

Washington County Maryland
Information Technology Management (ITM) Policy
Manual



NOVEMBER 2006

Washington County Maryland Information Technology Management (ITM) Policy

Table of Contents

<u>Section</u>		<u>Page</u>
	1 General Provisions	
1.1	Purpose	1 – 2
1.2	Distribution	2
1.3	Scope	2
1.4	Policy Exclusions	2 – 3
	2 General Management Guidelines	
2.1	General	4
2.2	Privacy Rights	4
2.3	Use of Technology	4
2.4	Management of Technology	4
2.5	Violations	4
2.6	Information Technologies (IT) Project Priorities	5
2.7	Guiding Policy Principals	5
2.8	Annual IT Plan and Development Process	5
2.9	Policy Review and Update	6
	3 Roles and Responsibilities	
3.1	Information Technologies Director	7
3.2	Information Technologies Staff	7 - 8
3.3	Division Directors and Department Heads	8
3.4	Information Technology Coordinators (ITC)	8
3.5	All Employees	9
3.6	Revision History	9
	4 Specific Management Policies	
4.0	Specific Management Policies Listing	10
4.1	Application Change Management Policy	11 – 15
4.1.1	General	11
4.1.2	Procedures	11 - 13
4.1.3	Application Change Prerequisites	13
4.1.4	Planning and Performing Project Acceptance Testing	14
4.1.5	Planning Change Training	15

Washington County Maryland Information Technology Management (ITM) Policy

Table of Contents

<u>Section</u>		<u>Page</u>
4.2	Data Management Policy	16 – 22
4.2.1	General	16 - 17
4.2.2	Roles and Responsibilities	17 – 18
4.2.3	Data Sensitivity	18
4.2.4	Procedures	18 – 21
4.2.5	Backup and Recovery	21 – 22
4.2.6	Violation of Policy and Misuse of Data	22
4.3	Hardware Management Policy	23 – 26
4.3.1	General	23
4.3.2	Ownership	23
4.3.3	Procurement of Hardware and Related Services	23 – 24
4.3.4	Replacement Strategy	24
4.3.5	Replacement and Upgrade Budgeting	24
4.3.6	Budgeting for Capital Projects and New Positions	24 – 25
4.3.7	Replacement Process	25
4.3.8	Refresh Process	25
4.3.9	Recycling Computers and Technology	25
4.3.10	Hardware Installation, Maintenance and Technical Support	25
4.3.11	Non-County Owned Computer Hardware	26
4.4	Software Management Policy	27 – 30
4.4.1	General	27
4.4.2	Ownership	27
4.4.3	Software Manager	27
4.4.4	Procurement of Software and Related Services	27 – 28
4.4.5	Budgeting for Software	28
4.4.6	Registration of Software	28
4.4.7	Software Licensing	28
4.4.8	Duplication and Distribution of Software	29
4.4.9	Employee Software Training	29
4.4.10	Installation of Software	29
4.4.11	Software Maintenance and Technical Support	29
4.4.12	Open Source (OSI) Software	29 – 30
4.4.13	Periodic Audits and Policy Violation	30
4.4.14	What is the Federal Law?	30
4.5	Telecommunications Management Policy	31 – 32
4.5.1	General	31
4.5.2	Telecommunication Services Provision and Management	31
4.5.3	Telecommunication Services Usage and Charges	31 – 32

Washington County Maryland Information Technology Management (ITM) Policy

Table of Contents

<u>Section</u>		<u>Page</u>
4.5.4	Requests for Service or Assistance	32
4.5.5	Trouble Reporting	32
4.6	Systems and Electronic Communications Use Policy	33 – 37
4.6.1	General	33
4.6.2	General Responsibility	33
4.6.3	Limited Personal Use	33 – 34
4.6.4	Privacy Rights	34
4.6.5	Monitoring	34
4.6.6	Backup	34 – 35
4.6.7	Employee Owned Electronic Devices and Equipment	35
4.6.8	Passwords	35
4.6.9	Software	35
4.6.10	Computer and Data Safeguards	35 – 36
4.6.11	Internet and Email	36
4.6.12	Prohibitions	36 – 37
4.6.13	Violation of Policy	37
4.7	Access Control Policy	38 – 42
4.7.1	General	38
4.7.2	Personnel Security Procedures (new hires, transfers, separation, and certification)	38 – 39
4.7.3	User Identification and Passwords	39 – 41
4.7.4	Enforcement	41
4.7.5	Access Restriction	41 - 42
4.8	Network and System Security Policy	43 – 49
4.8.1	General	43
4.8.2	Policy Goals	43
4.8.3	Roles and Responsibilities	43 – 44
4.8.4	General System Security Procedures	44 – 47
4.8.5	Network Security Practices	48 - 49
4.9	Documentation and Equipment Information Policy	50 – 51
4.9.1	General	50
4.9.2	Format and Storage	50
4.9.3	Documentation Requirements	50 – 51
4.9.4	Equipment Information	51
4.10	Information Technology Steering Committee	52 – 54
4.10.1	General	52

Washington County Maryland Information Technology Management (ITM) Policy

Table of Contents

<u>Section</u>		<u>Page</u>
4.10.2	Responsibilities	52
4.10.3	Membership	52 - 53
4.10.4	Sub-Committees and End-User Task Teams	53
4.10.5	Meeting Schedules	53 – 54

Appendices

	Appendices Listing	55
A	Acknowledgement of Information Security Responsibility Form	56 – 57
B	Privileged Access Agreement Form	58 – 59
C	IT Policies and Guidelines Summary	60

INFORMATION TECHNOLOGY MANAGEMENT (ITM) POLICY

Washington County Maryland

1. GENERAL PROVISIONS

1.1 Purpose

The purpose of this document is:

- to establish policy guidelines for Washington County Government (WCG) in managing information technologies (IT). These resources include data processing, telecommunications and office automation hardware, software, and services;
- to help ensure efficient use of limited automated information and telecommunications resources;
- to help prevent fraud, waste, and abuse in the use of such automated information and telecommunications resources;
- to help protect WCG, its employees, and any authorized user of Washington County's information technology from liabilities and service interruptions due to inappropriate use of Washington County's computers/terminals and/or information technology services and breaches of information technology security;
- to establish the roles and responsibilities for managing WCG's automated information and telecommunications resources;
- to provide guidelines for managing current systems and applications;
- to provide instructions and guidance for all information technology hardware, software, and telecommunications acquisitions and installations;
- to provide instructions and guidance for all telecommunications customer premise equipment and line acquisitions; and
- to provide instructions and guidance for developing and implementing all information technology and telecommunications applications in WCG.

For the purpose of this document, information technology refers to any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission or reception of data/information, or any other related data processing or office automation activity. Information technology systems/tools refers to all hardware, software, and any automation services or tools owned or licensed to WCG and available for **“official use”** by Washington County employees and all authorized personnel including, but not limited to, computers, servers, terminals and related peripheral equipment, software, voice mail, Internet connectivity and access to Internet services, and E-mail.

For the purpose of this document, telecommunications refers to all voice, data, image, and other communications such as wireless, satellite, and sensors. This includes, but is not limited to, modems, telephones, private or public analog/digital telephone lines, facsimile, switches, routers, electronic conferencing (video and audio), and all related equipment.

1.2 Distribution

The Information Technologies (IT) Director will distribute this policy to division directors and department heads. This document is provided as reference concerning IT management at WCG and as guidance for all systems users. Division directors and department heads will be responsible for ensuring their employees are aware of this policy and its contents.

1.3 Scope

This policy applies to all current and proposed information technology operating at WCG regardless of funding source. This includes, but not limited to, all requirements for IT equipment (personal computers, workstations, terminals, printers); communication links (asynchronous, synchronous, Frame Relay, TCP/IP); auxiliary equipment and hardware; software; management information systems; Internet access; IP address management; Web site development and management; electronic commerce systems; data warehousing; document management and imaging systems; all related services - national and local; and all studies for the development and evaluation of such systems or requirements.

This policy also covers telecommunications, data communications as well as voice communications. It includes all requirements for modems, data switches, multiplexers, private branch exchanges (PBX), key telephone systems, single and multiple line phones, FAX servers/machines, answering machines, voice mail, satellite reception, video conferencing, all related dial tone services, and all studies for the development and evaluation of such systems or requirements.

This policy applies to the preceding scope of activities regardless of their funding sources, organizational control, and performance by WCG or contractor staff.

1.4 Policy Exclusions

The Communications Maintenance Department manages and maintains WCG's public safety UHF radio communications system. The Communications Maintenance Manager provides for the overall management of the Public Safety UHF radio communications system and component assets and therefore management of the Public Safety UHF communications system and component assets are excluded from this policy.

The Department of Water Quality operates and manages a water quality process control network. The Director of Water Quality provides for the overall management of the water quality process control network and component assets that includes a broadband wireless network and therefore management of the water quality process control network and component assets are excluded from this policy.

Additionally, management and oversight of cellular telephones and services is addressed in Washington County Policy P-6, Cellular Telephones and Services and the deployment, management and oversight of pagers (digital and/or analog) and paging services is the responsibility of each department head and therefore management of cellular telephones, pagers and respective subscript services are excluded from this policy.

2. GENERAL MANAGEMENT GUIDELINES

2.1 General

Information technology resources are to be acquired, managed, and used in the manner most beneficial to Washington County Government (WCG) and its business operations.

2.2 Privacy Rights

All information contained in or communicated through WCG provided systems, regardless of by or to who sent or received, or however stored or filed, is owned by WCG. WCG reserves the absolute right, in its discretion, to monitor, access, and disclose all information accessed by, contained in or communicated through these electronic systems. As such, employees enjoy no expectation of privacy with respect to their use of WCG's electronic systems. Furthermore, from time to time, and whether as a part of the WCG's electronic retention policy, maintenance or otherwise, WCG reserves the absolute right to delete, erase, or otherwise dispose of any information contained within the electronic systems.

2.3 Use of Technology

WCG will strive to utilize the most advanced information technology resources and telecommunication solutions, but only when they prove to provide efficient and cost effective results as determined by the Board of County Commissioners (BOCC) and/or County Administrator and/or division director(s) and/or department head(s).

2.4 Management of Technology

The Information Technologies Director is responsible for the overall management of the Information Technology Management (ITM) Policy, as well as technology procurement, installation, inventory, security, usage, and monitoring. All technology procurement (i.e. hardware, software and related services, maintenance contracts, on- or off-site repairs, upgrades or modifications, etc.) will be performed using established WCG purchasing policy. It is the responsibility of the division director and/or department head to approve and monitor specific technology requests for hardware, software and related services for appropriateness.

2.5 Violations

Penalties for violating the Information Technology Management Policy will vary depending on the nature and severity of the specific violation. Any employee who violates this policy will be subject to disciplinary action as described in the Washington County Employee Handbook, including but not limited to counseling, reprimand, suspension, and/or dismissal from Washington County Government employment.

2.6 Information Technologies (IT) Project Priorities

Information Technologies prioritizes IT projects and/or activities into four categories. The highest priority will be assigned to the installation and support of WCG's enterprise business systems. The next priority will be given to the development, installation and support of divisional/departmental information technology initiatives and/or systems. The next priority will be assigned to individual employee requests. The lowest priority will be assigned to all projects and activities provided to non-profit agencies supported by WCG.

2.7 Guiding Policy Principals

The following principals are intended to guide, facilitate, and expedite the orderly implementation of information technology into WCG's business operations and are as follows:

- make information technology decisions based on business needs
- make sure that the technology infrastructure is stable and reliable
- share data and make it accessible (where permitted)
- establish standards and ensure compatibility

2.8 Annual IT Plan and Development Process

During the fiscal budget preparation process, it will be the responsibility of the department head to plan, budget and justify capital hardware, software and related service expenditures. IT will assist and support department heads in performing this task. Budgeting for non-capital hardware technology, software products and related services is not required, but is highly recommended.

After the fiscal year budget has been formally adopted by the Board of County Commissioners (BOCC), Information Technologies will schedule meetings with each division director and/or department head to discuss their IT related requirements and/or funded projects for the coming fiscal year. From this information, IT will develop a preliminary plan that consolidates and prioritizes these requirements based on criticality to operations, technical merit, and anticipated improvement to productivity, and/or service to our clients. This preliminary plan will then be presented to the County Administrator and senior management team for their review and consideration.

