedures to:

- (1) Minimize the risk of introducing viruses and other malicious software.
- (2) Ensure timely detection of viral infections.
- (3) Eliminate viral infections from the County's inventory of microcomputers (PCs).
- (4) Minimize the risk from malicious programs to larger systems, or systems where virus detection software is not yet available. If such violations are detected or suspected, they are to be reported immediately to the Washtenaw County ITS Customer Support.

| | | | | | |
|---|-------------------------------------|--------------------------------------|-----------------------------------|--------------------|--|
|  | WASHTENAW COUNTY POLICY | GENERAL OPERATIONS - VOLUME I | | | |
| TITLE: Security for E-Government Initiatives | RESOLUTION NUMBER 01-0232 | SUPERCEDE: | EFFECTIVE DATE 10/17/01 | PAGE OF 3 6 | |

Contingency and Disaster Recovery Plan

Washtenaw County ITS and its third party E-Government vendor are responsible for the development and maintenance of contingency plans that address the following activities:

- (1) Backup and retention of data and software.
- (2) Selection of a backup or alternate operations strategy.
- (3) Emergency response actions to be taken to minimize the impact of the emergency.
- (4) Actions to be accomplished to initiate and effect backup or alternate site.
- (5) Resumption of normal operations in the most efficient and cost-effective manner.

The contingency plan for disaster recovery will provide reasonable assurance that critical data processing support can be continued, or resumed quickly, if normal operations of the system are interrupted.


Hardware Security

Washtenaw County departments, in conjunction with ITS and its third party E-Government vendor, shall assure that appropriate technical security requirements are included in specifications for the acquisition or operation of equipment intended to process secure or sensitive information. These specifications shall be reviewed and approved by the Washtenaw County ITS prior to the development. It may not be feasible or cost effective to retrofit existing, older computer hardware. However, the security requirements should be considered when acquiring or developing new systems, to ensure that they are incorporated either within the hardware or operating system software.

Software Applications

Prior to placing a secure or sensitive software application into operation, Washtenaw County operating units will verify that the required user functions are being performed completely and correctly, and that the specified administrative, technical and physical safeguards are adequate for the protection of the information.

Application Software - An application that processes sensitive data, or requires protection because of the risk and magnitude of loss or harm that could result from improper operation, manipulation or disclosure, must be provided protection appropriate to its sensitivity. The following will be considered as the minimum controls to be applied to sensitive applications, with additional controls or safeguards to be imposed if appropriate:

| | | | | | |
|---|-------------------------------------|--------------------------------------|-----------------------------------|--------------------|--|
|  | WASHTENAW COUNTY POLICY | GENERAL OPERATIONS - VOLUME I | | | |
| TITLE: Security for E-Government Initiatives | RESOLUTION NUMBER 01-0232 | SUPERCEDE: | EFFECTIVE DATE 10/17/01 | PAGE OF 4 6 | |

(1) Security requirements will be defined, and security specifications approved, by the user prior to acquiring or starting development of applications, or prior to making a substantial change in existing applications.

(2) Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified by the user.


(3) New or substantially modified sensitive applications shall be thoroughly tested prior to implementation to verify that the user functions and the required administrative, technical and physical safeguards are present and are operationally adequate.

(4) Live sensitive data or files will not be used to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.

(5) Sensitive application software will not be placed in a production status until the system tests have been successfully completed and the application has been properly certified.

Physical Security

Adequate physical security measures must be provided for the protection of human resources, physical and logical assets and sensitive applications and data. Physical security measures must be selected and implemented in consideration of the sensitivity of the E-Government resources and their criticality to the supported functions. For the purposes of these policies, controlled areas are those which encompass or allow access to potentially sensitive information resources, resources which are essential for the processing of sensitive data, or resources essential to accomplishment of organizational missions. These areas include, but are not limited to: any spaces housing computer equipment, including PCs and file servers; data storage libraries; input/output areas; data conversion areas; programmer areas and files; documentation libraries; communication equipment areas; computer maintenance areas; mechanical equipment areas; telephone closets; environmental controls and power systems; and supply storage areas.

| | | | | | |
|---|---|--------------------------------------|---|---------------------------|--|
|  | WASHTENAW COUNTY POLICY | GENERAL OPERATIONS - VOLUME I | | | |
| TITLE: Security for E-Government Initiatives | RESOLUTION NUMBER 01-0232 | SUPERCEDE: | EFFECTIVE DATE 10/17/01 | PAGE OF 5 6 | |

A risk analysis of the physical security requirements of controlled areas will be directed by the Washtenaw County ITS Director and Risk Manager. When automation or data communications equipment are located within user areas, the user management officials in that department, in conjunction with the Washtenaw County ITS, will assess the sensitivity of the data, automated resources and functions performed and, if warranted, designate the area as a controlled area. The operational areas of major computer installations, including local area network file servers, will be designated restricted areas in which access will not be permitted unless specifically authorized or required for job performance.

Controlled and restricted areas will be protected by physical security and other means which are deemed appropriate for the sensitivity or criticality of the system as determined by the results of a risk analysis and as defined in the Washtenaw County ITS for the system. At a minimum, access to controlled areas will be limited to those individuals having an official need to be in the area. E-Government devices which are easily moved, have non-removable hard drives and are used for sensitive information will not be allowed outside of the controlled area. If the sensitive data remaining on the media has been completely erased or obliterated, the removal of these devices from the work area may be approved by the Washtenaw County ITS Director.


Media used to record and store sensitive software or data will be externally identified, protected, controlled and secured when not in actual use. Technology equipment rooms of all types will be secured with a high-quality security system.

Environmental Safeguards

Adequate environmental safeguards must be installed and implemented to protect IT system resources as deemed appropriate for the sensitivity or criticality of the system as determined by the results of a risk analysis and as defined in the Security Plan for the system. At a minimum, the following environmental safeguards must be considered:

- I. Fire prevention, detection, suppression and protection
- II. Water hazard prevention, detection and correction
- III. Electric power supply protection
- IV. Temperature control
- V. Humidity control
- VI. Natural disaster protection from earthquake, lightning, windstorm, etc.
- VII. Magnetism protection

VIII. Software Security

| | | | | | |
|---|--|--|-------------------|---|-----------------------------|
|  | <p align="center">WASHTENAW COUNTY POLICY</p> | <p align="center">GENERAL OPERATIONS - VOLUME I</p> | | | |
| <p>TITLE: Security for E-Government Initiatives</p> | | <p>RESOLUTION NUMBER 01-0232</p> | <p>SUPERCEDE:</p> | <p>EFFECTIVE DATE 10/17/01</p> | <p>PAGE OF 6 6</p> |

Washtenaw County ITS will continue its investigation in Security through ongoing research, vendors and third party partners.

Washtenaw County will be using a third party consultant to develop E-Government applications and the consultant will be responsible for application development, maintenance and hosting. Security guidelines for the third party consultant will be reviewed once the contract is signed. Establishing an E-Government security policy will be one of the first responsibilities of the E-Government policy committee working in conjunction with our E-Government vendor.