On approval by the County Administrator, this plan becomes the annual (fiscal year) working IT plan. The annual IT plan is implemented as financial and operational restrictions allow. Any needs that arise during the fiscal year will be incorporated into the plan and will be prioritized taking into consideration all needs previously submitted but not fulfilled as agreed upon by the County Administrator and senior management team.

2.9 Policy Review and Update

This overarching policy and each of the specific management policies shall be reviewed annually and revised as necessary, as directed by the IT Director. Revisions will then be submitted to the Information Technology Steering Committee for their review and comments and subsequently to the Board of County Commissioners for their approval.

3. ROLES AND RESPONSIBILITIES

3.1 Information Technologies Director

- Establishes IT Policy and the annual IT Plan and delegates oversight for carrying them out to IT staff.
- Resolves any conflicts regarding IT and telecommunications issues and/or equipment which are presented to the Director.
- Provides oversight and direction for present and future IT and telecommunications strategies within WCG.
- Provides oversight regarding the allocation of both IT and telecommunications resources.
- Assumes responsibility and accountability for all IT and telecommunication acquisitions made.
- Advises and assists division directors and department heads in strategic long-range planning, acquisitions, allocation and management of WCG's information technology resources, including all matters relating to this IT policy.

3.2 Information Technologies Staff

- Serves as the Director's representatives and spokes-persons on all aspects of the IT program within WCG including resources, oversight and management of all IT related activities.
- Provides technical expertise and advice to the IT Director for all decision making and planning associated with all Information Technologies activities.
- Develops, updates, and maintains long- and short-term goals, objectives, plans, and strategies, within the guidelines established by the Information Technology Management (ITM) Policy including disaster recovery planning and implementation.
- Reviews and recommends action to the Director on studies, analyses, and proposals related to the ITM Policy.
- Monitors implementation of this policy, identifying problems and deficiencies, and works to resolve them.
- Monitors the design and conduct of operational tests and evaluations of information systems acquired, developed, or installed for use at WCG in order to determine the effectiveness of these systems in meeting established requirements and design specifications.
- Reports to the Director on progress and performance in achieving planned goals and objectives.

- Develops necessary guidelines for the control, security, and dissemination of data from assigned systems, in compliance with Privacy Act and Freedom of Information Act regulations.
- Provides day-to-day technical support and expertise where required.
- Provides oversight and management of all WCG telecommunications equipment, services and support for both voice and data.

3.3 Division Directors and Department Heads

- Ensures their employees are aware of the Washington County ITM policy, as well as other County policies, and federal laws related to the use of IT resources; ensures that their employees are using information technology resources appropriately; and ensures that their employees participate in and complete appropriate security awareness training.
- Have the ultimate responsibility for the stewardship of information systems and data under their administrative control.
- On an annual basis, plan, budget and justify capital hardware, software and related service expenditures and discuss these IT related requirements and/or funded projects with IT for inclusion into the annual IT Plan.
- Reviews, approves, and submits to Information Technologies, additional divisional/departmental IT needs and requirements throughout the year for inclusion into the annual IT Plan.
- Reviews, approves, and submits to Information Technologies, proposals for design, development, and implementation of divisional/departmental applications prior to submitting to the IT Department for action.
- Designates divisional/department IT Coordinator and alternate and informs Information Technologies of any changes.
- Provides adequate (initial and ongoing) training programs for users of departmentally specific software applications and/or information systems, where applicable.

3.4 Information Technology Coordinators (ITC)

- Serve as the focal point for information technology management activities within the division/department.
- When directed by the division director/department head represents their division/department and coordinates division/department IT activities with Information Technologies.
- Informs the division director/department head of any pertinent information technology related issues and activities affecting their division/department.

3.5 All Employees

- Each employee of the County is responsible for maintaining the security of the equipment, the integrity of all databases, and the confidentiality of information relating to County business where required.
- Notwithstanding the County's monitoring and retention/destruction policies, each employee is responsible for the proper and ethical use of electronic devices and the contents of communications recorded in electronic systems.
- Employees are obliged to inform appropriate staff upon discovering foreign matters or security breaches.
- Each employee should also bear in mind that the ease and convenience of such electronic devices as a means of communication, either with one person or entity, or a group, does not reduce one's obligations, professionalism, and courtesy to others.
- Each employee shall read, review, and where applicable execute an Acknowledgement of Information Security Responsibility form and forward this completed form to the Human Resources department for inclusion in your personnel file.

3.6 Revision History

Adopted: November 21, 2006

4. SPECIFIC MANAGEMENT POLICIES

- 4.1 **Application Change Management Policy**
Adopted: 11/21/2006
- 4.2 **Data Management Policy**
Adopted: 11/21/2006
- 4.3 **Hardware Management Policy**
Adopted: 11/21/2006
- 4.4 **Software Management Policy**
Adopted: 11/21/2006
- 4.5 **Telecommunications Management Policy**
Adopted: 11/21/2006
- 4.6 **Systems and Electronic Communications Use Policy**
Adopted: 11/21/2006
- 4.7 **Access Control Policy**
Adopted: 11/21/2006
- 4.8 **Network and System Security Policy**
Adopted: 11/21/2006
- 4.9 **Documentation and Equipment Information Policy**
Adopted: 11/21/2006
- 4.10 **Information Technology Steering Committee**
Adopted: 11/21/2006

4.1 Application Change Management Policy

4.1.1 General

Change management is the planning, coordinating and controlling of the implementation of changes to the production (operational) environment and may be described as a process in which changes are successfully promoted to the production environment. The goal of change management is to implement changes to the production environment so that new services and service levels are provided to the customer but existing services and service levels are not affected by the application of the change to the system.

This policy establishes procedures and prerequisites for managing the application change process for non-COTS enterprise and departmental software systems utilized by Washington County Government (WCG). COTS is an acronym for commercial off-the-shelf which describes software or hardware products that are ready-made and available for sale to the general public. COTS products are designed to be implemented easily into existing systems without the need for customization and therefore are not required to be implemented using this policy. For example, Microsoft Office is a COTS product that is a packaged software solution for business.

Changes include the application of release/version upgrades and/or patches/fixes or software modification/enhancement developed by Information Technologies (IT) staff, or contract personnel.

The intent of these procedures is to:

- Assist in a clear understanding of, and agreement on, the role that different departments should play in the change process.
- Help users and developers (IT staff, contract personnel, etc.) understand and agree on appropriate steps in the change process.
- Increase the likelihood that application system changes will be effective (meet the needs of present and future users).

4.1.2 Procedures

1. A managing customer (division director, department head, or departmental IT coordinator) submits a project request to the IT staff person responsible for supporting their application. A project is defined as a software enhancement; vendor provided release, service pack or patch; or a problem resolution issue. Upon receipt of a project request, the responsible IT staff person arranges for both parties to meet and jointly determine if the project and any subsequent changes (technical and/or operational) are feasible and comply with existing policy and procedure. Project feasibility is generally determined by resource requirements (time, funding, staffing, etc.) weighed against the expected results.
2. The managing customer and the responsible IT support staff are then required to prepare a project description document. This document shall include:
 - a. project identification – is project a software enhancement; vendor provided release, service pack or patch; or a problem resolution issue

- b. project scope – describe the scope of the project to include any expected technical and/or operational changes and improvements
 - c. project resource requirements – identify all resources required, computer system(s) to be replaced and/or upgraded, funding sources, etc.
 - d. project collateral tasks – identify any interfaces to other computers systems that may require modification and identify possible impacts to information security (e.g. identification of new restricted data, new/changed access requirements, segregation of duties, etc.) as well as backup procedures and/or disaster recovery plans
 - e. project test plan – describe acceptance testing procedures and scripts, assign responsible parties
 - f. project training plan – a plan for training end users on new or modified functionality (where applicable)
 - g. project schedule - include project milestones and/or benchmarks that identify all responsible parties
3. The managing customer and the responsible IT support staff shall then forward the project description document to the Information Technologies (IT) Director for review and consideration. The IT Director may then request a meeting with both parties to review project scope, resource requirements, and departmental commitments before making a final decision. Due consideration shall be given to resource requirements, project scope, test environment requirements and preparation, and safeguarding unauthorized access to any personnel data contained in the proposed application in accordance with the provisions and guidelines of the Privacy Acts (HIPPA, Sarbanes/Oxley, etc.).
 4. If it is determined that the scope of the project is beyond the technical capabilities and/or capacity of IT to perform then a decision shall be jointly made to either abandon, postpone or seek the assistance of a third party vendor to complete the project. In the case of obtaining third party assistance, the managing customer, the responsible IT support staff, and the IT Director would jointly pursue the approval, procurement, and implementation for this option. Procurement documentation, technical specifications and vendor response documentation would then manage the project’s implementation and acceptance.
 5. For IT capable projects, the responsible IT staff person shall then develop a suitable problem resolution (where applicable) and subsequently prepare a set of technical performance characteristics called change requirements and submit them to the Database Administrator (DBA) for review and approval. Change requirements shall include the following:
 - a. project resolution- a description of how the project is to be suitably completed, include source code, table modifications, information security adjustments, version/release or release, service pack, patch/fix identification (where applicable)
 - a. project test plan – describe acceptance testing procedures and scripts, assign responsible parties
 - b. project training plan – a plan for training end users on new or modified functionality (where applicable)
 - c. project schedule - include project milestones and/or benchmarks that identify all responsible parties
 6. The DBA will review the change requirements document with the responsible IT staff person and prioritize the project according to the urgency of the request, the estimated effort, resources involved, and the foreseeable risks. On approval by the DBA, the DBA will then submit the change requirements document to the managing customer for their final approval.
 7. Once final approval has been given, the DBA will log the change and prepare for implementation of the change. The DBA will coordinate with the responsible IT staff person, who will be responsible for

ensuring that any operation changes that may be required occur in conjunction with the application of the change. The change will be applied according to the project schedule. Changes that require system downtime, the DBA will send out notice of the scheduled outage to all application users. The DBA will confirm with the responsible IT staff person, the managing customer, and system users when the changes have been applied and the system is again, available for use.

8. The DBA will require feedback from the users as to whether or not the change is working in the production environment. Providing feedback will be the responsibility of those personnel. Feedback should be provided via telephone or email. The DBA has the authority to determine whether or not a change should be rolled out of the production environment. If a change is rolled back, the problem with the change should be corrected by appropriate resources and the change management process shall be repeated.

4.1.3 Application Change Prerequisites

The following prerequisites establish eligibility requirements for software releases (versions), service packs (bundles), and independent patches (bug fixes to any release that the vendor has yet to “package” into a release (major, point, or service pack) to be applied to a production environment. Software releases are generally made available by the vendor in the form of a major and minor (point) release. Major releases are usually designated with a whole number designation (e.g. 8.0) and minor or point releases are usually designated with digits to the right of the decimal point and may also include alphabetic characters (e.g. 6.2, 4.91B). A service pack is an update to a software release that fixes existing problems or provides enhancements to the product that will appear in the next release of the product. When the new product version is released, it usually contains the fixes and updates from the service pack.

Major Releases

1. must be older than 90 days old as specified by the vendor’s release date
2. all available patches will be applied with the major release (patches do not have to be 90 days old)
3. Upon notification of a major release by a vendor, the responsible IT support staff will communicate via email the availability of the release to the DBA and all managing customers. This email will include, as an attachment, all pertinent vendor provided release documentation.
4. During the minimum 90 day wait period it is expected that the responsible IT support staff and the managing customer will review all release documentation in detail and cooperatively develop test plans based on critical business processes and changes to the release. They will also be expected to begin plans for training end users on the release function.
5. Because the change management process requires extensive testing and signoff from users before promoting a release into production, IT will not rollback to a previous release level once a release is in production.

Minor Releases

1. must be older than 45 days old as specified by the vendor’s release date
2. all available patches will be applied with the minor release (patches do not have to be 45 days old)
3. a point release will not be applied within 30 days of a major release unless it contains mandated or regulatory required function

4. Upon notification of a minor release by a vendor, the responsible IT support staff will communicate via email the availability of the release to the DBA and all managing customers. This email will include, as an attachment, all pertinent vendor provided release documentation.
5. During the minimum 45 day wait period it is expected that the responsible IT support staff and the managing customer will review all release documentation in detail and cooperatively develop test plans based on critical business processes and changes to the release. They will also be expected to begin plans for training end users on the release function.
6. Because the change management process requires extensive testing and signoff from users before promoting a release into production IT will not rollback to a previous release level once a release is in production.

Service Packs and Patches

1. Service packs and patches will be applied on a case by case basis on the mutual consent of the responsible IT support staff and managing customer.

4.1.4 Planning and Performing Project Acceptance Testing

The purpose of testing is to ensure that there are no surprises in store for a department when change is applied to the production environment. Departments who are operating in the production environment are required to perform acceptance testing. Acceptance testing shall be performed on the application software module specific to the department as well as the general module if the general module impacts the department. Managing customers are responsible for ensuring that their department completes acceptance testing as specified in the project test plan. Recommended tasks for acceptance testing include:

1. Review vendor provided release* notes for new and changed business processes and/or function that will be required or desired for use by WCG.
2. Identify business processes that are changed in the release that may have been previously customized by IT or a third party vendor.
3. Keep a list of critical business processes that should always be tested when a new release is being applied.
4. Document the business processes in 1, 2 and 3 above and determine how you want them to work within the new release.
5. Set up test scripts and/or create a series of tests to validate standard transactions, reporting, batch processes, and key infrequent processes (e.g. month-end, quarter-end, year-end, etc.) are working as expected, assign personnel responsible for performing these tasks, perform the tests, and document the results. This step cannot be performed until the release and all available patches have been applied to the test environment and any desired previously customized code has been resynchronized.
6. Prepare test environment by cloning the production environment. Then apply the release over the clone environment followed by the application of all available patches and/or fixes. Test data sets shall conform to Data Management Policy guidelines and specifications.
7. Perform iterations of each business process to determine that each works as expected.
8. Verify that user access privileges are maintained or modified per information security requirement.
9. Verify that any identified impacts to information security (e.g. identification of new restricted data, new/changed access requirements, segregation of duties, etc.) as well as backup procedures and/or disaster recovery plans have been addressed and successfully tested where applicable.

Upon completion of acceptance testing the managing customer will be required to sign off that the change is acceptable to them. They may do this by sending an email to the DBA.

4.1.5 Planning Change Training

The purpose of change training is to ensure that users of an application software module are familiar with the new business function supplied in the change prior to those users being required to perform those functions in the production environment. There are no specific requirements for completing change training. Departments that are operating in the production environment and have functional changes made in a software release must perform change training. Recommended tasks for change training are:

1. Review vendor provided release* notes for new and changed business processes and/or function that will be required or desired for use by WCG.
2. Identify business processes that are changed in the release that may have been previously customized by IT or a third party vendor.
3. Identify the personnel who will be responsible for performing those business processes to include a review of segregation of duties among these identified personnel.
4. Identify the magnitude of the changes. Training should be proportional to the magnitude of change where large changes may require a formal classroom setting and minimal changes may be delivered via an email communication and/or attachment.
5. After release testing is complete, deliver appropriate training to your users. Announce to them the effective date of these changes and what will be expected of them.

***Note: release may refer to release (major, minor), service pack and/or patch**

4.2 Data Management Policy

4.2.1 General

Washington County Government (WCG) owned information (hereafter county data) must be managed, used and protected in accordance with federal and state law and WCG policy so as to ensure its integrity, availability, privacy and confidentiality. Each employee, agent, or affiliate of WCG, who handles county data for the purpose of performing his or her job duties, or other functions directly related to his or her contractual affiliation with WCG, is a steward of county data and is responsible for the proper handling of county data resources under his or her control. County data is all data owned by WCG that are prepared, supplied, used, or retained by WCG employees, within the scope of their employment, or by agents or affiliates of WCG, under a contractual agreement. Some examples of types of county data are payroll, personnel, financial, land, facilities-related, gaming, and tax. County data can be contained in any form, including but not limited to documents, spreadsheets, databases, email, and Web sites; represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof; communicated in any form, including but not limited to handwriting, typewriting, printing, photocopying, photographing, and Web publishing; and recorded upon any form, including but not limited to papers, maps, films, prints, disks, drives, memory sticks, and other devices.

Data in their many forms are one of WCG's most important assets. In every area, and at every level of WCG, employees, agents, and affiliates of WCG are managing or using county data. As with other assets, (i.e., financial, physical) managing data requires each of us to take responsibility for its reliability and security. The integrity of data must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. While we cannot perfectly protect data, we can implement responsible management practices that improve both the confidentiality and accuracy of our data while reducing overall risk and liability to individuals, departments and WCG.

This policy describes the proper management, use, and protection of county data. It is intended to foster clear accountability, increase the effectiveness of data administration, reduce risk from potential threats, and minimize legal exposure and liability associated with the improper use of county data. It articulates data stewardship roles and responsibilities and establishes procedures for carrying out those responsibilities.

The guiding principles for this policy are:

- County data are an essential and valuable asset whose proper management and use is instrumental to organizational effectiveness and efficiently managed resources. The proper exchange of data increases and improves planning, decision-making, and accountability.
- WCG operates under the general assumption of the free flow of information, giving all WCG employees, agents, and affiliates access to information to which they have a legitimate right, except in cases where it is specifically restricted by law, WCG policy, or as a result of a risk determination by a Data Proprietor.
- WCG is committed to the development of an integrated and collaborative data environment using Web-enabled technologies to maximize access to data and to improve the exchange of needed information across WCG.
- The privacy and security of restricted data is of paramount importance.

- All data are not the same, and must be treated differently based on levels of sensitivity and criticality.
- Different levels of data access and security must be established for various constituencies, including but not limited to WCG employees, agents, affiliates, and the general public.

4.2.2 Roles and Responsibilities

By articulating data stewardship roles and responsibilities, this policy assists WCG employees, agents and affiliates to identify their roles(s) in the relationship to the data in their custody, and determine what actions are required in order to fulfill their duties for managing and protecting the data.

Data Proprietors (division directors, department heads, or other designated supervisory employee having the ultimate responsibility for the stewardship and determining the purpose and function of county data under their control):

- Promote best practices for the management, use, and protection of WCG data based on pertinent regulations and policies.
- Document the specific criteria (law or policy) that apply to the designation of certain data as restricted.
- Oversee the accuracy, integrity, and integration capability of data generated under their direction.
- Ensure that staff is adequately trained in proper data management, use, and protection, in accordance with the training guidelines in the Procedures section of this Data Management Policy.
- Specify adequate data retention in accordance with applicable records retention policy.
- Communicate requirements (e.g., use, security, disclosure, disposition, etc.) to users of the data.
- Perform departmental/unit risk assessments to ensure that access and security requirements and disaster recovery plans are properly implemented and tested.

Data Users (WCG employees, agents, and affiliates granted authorization to access or create county data and who invoke or access data for the purpose of performing their job duties or other functions directly related their affiliation with WCG):

- Learn, understand, and comply with all WCG policies, procedures, guidelines, and standards governing the use of the data they are handling.
- Access data only in the performance of assigned duties.
- Use data for authorized purposes only.
- Accurately prepare, use, and retain data.
- Understand the sensitivity levels of the data they are using.
- Respect the confidentiality and privacy of individuals of whose records they access.
- Protect data from unauthorized changes.
- Ensure that appropriate security protocols are in place when viewing and storing restricted data.
- Protect restricted data from inadvertent and unauthorized access during transmission or downloading.
- Report violations of WCG policy to appropriate supervisory personnel for investigation and review.

Data Custodians (Information Technologies Department staff, agents, or affiliates that function as a technical partner and are responsible for the implementation of information systems and the technical management of data resources):

- Ensure the integrity of data resources under their supervision and/or care.
- Establish and implement standards and procedures to ensure that all data resources are managed consistent with the needs and requirements set forth by the Data Proprietor. These procedures may include, but not limited to, implementing business rules, following a security plan or protocol, managing the flow of data, implementing changes to data, providing and executing appropriate back-up procedures, and meeting data retention requirements.
- Establish security standards and procedures for systems, applications, and data, following the level of access security identified by the Data Proprietor.
- Implement, at the direction of the Data Proprietor, a disaster recovery plan for data resources deemed essential and for the preparation and general oversight of the performance of a disaster recovery in the event of a disaster.
- Protect data from unauthorized change, destruction, or disclosure, whether intentional or accidental.
- Protect restricted data from inadvertent and unauthorized access during capture/creation, transfer, storage, viewing and destruction.
- Ensure the destruction of restricted data by third party vendors upon the completion of data-sharing arrangements with vendors.
- Read, review, and execute appropriate Privileged Access Agreement(s).

4.2.3 Data Sensitivity

Data sensitivity is a risk characteristic used to assess the level of access and security controls required to protect data. Data falls into two levels of sensitivity: restricted and unrestricted (most WCG data is unrestricted).

Restricted data is all data to which use is restricted by federal or state law or WCG policy; or data that a Data Proprietor has designated as protected from general access or modification, even if such access may not be prohibited by federal or state law or WCG policy. Types of restricted data include, but are not limited to, data that identifies or describes an individual and data to which unauthorized access, modification, or loss could seriously or adversely affect WCG, its employees, or the public. Examples of restricted data include social security number, employee home address, and date of birth, financial information such as bank account number or credit card number, and responses to a Request for Proposal (RFP) before a decision has been reached by the Board of County Commissioners (BOCC).

Unrestricted data is all data to which access or modification is not restricted by federal or state law or WCG policy and to which access is permitted by the Data Proprietor. Examples of data that are unrestricted include data contained WCG financial reports, general divisional and/or departmental published information, and information made available through WCG's web site.

4.2.4 Procedures

This section describes procedures meant to assist divisions and departments in executing their data stewardship responsibilities through physical, logical and managerial measures. All divisions, departments and individuals are encouraged to follow these recommended procedures.

A. Data Collection and Control

Data collection and control involves controlling the processes of data capture/creation, transfer, storage, viewing/editing, security, and destruction. Implementation of data control techniques is critical to successful management of information technology resources and includes the following elements:

1. Data capture/creation and quality control - will be the responsibility of those individuals directly involved with the work process being automated and application design will enable data elements to be entered only once and as close to the data source as possible.
3. Data storage - generally speaking, end user data will be stored on the network as opposed to the local PC hard drives, CDs, or diskettes for purposes of data retrieval and security. End users will not create hidden or password protected directories or files.
4. Data editing - data verification, editing, error identification, correction, and updating will be performed by machine and/or software application after entry.
5. Data viewing, transfer and security - data access, retrieval and/or transfer will be provided to those individuals who have a valid need for the data without regard to their divisional affiliation and with due regard to rights of individual privacy, data security, and WCG policy.
6. Data destruction – the proper disposal and destruction of data (restricted and unrestricted) in any media or form shall be performed per the agencies Records and Retention and Disposal Schedule as authorized by the State Archivist.

B. Data Management

Data Proprietors are required to:

1. Conduct risk assessments to identify data resources that are “restricted” or “essential” and require protection; to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability; and to communicate security requirements for departments and individuals to follow. Risk assessments should take into account the potential adverse impact on the County’s operations and assets. Risk assessments should be conducted by teams composed of appropriate managers, IT staff, and other personnel associated with activities subject to assessment. WCG will attempt to provide risk assessment guidance and tools.
2. Keep a log of access rights assignments in each department. Review and update log annually.
3. Keep a log of restricted data elements in use in each department. Review and update the log annually.
4. All data should be backed up on a scheduled basis as appropriate to the data. In cooperation with IT, develop, document, and implement a back up schedule sufficient to satisfy disaster recovery requirements.

5. Periodically review the system administration work performed by employees (IT support staff, departmental system administrators) with access to privileged system administration accounts on shared servers (requires executed Privileged Access Agreement).

C. Restricted Data

As a practical matter, there is no single or common prescription for the protection of personal or restricted data. Technical challenges are more difficult than might appear and security regulations and tools are constantly changing. The following are basic practices that must be adhered to when handling personal or restricted data.

1. Information systems should not include restricted information unless absolutely necessary. These data elements are often protected by law, or sometimes by WCG policy. Examples of restricted data elements include social security numbers, employee home addresses, date of birth, and financial information such as bank account number or credit card number, and responses to a Request for Proposal (RFP) before a decision has been reached by the Board of County Commissioners (BOCC).
2. Do not store restricted data on workstations, laptops or portable computing devices and storage devices unless absolutely necessary. If restricted data must be maintained on such devices, do so only on a temporary basis and employ protective measures, such as encryption, to safeguard the confidentiality or integrity of the data in the event of theft or loss of the equipment. Permanent copies of restricted data should never be stored for archival purposes on workstations or portable equipment.
3. Do not email restricted data, either in the body of an email or as an attachment, unless encrypted. Email is not a secure form of communication. Additionally, the email recipient may have a less secure computer or may elect to forward the information to another person who should not receive the restricted data.
4. Never leave restricted data exposed on unattended computer screens or leave computer screens unattended without appropriate screen access controls.
5. Delete information that personally identifies an individual when there is no longer a business need for its retention on computing systems.
6. Redact personal or restricted information not critical to the task when distributing full data sets to downstream users.
7. When personal or restricted information is included in the distribution of data to any downstream users, include notification of that fact, including reference to applicable policies and regulations (Health Insurance Portability and Accommodation Act (HIPAA), etc.).
8. Be prepared in advance to notify individuals immediately if data about them has been compromised.

D. Vendor Relationship

When passing data or providing data access to a third party agent of WCG, be sure to do so with a written contractual agreement (including terms and conditions) that provides, at a minimum for:

1. disallowance of disclosure by the agent or affiliate to other third parties including subcontractors
2. the requirements that all agents and affiliates must observe the laws and policies required of WCG for privacy and security, including federal and Maryland law and WCG policies
3. a specific plan by the agent or affiliate for the implementation of logical, physical, and managerial security strategies
4. a specific plan for the destruction of restricted data upon completion of the agent's or affiliate's work for WCG

E. System Development

When designing a new system, modifying an existing system, or performing system acceptance testing, consider the following issues.

1. Define data elements so they are consistent with other data elements present in other WCG information systems.
2. Restricted data elements should never be used as the “key” to a system. For example, if maintaining a listing of employees, never select social security number as the key field.
3. When designing databases, use naming conventions with documentation that easily identify restricted data (e.g. “SSN” as opposed to “Employee Code” for social security number), so that technical staff and downstream users can readily determine the presence of restricted data in the data they are managing or using.
4. Do not maintain actual data in a test or development environment; rather, “mask” the restricted data such as social security number with dummy information.

F. Training

It is the responsibility of the division director and department head to ensure that each person within their administrative purview who has access to county data is adequately trained in the proper management, use, handling, and protection of data in their custody. Training should minimally include the employee's review of each of the specific management polices contained in the Information Technology Management (ITM) Policy, departmental procedures and if applicable, regulations governing specific restricted data (HIPPA, etc.)

4.2.5 Backup and Recovery

Backups are performed on the county data production environment to mitigate the risks associated with data loss and system downtime that could result from the corruption of data, programs or operating systems. IT staff schedules and verifies automated daily backup jobs that backup county data residing on

networked file and application servers (downtown core and remote site locations) to disk and/or tape media. These backups may consist of a full backup, incremental backup, database instance backup, and special requested backups. IT uses disk to tape, disk to disk, and BrightStor ARCserve Backup software for Windows technology to provide backup services.

Recovery is the process of restoring data, programs or operating system files from backup media (disk, tape) to a server or workstation in the event of corruption or loss. The general recovery procedure is as follows:

1. Initial notification will include IT Service (email support address), IT support staff and the appropriate Data Proprietor. IT staff may include the IT Director, DBA, Network Engineer, Senior Technical Support Analyst, and the IT staff person responsible for supporting the affected system.
2. The above personnel will determine the scope and type of corruption as well determine and plan the best corrective action. Generally, the IT staff person responsible for supporting the affected system will manage the corrective procedure.
3. Determine whether or not the system will be available during the corrective procedure and if not, approximate the downtime and notify those affected.
4. IT technical support will secure and verify the hardware.
5. IT will save the existing data if possible.
6. IT will secure the appropriate backup.
7. IT will load the backup to the appropriate server and initialize media restore procedures.
8. IT will ensure that the restore has completed successfully and verify data recovery.
9. IT and the appropriate Data Custodians will test the “restored system” to ensure the system is once again working properly.
10. IT will notify those affected that the system is once again available for use.
11. IT will review the occurrence of the corruption and attempt to prevent further reoccurrence.

4.2.6 Violation of Policy and Misuse of Data

Violations of this policy include, but are not limited to; accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedure, or other relevant regulations or laws; inappropriately altering, damaging, or destroying data; inadequately protecting restricted data; or ignoring the explicit requirements for the proper management, use, and protection of data resources.

Penalties for violating the Data Management Policy will vary depending on the nature and severity of the specific violation. Any employee who violates this policy will be subject to disciplinary action as described in the Washington County Employee Handbook, including but not limited to counseling, reprimand, suspension, and/or dismissal from Washington County Government employment.

4.3 Hardware Management Policy

4.3.1 General

Computer hardware and technology is an indispensable work tool used in every department at Washington County Government (WCG) and it is essential that this technology support the business processes and applications utilized in each department. This policy describes an orderly approach to managing WCG owned computer hardware and technology (purchases, upgrades or replacements).

4.3.2 Ownership

All computer hardware and technology acquired for or on behalf of the Washington County Government (WCG) or developed by WCG employees or contract personnel on behalf of WCG are and shall be deemed WCG property. All WCG owned computer hardware and technology is therefore eligible for subsequent upgrade, replacement, and technical support over its effective life, as outlined in this policy. Additionally, all such computer hardware and technology shall be used in compliance with applicable licenses, notices, contracts, and agreements.

4.3.3 Procurement of Hardware and Related Services

The procurement ordering of all computer hardware, technology, and related services shall be handled exclusively by or in collaboration with the Information Technologies Department to ensure that all purchased equipment conforms to WCG computer hardware and technology standards and is purchased at the best possible price following established WCG purchasing policy. Computer hardware, technology, and related services may not be purchased for WCG by employees privately from funds, such as petty cash or credit card, without the prior authorization from Information Technologies and the department head. **All requests for hardware acquisition and/or installation must be approved by the department head.** Such requests must be forwarded via email or inter-office mail to **IT Service** (IT Service is an administrative mailbox used for receiving and monitoring IT related service requests) and/or the Senior Technical Support Analyst. The Senior Technical Support Analyst is responsible for computer hardware, technology, and related services procurement ordering, inventory and subsequent installation.

Examples of hardware and related services include but are not limited to:

- Desktop computers and peripherals (mouse, printer, keyboard, memory, monitor, wireless peripherals, etc.)
- Laptop, notebook, tablet, PDA computers
- Networking equipment and services (cables, cabling systems, connectors, interface cards, hubs/switches, routers, fax/modems, wireless networking technology (voice, video, data), remote access, VPN and SSL technologies, web domain hosting/registration and ISP services, firewalls, proxies and web appliances, etc.)
- Telecommunications equipment and services (telephone hand/head sets, Nortel or telephony equipment, frame relay, DSL, ISDN, POTS, etc.)
- Servers, terminal servers, print servers, DHCP servers, web servers (WWW, DNS, e-mail), network security and intrusion detection systems
- Auxiliary data storage systems (SAN, NAS, hard drives, tape systems, flash keys, USB and zip drives,

- etc.)
- Battery backup and uninterruptible power systems
- Digital imaging technology (digital cameras, scanners, projectors, plotters, etc.)

4.3.4 Replacement Strategy

Computer hardware and technology has an effective life in specific installations and is planned for replacement generally on a five year cycle. Additionally, replacement and/or upgrade may occur prematurely if the installed hardware and/or technology becomes a barrier to the user or other business requirement(s) dictates it (such as sought after functionality enhancements or new features). This replacement primarily happens when a required business software application or suite will not run effectively on the existing hardware platform or a sought after functionality/feature enhancement requires an upgraded or new hardware platform.

When replacing and/or upgrading computers and/or computer technology the strategy is to upgrade to a faster, more advanced computer and/or computer technology with increased capabilities and robustness and with enough technical capacity to support the user through the entire life cycle. Consideration is also given to the type of work being done, the type of software being used, and the demands of the applications used. The minimum standard platform by which WCG manages its upgrade strategy is transitory in nature and follows standards set by overall IT infrastructure requirements for operating systems, enterprise and departmental application systems, file sharing, e-mail, network architecture, current industry standards, and applicable hardware vendor specifications.

4.3.5 Replacement and Upgrade Budgeting

During preparation of Information Technologies' fiscal year budget request, IT technical support staff reviews WCG's computer technology inventory and identifies all units eligible for replacement. A decision is then made to either replace or upgrade all eligible units based on recommended minimum hardware configuration, technology availability and feasibility, and operational efficiency. Replacement costs are prepared and inserted into Information Technologies' fiscal year budget request; therefore, division directors and department heads generally do not budget for replacement eligible (end of life cycle) computers and/or computer technology.

4.3.6 Budgeting for Capital Projects and New Positions

It will be the responsibility of the department head to plan, budget and justify departmental capital project expenditures for computer technology hardware and related services. Capital projects are projects that require funding in excess of ten thousand dollars which may include new departmental technology initiatives, major enhancements and/or upgrades to a current system, application or business process. Additionally, if a New Position Request is included in the department's fiscal year budget request and it is expected that the individual in the new position will need access to computing and/or telecommunications technology then the departmental budget request shall include funding to acquire the necessary equipment (computer, telephone, appropriate software license(s), or other tools and technology). Information Technologies will assist and support department heads in performing these tasks. Please note that

budgeting for non-capital computer technology hardware and related services is not required, but is highly recommended.

4.3.7 Replacement Process

In an effort to balance the need to upgrade with the negative effects of replacement on the end user, the procurement, inventory and subsequent installation of computers and/or computer technology must be orderly and planned in advance. IT technical staff will work directly with department heads or their designated IT Coordinators to provide notification of procurement and to schedule a mutually convenient time for the installation of all replacements and/or upgrades.

4.3.8 Refresh Process

In the event that an employee leaves WCG employment, IT technical staff will work directly with department heads or their designated IT Coordinators to schedule an inspection of the employee's computer and peripherals and where applicable, repair, replace, upgrade, and/or perform an operating system refresh/reformat prior to the replacement's start date. This inspection should be scheduled and all work completed within ten (10) business days after the employee's effective termination date.

4.3.9 Recycling Computers and Technology

Computers and computer technology are the property of WCG and are provided as tools to support the County's mission. When a computer or computer technology is replaced, it becomes available for reassignment to other uses or may be prepared for non-profit organization donation or appropriate disposal.

4.3.10 Hardware Installation, Maintenance and Technical Support

Information Technologies staff is responsible for installing, maintaining and supporting all hardware purchased for the benefit of WCG. Computer technology hardware and related service vendors may also provide installation, maintenance and technical support. Other technically qualified WCG employees may also provide installation, maintenance and technical support; however, only at the direction and coordination with Information Technologies technical support staff. It will be the responsibility of the department head to plan and budget for annual technical support and hardware maintenance fees (annual maintenance contracts and/or agreements) for departmentally specific hardware platforms, where applicable. Information Technologies will assist and support department heads in this task and assist in planning for subsequent hardware upgrades as deemed appropriate or required. Requests for maintenance and/or technical support services should be sent via email to **IT Service** or directly (phone and/or email) to the Senior Technical Support Analyst. The Senior Technical Support Analyst is responsible for managing maintenance and technical support services.

4.3.11 Non-County Owned Computer Hardware

Due to a variety of security issues and possible liabilities, computer hardware and/or technology that is not owned by the County (e.g., computer hardware that is an employee's personal property) **shall not** be plugged into the County's network or linked to any computing system without the **prior approval** of the Information Technologies (IT) department. Non-County owned computer hardware and technology is not eligible for IT provided assistance, maintenance and/or technical support unless otherwise directed by the Board of County Commissioners (BOCC) or the County Administrator.

4.4 Software Management Policy

4.4.1 General

Washington County Government (WCG) is committed to managing its software assets for maximum benefit to the organization and its employees and will provide copies of legally acquired software to meet all legitimate business needs and in sufficient quantities. Please note that the use of software obtained from any other source could present security and legal threats to WCG, and such use is strictly prohibited.

4.4.2 Ownership

All software acquired for or on behalf of Washington County Government (WCG) or developed by WCG employees or contract personnel on behalf of WCG is and shall be deemed WCG property. All such software shall be used in compliance with applicable licenses, notices, contracts, and agreements.

4.4.3 Software Manager

It is the policy of WCG to respect the rights of others in computer software and to adhere to the terms of all software licenses, notices, contracts, and agreements to which WCG is a party. The Information Technologies (IT) Director (or his/her designee) is WCG's Software Manager, and is charged with the responsibility for enforcing these guidelines.

4.4.4 Procurement of Software and Related Services

The procurement ordering of all commercial software and related services or the acquisition of all Open Source Initiative licensed software products such as shareware or freeware shall be handled exclusively by or in collaboration with the Information Technologies department to ensure that all software applications are compatible and capable of executing on existing computer hardware technology, conform to WCG software standards and are purchased at the best possible price following established WCG purchasing policy. Software may not be purchased for WCG by employees privately from funds, such as petty cash or credit card, without the prior authorization from Information Technologies and the department head. Software acquisition channels must be restricted to ensure that WCG has a complete record of all software that has been purchased and installed on WCG computers and can register, support and upgrade such software accordingly. **All requests for software acquisition and/or installation must be approved by the department head.** Such requests must be forwarded via email or inter-office mail to **IT Service** (IT Service is an administrative mailbox used for receiving and monitoring IT related service requests) and/or the Senior Technical Support Analyst. The Senior Technical Support Analyst is responsible for software and related services procurement ordering, inventory, and subsequent installation.

Examples of software and related services include but are not limited to:

- Operating systems (Windows, Linux, UNIX, virtualization, etc.)
- Business applications (Microsoft Office, Word, Excel, PowerPoint, Access, personal organizer,

- business intelligence, e-commerce, document management, etc.)
- Utility (backup, cloning, systems management (disk, desktop, patch), OCR, FAX, multi-media, etc.)
 - Development (Visual Basic, C++, COBOL, Perl, Java, SQL, XML, database, database tools, interpreters, compilers, etc.)
 - Graphics (Adobe, CAD/CAM, GIS, etc.)
 - Malware/Security (anti-virus, anti-spyware, anti-spam, firewall, threat management, etc.)
 - Internet/Web (e-mail, browser, web tracking, web development and management, etc.)
 - Network (network utility, monitors, sniffers, IDS/IPS, VPN, bandwidth management, etc.)
 - Open Source Initiative (OSI) approved licenses (freeware, shareware, non-commercial, etc.)

4.4.5 Budgeting for Software

It will be the responsibility of the department head to plan, budget and justify departmental capital software and related service expenditures. Capital software is software and software related services that require funding in excess of ten thousand dollars which may include new departmental technology initiatives, major enhancements and/or upgrades to a current system, application or business process. Information Technologies will assist and support department heads in performing this task. Budgeting for non-capital software products such as COTS products and related services is not required, but is highly recommended. COTS is an acronym for commercial off-the-shelf which describes software or hardware products that are ready-made and available for sale to the general public. COTS products are designed to be implemented easily into existing systems without the need for customization. For example, Microsoft Office is a COTS product that is a packaged software solution for business.

4.4.6 Registration of Software

Software shall be delivered to the Software Manager to complete registration and inventory processing prior to software installation. The Software Manager is responsible for registering the software. Software shall be registered to Washington County Government and/or Washington County Government and department name (in which it will be used). Because of personnel turnover, software shall never be registered in the name of an individual user. The Software Manager shall maintain an inventory of software licensed by Washington County Government to include appropriate purchasing records.

4.4.7 Software Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on WCG owned computers and/or technology. Information Technologies will assist employees in understanding their legal responsibilities and obligations, and provide further clarification upon request. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of this policy.

4.4.8 Duplication and Distribution of Software

The unauthorized duplication of copyrighted software or documentation is violation of federal law and is contrary to established standards of conduct for Washington County Government employees. WCG employees may not duplicate any licensed software or related documentation unless expressly authorized to do so by applicable licenses, notices, contracts, and agreements. Additionally, WCG employees may not provide copies of software to others unless expressly authorized to do so by applicable licenses, notices, contracts, and agreements. Employees may use software on local area networks or on multiple machines only in accordance with applicable licenses, notices, contracts, and agreements.

4.4.9 Employee Software Training

It will be the responsibility of the department head to assure that their employees receive appropriate software training. Training opportunities may be obtained from in-house resources; traditional educational/training venues or web based training vendors. Upon completion of this training, employees that participated may be required to sign a training acknowledgment, which will be incorporated into his/her personnel file.

4.4.10 Installation of Software

After the registration requirements have been met, personnel assigned to the Information Technologies (IT) department will install the software. Software and related service vendors may also provide installation, configuration and implementation services in collaboration with IT staff. Manuals, tutorials, and other user materials will be provided to the user as deemed appropriate by the department head. Once the software is installed, the original media shall be kept in a safe storage area maintained by the Software Manager.

4.4.11 Software Maintenance and Technical Support

The Information Technologies department is generally responsible for installing, maintaining and supporting all software purchased for the benefit of Washington County government. Software and related service vendors may also provide on-going maintenance and technical support. It will be the responsibility of the department supervisor to plan and budget for annual technical support, software maintenance, and subsequent software upgrade fees and related costs for departmentally specific business software applications and/or systems. Information Technologies will assist and support department heads in performing this task.

4.4.12 Open Source Initiative (OSI) Software

OSI software is software whose source code is available under a copyright license (open-source license) that permits users to study, change, and improve the software, and to redistribute it in a modified or unmodified form and is generally available through on-line systems and the Internet. Registration of OSI

products should be handled the same way as commercial software products and shall be used in accordance with any applicable license.

4.4.13 Periodic Audits and Policy Violation

The Software Manager will conduct periodic audits of all WCG owned computers and related equipment to ensure that WCG is in compliance with all licenses, notices, contracts, and agreements and in sufficient quantities. Such audits may be unannounced and without prior notice. During the audit process, IT staff or software auditor may search for any unauthorized software packages and eliminate any that are found. Failure to cooperate with any such audit or any other provision in this policy will be grounds for disciplinary action up to and including termination. Unauthorized use or duplication of software may subject employees and WCG to both civil and criminal penalties under federal law. Furthermore, employees who knowingly violate this policy will be subject to disciplinary action up to and including dismissal from County employment.

4.4.14 What is the Federal Law?

The US Copyright Act, found at Title 17 of the US Code, automatically protects software from the moment of its creation and fixation in tangible form. Except for the rights to *(i) copy the software onto a single computer* and *(ii) make “another copy for archival purposes only,”* which are provided in the act (Section 117), any other use without the permission of the copyright owner is prohibited.

The US Copyright Act also gives exclusive rights to the copyright owner, namely to *“reproduce the copyrighted work”* and *“to distribute copies ...of the copyrighted work”* (Section 106). The right of reproduction includes making copies of software in any format. The exclusive right of distribution includes any sales, lease, rental, or transfer of such copies. The right of distribution also includes the exclusive right to offer to transfer copies, regardless of whether payment is received. Moreover, it embodies distribution by any means, including electronic distributions via the Internet and other networks.

The US Copyright Act also states that *“anyone who violates any of the exclusive rights of the copyright owner...is an infringer of the copyright”* (Section 501). This section proceeds to list several penalties for this infringement, including liability for damages suffered by the copyright owner plus any profits of the infringer that are attributed to the copying, or statutory damages of up to US \$150,000 for each work infringed, in addition to recovering attorney’s fees from the infringer. The unauthorized copying and distribution of software is a federal crime if done *“willfully and for the purpose of commercial advantage or private financial gain.”* This includes the receipt of anything of value, like bartered software, or willfully making multiple copies with a value of more than US \$1000. Criminal penalties include fines of as much as US \$250,000 and jail terms of up to five years.

4.5 Telecommunications Management Policy

4.5.1 General

This policy establishes and defines the areas of responsibility for the provision and management of coordinated telecommunications services that support the business operations of Washington County Government (WCG). Telecommunications refers to any technology, service, system, or other resource that provides or ensures transmission of electronic data and information. Telecommunications resources may be voice and data networks, telephones, wireless services, messaging and directory services, high speed data communications, facsimile devices, personal digital assistants, network servers, routers, switches, or any other device, service, or system used in the transmission of electronic communication, including the connectivity to and between devices.

4.5.2 Telecommunication Services Provision and Management

Information Technologies (IT) is responsible for providing telecommunications transport services and infrastructure and coordinating the development and procurement of telecommunications equipment, systems and services for Washington County Government (WCG). **This includes but not limited to:**

- voice and data twisted pair (UTP/STP) network cabling systems (new construction/renovations)
- fiber infrastructure within and between WCG owned buildings (new construction/renovations)
- voice and data networks
- local dial tone
- private branch exchange (PBX) analog and digital services, calling features including PBX fax option
- long distance services
- voice and video conferencing
- telephone equipment and instrumentation
- directed add, moves, or changes
- wireless technologies
- email and voice mail (PBX)
- high capacity data and circuit services (frame relay, DSL, ISDN, T-1,etc.)
- coordination of in-house or vendor provided maintenance services (repairs, outages, upgrades)
- coordination of blue, white, and yellow page directory listings

Please note that the management and oversight of cellular telephones and related services is addressed in Washington County Policy P-6, Cellular Telephones and Services and therefore management of cellular telephones and related services are excluded from this policy.

4.5.3 Telecommunication Services Usage and Charges

It is the responsibility of each department and respective department head to verify that telecommunication services are being used responsibly and in accordance with WCG policy and to budget and pay for all incurred departmental expenses. **These expenses include but are not limited to:**

- non-recurring charges (costs for telecommunication vendor provided equipment, products or services that are added, installed, modified, or relocated)
- recurring monthly and/or annual charges (costs for telecommunication vendor provided products or services such as dial tone, long distance services, high capacity data and circuit services, pro-rated PBX ISDN trunk line expenses, directory service advertising (yellow pages), etc.)

4.5.4 Requests for Service or Assistance

Requests for non-critical telecommunications service or assistance should originate from the department head or the department Information Technology Coordinator (ITC) and may be submitted via telephone, inter-office mail, or email. The preferred method for sending non-critical requests is via email to **IT Service**. IT Service is an administrative mailbox used for receiving, scheduling, and monitoring IT related service requests. Non-critical requests generally involve new product(s) procurement, data networking enhancements, network access and/or application privileges, wiring or connectivity installations, equipment or telecommunication service additions, deletions, moves, and/or changes to existing telephone equipment and services.

Critical requests are given top priority and generally involve telecommunications service failures, outages, or malfunctions. These requests may be submitted to IT using the most convenient method available and by any employee affected. In the event of an outage, Information Technologies will notify the affected division/department personnel as to the cause of the outage and the anticipated time service(s) will be restored. Additionally, IT will provide timely updates where applicable.

4.5.5 Trouble Reporting

Any employee experiencing telecommunications problems should first report the trouble to Information Technologies and provide a full description of the nature of the problem, including the name of the person experiencing the problem, and which telephone, computer, or application the problem was experienced on.

Problems are generally those that include:

- low transmission quality
- noise (hissing and static)
- cross-talk
- inability to hear
- inability to be heard
- cutoffs
- phone company recordings
- wrong numbers
- echo
- dead line after dialing
- clipping (portions of words cut off)
- inability to logon to specific Hosts
- inability to transmit or receive data

4.6 Systems and Electronic Communications Use Policy

4.6.1 General

Washington County Government (WCG) is a user of an array of electronic communication tools and equipment (hereafter electronic systems), including but not limited to telephones and telecommunications systems, email and voice-mail services, pagers, personal digital organizers, fax machines, modems, servers, computers, software, information systems, voice and data networks, network tools, browsers, and Internet access facilities. These electronic systems are owned and maintained by WCG and, as a general rule, are to be used for business purposes only, including, without limitation, Internet and email usage. Information communicated electronically through email, the Internet or the sharing of electronic documents is subject to Maryland laws, regulations, WCG policies and other requirements, as is information communicated in other written forms and formats.

Additionally, as Washington County Government becomes more reliant on Internet access, we all must be mindful of using the Internet and email in a responsible, efficient, ethical and legal manner in accordance with the mission of WCG. The ultimate objective of having Internet and email access remains to facilitate the accomplishment of work and to advance the mission of WCG. All employees of WCG must exercise common sense and good judgment in their use of WCG Internet and email resources and official government business always takes precedence over personal use. The purpose of this policy is to ensure the proper and ethical use of these electronic system resources.

4.6.2 General Responsibility

Each employee of WCG is responsible for maintaining the security of the equipment, the integrity of all databases, and the confidentiality of information relating to WCG business. Notwithstanding WCG's monitoring and retention/destruction policies, each employee is responsible for the proper and ethical use of electronic systems and the contents of communications recorded therein. Employees are also obliged to inform appropriate staff upon discovering foreign matters or security breaches. Each employee should also bear in mind that the ease and convenience of such electronic systems as a means of communication, either with one person or entity, or a group, does not reduce one's obligations, professionalism, and courtesy to others. If you have questions about appropriate use, consult with your supervisor or department head.

4.6.3 Limited Personal Use

The Systems and Electronic Communications Use Policy permits the limited personal use of the electronic systems by employees in the workplace on an occasional basis provided that the use:

- involves minimal expense to WCG (when noticeable incremental costs for personal use are incurred, users shall follow WCG guidelines and procedures for reimbursement to WCG);
- does not interfere with official business (official business always takes precedence over personal use);
- does not cause congestion, delay, or disruption of services to any WCG system or service;
- makes clear that each personal communication, is personal in nature and not in any way identified as an official Washington County Government communication;
- involves employees exercising common sense and good judgment to ensure the proper and ethical use of these electronic system resources.

WCG is not responsible for any loss or damage incurred by an individual as a result of personal use of WCG's electronic systems.

4.6.4 Privacy Rights

All information contained in or communicated through WCG's electronic systems, regardless of by or to whom sent or received, or however stored or filed, is owned by WCG. WCG reserves the absolute right, in its discretion, to monitor, access, and disclose all information accessed by, contained in or communicated through these electronic systems. As such, employees enjoy no expectation of privacy with respect to their use of WCG's electronic systems. Furthermore, from time to time, and whether as a part of the WCG's electronic retention policy, maintenance or otherwise, the WCG reserves the absolute right to delete, wipe, or otherwise dispose of any information contained within the electronic systems.

In compliance with federal law, audio or video telephone conversations shall not be recorded or monitored without advising the participants unless a court has explicitly approved such monitoring or recording.

4.6.5 Monitoring

Anyone using WCG's electronic systems consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity or employee misconduct, system security personnel may provide the evidence of such monitoring to appropriate WCG and law enforcement officials. Individuals are not guaranteed privacy and/or confidentiality while using WCG electronic systems and should, therefore, not expect it even though these systems may be accessed by using passwords. To the extent that employees wish that their private activities remain private, they should avoid using the WCG's electronic systems for such activities.

WCG system security personnel who operate and support electronic system resources regularly monitor transmissions for the purpose of ensuring reliability and security of WCG's electronic systems resources and services and in that process might observe certain transactional information or the contents of electronic communications. Except as provided elsewhere in this policy or by law, they are not permitted to intentionally search the contents of electronic communications or transactional information for violations of law or policy, or to disclose or otherwise use what they have observed.

4.6.6 Backup

Electronic systems are backed up on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process entails the copying of electronic data onto storage media that might be retained for periods of time in locations unknown to the originator or recipient of electronic communications. The practice and frequency of back-ups and the retention of back-up copies vary from system to system.

Users of electronic systems resources should be aware that even if they have discarded copies of an electronic communication stored on devices they can control, back-up copies could exist on other devices.

Back-up copies that are able to be retrieved might be subject to disclosure under Maryland or federal law or, in litigation, as the result of the discovery process.

4.6.7 Employee Owned Electronic Devices and Equipment

Due to a variety of security issues and possible liabilities personal owned computer hardware, software and/or technology (i.e. not owned by WCG) shall not be plugged into or linked to WCG's network or have access to any WCG computing systems containing nonpublic information, or process or store nonpublic information without the prior approval of the department head and the Information Technologies Director.

Utilization of employee owned personal telecommunication devices and related equipment while working on County business or County time within reasonable bounds is permissible; however, each employee is individually responsible for the proper, ethical, and lawful use of such equipment. Any use of employee owned personal telecommunication devices to harass or discriminate is unlawful and strictly prohibited. If you have questions about appropriate use, consult with your supervisor or department head.

4.6.8 Passwords

Confidential passwords that are issued to and/or created by employees should not be shared or published and should be changed periodically according to WCG's Access Control Policy. Each employee will be responsible for all use and any adverse impact stemming from the use of passwords they have been issued and/or created.

4.6.9 Software

Software that is installed on WCG computers is the legally licensed property of WCG and shall be installed by Information Technologies (IT) staff or by other technically qualified individuals in collaboration with IT staff (see Software Management Policy).

WCG maintains a standard computer configuration for the purpose of limiting the number of variables associated with keeping a system "trouble free" for official business purposes; therefore, employees, agents, or affiliates of WCG, unless specifically authorized because of their job functions, are not permitted to use unauthorized software (e.g. downloaded software, pirated software, software not licensed to WCG, software brought from home) on WCG owned computers. This includes, but is not limited to computer programs, executable modules, computer games, screen savers, chat programs, customized cursor or other personal software. Such authorization requires the prior approval of the department head and the Information Technologies Director. In addition, please note that there are security concerns with many of the "free" software programs available on the Internet.

4.6.10 Computer and Data Safeguards

WCG employees must take precautions against importation of computer viruses. Precautions include exercising common sense and good judgment when accepting data diskettes, CDs, Zip disks, or electronic

files received from vendors or clients, or downloading files from and/or through the Internet. All this external data must be scanned with Information Technologies (IT) provided anti-viral software prior to accessing and/or copying file(s) to any WCG server resource. Anti-virus software can be executed by selecting the virus checking software from the Windows Program Manager screen (currently **avast! Anti-virus**).

All employees should log out of the network when leaving the workstation for more than a very brief break and in areas where workstations are shared by two or more users, each user should log out after a session. At the end of each workday, each employee should log out, and shut off their PC. Any peripheral equipment attached should then be turned off for the day as well.

It is understood that due to legitimate business purposes an employee may require that their workstation not be shutdown at the end of the work day or that their workstation remain operational for extended periods of time. In this case, it is the department head's responsibility to promptly notify IT so that appropriate security safeguards and procedures may be utilized.

If you receive a message that harasses or threatens you, report it as soon as possible to your supervisor and/or department head for technical or managerial follow up.

4.6.11 Internet and Email

WCG's general strategy for using the Internet, World Wide Web (WWW), and related applications, tools, and utilities is for the exchange of WCG information and data with the general public, business partners and vendors, other government agencies, and as an internal transport medium.

WCG employees are responsible for using the World Wide Web as an enterprise tool to conduct daily government business that includes information and research gathering as well as the dissemination of government information for both internal and public use.

WCG employees must receive written authorization from their department head before participation or membership can be pursued in any Internet-based discussion groups, news groups, subscription services or similar activities. A copy of the written authorization/approval must be forwarded to IT for our records.

4.6.12 Prohibitions

While the occasional, incidental personal use of WCG electronic system resources on official time (i.e., in a duty status) is acceptable, some uses are strictly prohibited. **Prohibitions include, but are not limited to:**

- using resources to earn outside income, for private gain, for commercial purposes or in support of other "for profit" activities such as outside employment or business (e.g., selling real estate, preparing and copying a newsletter or preparing tax returns for a fee);
- using resources for activities which are inappropriate or offensive to co-workers or the public, including accessing, transmitting, sending, saving, viewing, offensive material or sexually explicit material or remarks, gambling, illegal weapons, terrorist activities or any other prohibited activities (**Offensive material includes, but is not limited to, comments, jokes, images of a sexual or racial nature, gender-specific comments, or any comments, jokes, or images that would offend someone on the**

basis of gender, race, national origin, religion, physical attributes, sexual orientation or any other classification protected by federal, state, or local law);

- using resources to harass or discriminate in any manner;
- using resources to create, copy or transmit chain letters or other mass mailings, regardless of the subject matter;
- using resources to create, copy or transmit any materials or communications that are illegal or offensive to fellow employees or to the public, such as hate speech, or material that ridicules others based on race, creed, religion, color, sex, disability, national origin or sexual orientation;
- using resources to engage in any outside fund raising activity, endorsing any product or service, participating in lobbying or prohibited partisan political activity (e.g., expressing opinions about candidates or distributing campaign literature), except as authorized by the employee's supervisor;
- using resources to log into and use commercial Instant Messaging (IM) services (Commercial Instant Messaging services include, but are not limited to, IM services provided by private/commercial companies such as AOL, Prodigy, Microsoft, and Yahoo!), except as authorized by the employee's supervisor and approval from the Information Technologies Director;
- using resources to copy or distribute copyrighted software to unauthorized licensed users and/or locations;
- using resources to acquire, reproduce, transmit, distribute, or use any proprietary data, audio, or video that is protected by copyright, trademark, privacy laws, or intellectual property rights beyond fair market use or applicable license;
- using resources as a staging ground or platform to gain unauthorized access to other internal and external systems or access unauthorized areas of WCG's computer system(s);
- using resources to review, duplicate, disseminate, delete, damage, or alter files, passwords, computer systems or programs, voice mail messages, or other WCG property without prior authorization;
- employees and authorized users will not take actions that cause congestion, delay, disruption or interference to WCG's data communications network by accessing streaming video or audio, except as authorized by the employee's department head and Information Technologies;
- software is not to be loaded or placed onto WCG computers, the network, or other IT equipment without prior authorization from IT;
- moving, disconnecting, or altering any IT or electronic systems equipment;
- adding, deleting or changing operating (Windows, Linux, etc.) system and/or configuration files used on the employee's computer.

4.6.13 Violation of Policy

Penalties for violating the Systems and Electronic Communications Use Policy will vary depending on the nature and severity of the specific violation. Unauthorized or inappropriate use may result in the loss or limitation of your privilege. In addition, you may also be subject to disciplinary action as described in the Washington County Employee Handbook, including but not limited to counseling, reprimand, suspension, and/or dismissal from Washington County Government employment, as well as any criminal penalties or financial liability.

4.7 Access Control Policy

4.7.1 General

Washington County Government (WCG) must ensure that county information systems are accessed by the appropriate persons for authorized use only. While we cannot perfectly secure system access, we can implement responsible management practices and procedures that improve access control and provide a framework for granting and withdrawing information system access and/or privileges.

This policy establishes access control practices, personnel security procedures and defines the areas of responsibility for the identification, authentication, and authorization of WCG information system users. Identification and authentication is a technical measure that prevents unauthorized people or processes from entering an information system. This usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses or privileges minimally required to perform their duties. User authorization requires the linking of activities or privileges on an information system to specific individuals and, therefore, requires the system to identify users. Personnel security involves safeguards that take into account the granting or withdrawing of physical and/or system access privileges upon hiring an employee, transferring or promoting an employee, or retirement, resignation, or termination of an employee and an annual review and certification of access and/or privileges.

4.7.2 Personnel Security Procedures

Personnel security begins with the staffing process. Once personnel have been staffed, personnel security safeguards are administered using the following procedures:

A. New Hires

1. Human Resources and/or the department head are responsible for notifying Information Technologies (IT) of any new hires that would require information systems access and/or privileges. This information should be emailed to IT Service at least five business days prior to the employee's assigned start date.
2. All employees must read, review and where applicable sign the WCG Acknowledgement of Information Security Responsibility upon employment with WCG.
3. The department head should determine the type of computer access and/or privilege(s) that is needed for each employee and the sensitivity/confidentiality of the information/data required for that position. Access and privilege information should be included in the employment notification email previously referenced above. Access will be granted to personnel based on least privilege (i.e. only up to the level needed to perform one's duties).
4. New hires that are granted system access and/or privileges must complete applicable security awareness training.

B. Employee Transfer/Promotion

1. The department head must review current access and determine the type of computer access and/or privilege(s) that is needed for the employee and the sensitivity of the information/data

required for that position.

2. IT will work with the department head to modify the employee's logical and physical access (where applicable) to meet the needs of the new position.
3. IT is responsible for granting the access and/or privilege(s) as authorized by the employee's department head.

C. Employee Separation

1. Human Resources and/or the department head are responsible for notifying Information Technologies (IT) when employees are separated from service or end their employment. This information should be emailed to IT Service at least five business days prior to the employee's assigned end date. In cases of abnormal termination (firing, death, etc.) the notification should be handled with urgency.

D. Annual Review and Certification of Access

1. At the beginning of each new fiscal year (July 1st), IT will forward departmental system access and/or privilege(s) information to the department head for their review and consideration.
2. All department heads are solely responsible for auditing/recertifying, where applicable, the access and/or privileges granted to their direct reports including consultants and/or vendors prior to July 31st each calendar year by notifying IT. Failure to provide notification could result in the individual's access and/or privileges being automatically suspended and in some cases revoked.

4.7.3 User Identification and Passwords

Password and password protection is key to the security and integrity of Washington County Government's (WCG) information technology environment. All WCG network users have a responsibility to protect and guard our network, information systems and data by keeping their access passwords secret. Passwords must not be shared with others or written down in plain sight (example: sticky notes attached to video monitors or under keyboards). User chosen passwords should be difficult to guess and follow the guidelines stated below (Users Accessing the WCG network).

Division directors and/or department heads are responsible for authorizing which information technology services their staff, and/or business partners will be permitted to use. **Access to WCG network and computer resources is restricted to authorized personnel only.** Authorized personnel identify themselves to network resources, information systems, departmental applications and/or a computer via user identification (userid/logon name) and an associated password. Information Technologies (IT) is responsible for establishing and maintaining network credentials (a unique userid/logon name and an initial password) for all authorized personnel. The unique WCG network userid/logon name provides exclusive identification for an authorized user and shall be utilized across all WCG supported information systems where applicable. Information systems and/or departmental applications that do not provide or allow for full integration with WCG's security infrastructure will be required to create and/or provide a separate password to be used in conjunction with the IT assigned userid/logon name. In this instance, passwords are administered at the department level using the guidelines stated below (Users accessing non-integrated

systems and/or departmental applications) and it will be the responsibility of the division directors and/or department heads to enforce these guidelines. Information Technologies will assist and support division directors and department heads in performing this task.

A. Userid (logon name) Creation and/or Assignment:

The userid/logon name shall uniquely identify authorized personnel for computer security purposes. The standard userid/logon name format is the first letter of the user's first name, and their full last name will be used. If there is a pre-existing userid/logon name based on the standard format, then the first two letters of the first name and the full last name will be used. Repeat this process until a unique userid/logon name is created. In the rare case, where all the letters of a user's first and last name are used, a digit(s) will be appended (in sequential fashion) to the last name portion.

B. Users Accessing the WCG Network:

- Passwords will expire every ninety (90) days and users must create/choose a new individualized password.
- The minimum password length is eight (8) alphanumeric characters; use of special characters is encouraged.
- Passwords must contain characters from three of the following four categories:
 - English uppercase characters (A...Z)
 - English lowercase characters (a...z)
 - Base 10 digits (0...9)
 - Non-alphanumeric (exclamation point [!], dollar sign [\$], pound sign [#], percent sign [%], etc.)
- The use of pass phrases is highly recommended. For example, the following phrase: My son was born in 89! Would yield an 8 character password of **Mswbi89!** Pass phrases make complex password easier to remember.
- Passwords must be different than the last three (3) passwords used.
- After three (3) unsuccessful logon attempts, your userid/logon name will become disabled. You must call IT to have your userid/logon name reset before trying again. This process usually requires ten minutes to complete.

C. Users Accessing Non-integrated Systems and/or Departmental Applications:

- Update these passwords every 180 days.
- Change all vendor-supplied passwords before a system is deployed.
- **Do not:**
 - use blank passwords
 - use the same password for multiple accounts
 - make the passwords the same as your user name
 - use passwords that are easily guessed by people

- use passwords that are easily guessed by automated software (such as your user name spelled backwards or words found in dictionaries)
- use serial or incremental names or words. For example, password, password1, password2, password3, etc.

D. Administrative Passwords

Administrative passwords are subject to stringent composition, frequent change and limited access. This includes passwords for routers, switches, WAN links, firewalls, servers, administrative-level network operating system accounts, and any other IT resource. Passwords for administrative purposes must meet the following criteria:

- password is at least ten (10) characters long with mixed case (upper and lower case characters)
- password contains at least three (3) non-alphanumeric characters; where permissible
- password contains at least two numbers (0...9)

4.7.4 Enforcement

It is the responsibility of Information Technologies to enforce this policy in cooperation with division directors, department heads, and all authorized personnel. Compliance requires that IT be diligent on several fronts and perform the following tasks:

- Run password scans and notify users when a password is too easy and needs to be changed.
- Set operating systems, client-server applications, and other resources to make users change their passwords on the prescribed basis.
- Examine workspaces for passwords attached to keyboards or video monitors.
- Establish an automated process to ensure that userids are disabled after sixty (60) days of inactivity and deleted after ninety (90) days of inactivity unless they are extended through the explicit approval of the department head.
- Establish an automated process that individual users sessions either time out or initiate a password protected screen saver after a period of thirty (30) minutes of inactivity.
- Maintain audit trails for the actions performed by IT staff with regard to personnel security and access control management.
- Review security logs daily and investigate, document, and remedy (where applicable) all security violations within one business day of a discovered occurrence.
- Offer information technology security awareness programs and training for employees (new and old).

4.7.5 Access Restriction

Eligibility to access or use WCG's information technology services or resources, when provided, is a privilege accorded at the discretion of division directors and/or department heads. This privilege is subject to the normal conditions of use, including procedures for initiation and termination of service eligibility, established by this policy.

In addition, use of WCG's information technology services or resources may be restricted or rescinded by division directors and/or department heads at their discretion when required by and consistent with law, when there is substantiated reason to believe that violations of law or WCG policies have taken place, when there are compelling circumstances, or under time-dependent, critical operational circumstances.

In compliance with the Digital Millennium Copyright Act, WCG reserves the right to suspend or terminate use of WCG's information technology services or resources by any user who repeatedly violates copyright law.

4.8 Network and System Security Policy

4.8.1 General

The Internet has brought about many changes in the way Washington County Government (WCG) conducts business and it would be difficult to operate effectively without the added efficiency and communications brought about by the Internet. At the same time, the Internet has brought about problems as the result of unauthorized network access attempts (intruder attacks), denial-of-service attacks, port scanning attempts, viruses, worms and other malware. Such malicious practices originating from outside the County's sphere of control could potentially cause data loss, data corruption, and service interruption; and therefore, securing WCG networks and system resources is essential. The purpose of this policy is to define goals, roles, responsibilities, procedures and practices for maintaining and managing security for network and system resources.

4.8.2 Policy Goals

The goals of this policy are:

- To protect WCG's networks, connected systems, and services from abuse, exploit, and inappropriate use by persons or software, whether internal or external to WCG.
- To protect WCG intellectual property from unauthorized access, alteration, theft, or deletion. Intellectual property includes County data (see Data Management Policy) and data that are protected by local, state or federal laws or regulations as well as information that are protected by copyright, license agreements or non-disclosure agreements.
- To provide network services that allows secure transmission of data with the expectation that the data will not be altered or tampered with en route to a WCG-controlled resource.
- To provide reliable network services to all customers of WCG's network with a minimum of unplanned outages, including those outages caused by customers.
- To maintain complete records of all equipment on WCG's network. This will facilitate prompt notification to customers of potential security deficiencies with their systems and notification to customers of planned network interruption arising from system upgrades or containment of security breaches.
- To provide an effective mechanism for responding to complaints and queries about real or perceived abuses of WCG networks and system resources.
- To describe how we will identify threats and breaches of WCG networks and system resources.

4.8.3 Roles and Responsibilities

Information Technologies (IT) will be the sole provider of network resources (wireless and cable systems) and security for the entire WCG community and in doing so will perform the following functions:

- Will be the primary security contact for all network security related activities.
- Will control access to all WCG intranet network traffic, all inbound and outbound Internet traffic, 802.11 wireless network services, DSL and frame relay services, and modem and VPN connections.

- Will provide firewall functionality at the border between the Internet and WCG network resources and at internal secure segments.
- Monitor network traffic, as necessary and appropriate, for the detection of network problems, intrusions, anomalous activity and investigate such activity as needed.
- Will coordinate investigations into any alleged computer or network security compromises, incidents, and/or problems. To ensure that this coordination is effective, IT requests that security compromises be reported to IT via phone or email (email: IT Service@washco-md.net).
- Will research new security threats as they arise and communicate such threats to WCG system users. Threats will be classified by the danger they pose. Examples of classification are:
 - possible denial of service to a single computer (end user)
 - possible compromise of a single computer where the attack cannot propagate past that computer
 - possible access to sensitive data
 - possible compromise of multiple systems and/or servers
- Will provide security resources such as managed antivirus services and mechanisms for automating patch retrieval and installation for WCG owned hardware.
- Will maintain and document the network architecture and its component resources including TCP/IP protocol suite administration and IP addressing.
- Will perform scans of the network for devices that are not sufficiently protected against current threats and when a vulnerable device is identified corrective action will be taken to resolve the vulnerability. If scans or network monitoring identifies security vulnerabilities, the cooperation of the system owners and department heads will be solicited. When a security problem (or potential security problem) is identified IT will take steps to disable network access to those systems and/or devices until the problems have been satisfactorily resolved.

Any individual who uses a computing or communications system to create, access, transmit or receive WCG related information is responsible for protecting that information in a manner commensurate with its sensitivity, value, and criticality. Appropriate procedures regarding confidentiality and privacy of information are to be followed at all times regardless of your access connection (at work or using remote access technology) and are detailed below.

Damage to, loss, or unauthorized disclosure of any WCG physical or informational assets must be promptly reported to the employee's immediate supervisor and the department head. Any incident where personal sensitive data is thought to have been compromised must be reported to the Information Technologies Director.

4.8.4 General System Security Procedures

This document outlines general procedures for securing a computing device used for conducting WCG business whether located on WCG owned premises or elsewhere. The procedures are strongly recommended for all computing devices whether connected to a network or not.

1. Understand and comply with WCG's IT and HIPPA policies.

All individuals who use WCG computing and network facilities are required to read and abide by WCG's Systems and Electronic Communications Use Policy and other relevant policies and must read, review and sign an Acknowledgement of Information Security Responsibility. The ITM policy is the overarching policy governing the use of computing technology at WCG which includes references to each individual IT related policy. HIPPA policies apply to individuals who create, access, transmit or

receive HIPPA related data. Contact Human Resources for information regarding WCG HIPPA policies.

2. Know your IT support providers and their role in information security.

All individuals who use WCG computing and network facilities have access to IT support staff. Know who they are and the services they provide before you need them. IT support staff are trained in routine information security and the County's Intranet web site provides comprehensive information on using information technology and security. If you have any questions about general IT technology information or about any IT security component, you should contact one of the IT staff.

3. Report IT security incidents.

If you believe sensitive data may have been compromised or if any WCG physical or information asset has been damaged, you must promptly notify your immediate supervisor, IT Coordinator and/or department head. It is the responsibility of the department head or the IT Coordinator (if so delegated) to notify IT immediately.

4. Recognize when your computer may be compromised.

Information security compromise of a system often results in a dramatic change in your computer's performance that can be observed by the user. If you notice your personal computer rebooting by itself, suddenly slowing dramatically or exhibiting any unusual behavior, seek assistance from your IT support provider to determine if your computer has been compromised.

5. Implement WCG password security recommendations.

Choose a password that is difficult to guess: use a minimum of 8 characters, varying the case of letters and intermix letters, numbers, and punctuation or special characters (if the system allows). Change your password periodically (minimally every 90 days). If your password is discovered or you determine that someone is using it to access your account, contact IT. Advice on selecting and constructing good passwords and other pertinent information regarding passwords is available in the Access Control Policy.

6. Ensure computing devices are physically secured.

Information displayed on your computer screen can be viewed casually by anyone within view. If you leave the area and sensitive and/or restricted data is visible on the screen of your computer, such information can readily be viewed by anyone nearby who chooses to look. Use a screensaver that hides the screen after 10 minutes of inactivity and requires a password to restore the display. When you are away from your computer for extended periods, secure the computer and/or space if possible. Microsoft Windows based computers may be secured by simultaneously keying CTRL, ALT, and Delete. A Windows dialogue box will appear. Simply click the Lock Computer option box with your mouse and you will receive notification that your computer has been locked.

Never leave portable computing devices unattended and unlocked. Make sure the access to data on the device and the access to the device itself is limited. Portable devices such as PDAs, USB memory sticks and laptops are all especially vulnerable in transit. They can be lost or stolen. Good protective measures include putting them in a locked brief case or cabinet or using password protection and/or encryption. Restricted data (see Data management Policy) should not be stored on portable computing

devices unless absolutely necessary. In this case, any sensitive and/or restricted data should be encrypted, if possible. Doing this may require technical expertise, please contact your IT support person for assistance.

7. Avoid activities that may compromise security.

When using a web browser, be aware that the less you know about a site, the greater the dangers. For secure sites (sites whose address begins with “https” instead of “http”) examine the web address carefully to assure it is as expected. Always examine embedded links to see that they point to an address consistent with what you would expect. If you have any question and/or concern, type in the expected address manually rather than follow a programmed link.

Do not install any programs on your computer (see Software Management Policy). Many programs that can be downloaded from the Web automatically install spyware or other malicious software (“malware”) on your computer. The following widely-used Internet programs represent significant potential security risks and are prohibited on any WCG owned computers.

- Peer-to-peer file sharing services such as Gnutella, Kazaa, Bittorrent, eDonkey and the like open a direct route to your computer which may be used by others for direct access and many of these programs may directly share files on your computer to the Internet;
- Video games, particularly any that might be downloaded from the Internet;
- Shareware utilities such as so called “Internet Accelerators.”

Some programs, such as Instant Messenger, WeatherBug and other useful and apparently benign software can also pose risks. As with peer-to-peer, WCG prohibits the use of these programs on WCG owned computers unless specifically approved by your department head and the Information Technologies Director.

8. Use email securely.

Use only official WCG email systems for WCG business related email. SPAM and virus filters are provided by WG email servers.

When using email, don’t open attachments unless you are expecting them and check any embedded links within emails to verify they point to the expected location.

The single greatest cause of email exposure of sensitive data is sending email to the wrong recipient so carefully check all addresses before sending.

9. Use secure file transfer.

Any “electronic data interchange” between WCG and vendors, consultants, agents or affiliates must be only via links with equal or better security to that of a virtual private network (VPN) connection. Consult your IT support person if you have any questions regarding this process.

10. Use facsimile and telephone securely.

Data transmitted by facsimile or telephone must be treated in the same manner as any data communicated by network where appropriate safeguards must be in place to prevent unauthorized

exposure of sensitive and/or restricted information.

11. Keep your operating system and application software up-to-date.

Keeping current with updates and patches provides an added layer of security. IT provides automated solutions to keep software up-to-date. Consult your IT support person if you have any questions regarding this process.

12. Backup your data files and directories.

So that if something happens to your computer, files and data will be recoverable. If you keep data files and directories on your local hard drive (“C:”) they should be copied to your home directory, generally specified as your “H:” drive. “H:” drives are logical mappings to disk resources located on centrally managed file servers that are supported by daily back-up services.

13. Destroy data and dispose of computers properly.

Many people assume deleting files totally removes the data. In fact, it does not and apparently deleted information can still be accessed by technical savvy people. If you have a device (including PC hard drives, CDs, diskettes, USB keys, PDAs) containing sensitive and/or restricted information, you must have all such data completely removed via such techniques as zeroing or degaussing or physically smashing the device. Contact your IT support person, who can provide guidance on the necessary steps.

14. Privacy and security requirements apply to ALL locations, including your home.

Access to sensitive and/or restricted data must be limited to those users with legitimate business need to access the information. Appropriate safeguards must be in place to prevent unauthorized exposure of sensitive and/or restricted information to anyone, including family members, friends and others.

Use encryption technology (e.g. VPN and SSL) when accessing WCG systems remotely or over wireless networks. Prior authorization is required to for such access. Contact your IT support person, who can provide guidance on the necessary steps.

15. Implement additional security requirements for portable or handheld, and wireless devices.

Wireless devices (including laptops, smartphones and PDAs) must be configured to minimize the ability of unauthorized individuals to gain access to WCG resources or to monitor data communications. Wireless networks inherently provide a lower level of security than wired networks, making them problematic when handling sensitive and/or restricted data. Clients should ensure that their wireless computing device is securely configured by contacting your IT support person.

Portable devices add another dimension to the problem of information security. Always protect a portable device with a password and to configure the device to shutdown (or lock down in some other way) after a period of inactivity. That, way, if the device is mislaid or stolen, access to the data will be made more difficult.

4.8.5 Network Security Practices

WCG makes reasonable efforts to provide secure and reliable network and system resources and is expected to follow appropriate professional best practices. The following practices and techniques assist IT staff to ensure the integrity and reliability of network and system resources under our control.

1. Banner text

The following banner text will be displayed at all system entry points and at all access points to servers, subsystems, and etc. where initial user logon occurs:

“Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, email, software, and other data generated by or residing upon this system are the property of Washington County Maryland Government (WCG) and may be used by WCG for any purpose.

An automatic pause, slow roll rate, or user acknowledgement shall be used to ensure that the banner can be read.

2. Dial-in access

Dial-in access shall be limited to Citrix server log in only. Citrix client access will be restricted to remote execution of pertinent software application(s) only. Use of any dial-in remote control products or other dial-in access products is strictly prohibited unless specifically pre-approved by the Information Technologies Director.

3. Firewalls and Network Devices

WCG networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. WCG firewalls shall be configured to block all services not required, unused ports will be disabled, comprehensive audit trails will be maintained, and will operate on a dedicated device or appliance.

All network devices (e.g. servers, routers, switches) shall have all services not required disabled and the security for these devices hardened per appropriate industry standard and practices. All devices shall have updates and patches installed on a timely basis to correct significant security flaws. Default or initial passwords shall be changed upon installation of all firewall and network equipment.

4. Intrusion Detection Systems (IDS)

WCG networks will be monitored by an IDS implemented at critical junctures. IT will establish and utilize scaled response procedures that are based upon the severity of an anticipated event(s) and/or occurrence(s).

5. Wireless Networks

Wireless networks provide great flexibility, especially for mobile computing; however wireless networks do not have the performance, reliability, or security of a wired network connection. For that

reason wireless networks are not recommended as the primary network connection for staff that must access administrative systems as a significant part of their duties. IT will make a best effort to provide a robust wireless network in the downtown core but departments should not depend solely on this network and should get a network jack for network access where security, performance, or reliability is required.

6. Private Branch Exchange (PBX)

A single dedicated dial-in connection will be available for remote vendor maintenance. Appropriate access controls, encryption of transmissions and an automated audit trail will be required.

4.9 Documentation and Equipment Information Policy

4.9.1 General

Accurate computer equipment (hardware or software) information and pertinent documentation is essential to maintaining the health and continuity of Washington County Government's (WCG) network and system resources. The purpose of this policy is to define responsibilities, requirements, procedures and practices for managing and maintaining network and system resource documentation and accurate equipment information and inventory.

4.9.2 Format and Storage

Network and system resources documentation shall be kept in written form or electronic form in a minimum of two physically separate locations and due to security issues, access to this documentation shall be restricted to appropriate technical support staff. The Information Technologies (IT) Director shall specify the physical storage location(s), the directory structure and access privileges of the network and system resources documentation. All documentation shall be created and maintained using Microsoft Word, Excel, PowerPoint, or Visio; however, this documentation may then be converted to other industry standard formats for appropriate distribution.

4.9.3 Documentation Requirements

Documentation shall be required for, but not limited to the following network and system resources. IT staff are responsible for creating and maintaining compliant system documentation for WCG network and system resources for which they are responsible or tasked with administering in a timely manner.

1. **In-house developed applications.** User and source code documentation shall exist for all in-house developed applications, to include instructions for modifying and maintaining the application, location of executables and data to include server and directory structure information, backup requirements, configuration information, and required access privileges where applicable.
2. **Vendor provided departmental and enterprise applications.** All pertinent information shall be documented to include instructions for modifying and maintaining the application to include applying upgrades, patches and/or fixes, location of executables and data to include server and directory structure information, backup requirements, server and client configuration(s), version information for all software components, vendor support and contact information, processes, procedures and inquiries, data dictionary and/or layout, dependency information, and required access privileges where applicable.
3. **File, print, and web servers.** The following is a list of items that must be documented for each server:
 - a. hardware components of the system to include make and model where applicable
 - b. list of software running on the server including operating system (service pack level), programs, and services (automatic and manual)
 - c. event log settings
 - d. emergency recovery disk location and date of last update
 - e. IP address, jack location and/or identification, switch port number

4. **Network physical and logical topology.** The network topology and configuration shall be documented and provide the following information:
 - a. IP addresses of all devices on the network with static IP addresses
 - b. Layer 3 network topology diagrams including placement of routers, switches, firewalls, IDS, servers, and external access points
 - c. IP addressing scheme to include masks, routes, and VLANs
 - d. DHCP server settings, including scopes and options
 - e. voice and data cable plant layout and database to include jack, switch port, and computer or telephone (handset) connections, and end user identification
5. **Routers and switches.** Description of each router and switch on the network (wired and wireless), including make, model, serial number, software version, installed components, supported protocols, and hardware/software configuration.
6. **Network appliances.** Description of each network appliance on the network including make, model, serial number, software version, installed components, hardware/software configurations, appliance functionality, scope of use and maintenance agreement information.

4.9.4 Equipment Information

Equipment information and inventory shall be maintained for all non-consumable computer equipment (hardware or software) components whose unit cost is greater than or equal to \$50.00. IT technical support staff will maintain an equipment management system(s) of all IT and telecommunications related equipment for the purpose of tracking equipment distribution, status and licenses (where applicable). IT technical support staff shall be responsible for tracking, receiving, and inspecting shipments and subsequently updating the equipment management database(s) in a timely manner to reflect the current status. All appropriate equipment will be marked with a WCG equipment tag as required. Equipment asset records and/or documentation shall include but not limited to the following:

1. vendor information (name, invoice number)
2. manufacturer, model, version, serial number, and part number (where applicable)
3. unit cost
4. purchase, installation and warranty expiration dates (where applicable)
5. end user or computer (primary asset for components and/or peripherals) to include department

In cooperation with department heads and/or the departmental IT coordinators, IT technical support staff will annually conduct departmental equipment verification audits. These audits will consist of department heads and/or the departmental IT coordinator verifying departmental ownership of recorded equipment assets and reconciling the equipment inventory.

4.10 Information Technology Steering Committee

4.10.1 General

Divisional and departmental collaboration and planning is paramount if Washington County Government (WCG) is going to provide and coordinate efficient and effective public services in an open and cooperative manner. The purpose of this policy is to establish an internal Information Technology Steering Committee that builds support within county government and the general public for technological innovation. The committee's focus is to set the strategic direction for the cooperative and creative use of information technology within County government. This approach takes advantage of a wide-ranging set of expertise and provides a coordinated approach in the selection and implementation of technology across departmental and divisional boundaries.

4.10.2 Responsibilities

The Information Technology Steering Committee has the following responsibilities.

- Explore and evaluate new technologies that improve the quality or lower the cost of services, or create new services or better ways of doing business. Recognize that innovative ideas can come from anywhere within or outside the organization and work to bring these ideas into the open.
- Facilitate countywide strategic planning to build a technology-enabled government. Promote coordination and cooperation among county departments and divisions for effective technology integration and high quality services. Explore the application of emerging technology to the solving of business problems. Work with end-user task teams to utilize best practices for implementing enterprise-wide information systems and/or upgrades.
- Explore service integration across organizational boundaries. Form information technology related partnerships internally and with non-county governmental organizations to stimulate economic development and share costs.
- Assist in the development of an e-government strategy with wide opportunities for “anytime, anyplace” service. Identify, review, and recommend the implementation of Web enhancement technologies and/or e-government applications, business processes, and procedures.
- Review standards, policies, procedures, etc. being considered by Information Technologies for adoption. Establish and contribute to a results-oriented strategic planning process to help departments and divisions complete projects in order to accomplish their missions.

4.10.3 Membership

The Information Technology Steering Committee shall be limited to ten (10) members. The membership may consist of one appointed representative from the following:

Budget & Finance

Human Resources

County Treasurer's Office
Emergency Services
States Attorney's Office
Community Partnership for Children and Families

Sheriff's Department
Planning & Community Development
Public Works (2 appointed members)

The committee is composed of persons appointed by their director, department head or elected official to represent their organization. Each member will be the liaison to their respective organizations and will represent them and their interests on the committee. The Information Technologies (IT) Director shall serve as the chairperson. A quorum shall be a simple majority of all the members. A decision on any matter coming before the Information Technology Steering Committee shall be made by simple majority vote of the members present.

The committee, as a whole, should have the following qualifications:

- An understanding of the objectives and philosophies of Washington County government
- General understanding of information technology techniques and services
- Awareness of, or the ability to understand, the operational needs and desires of various existing and potential users of automated information systems
- Independent viewpoint regarding information technology issues
- Ability to evaluate information technology alternatives

4.10.4 Sub-Committees and End-user Task Teams

Information Technology Steering Committee members may be appointed to serve on sub-committees, which may form from time to time, to accomplish a specific task or to address a particular need. In addition, the Information Technology Steering Committee shall encourage the establishment of end-user task teams for vendor supplied software products that cross departmental/divisional boundaries. The focus of each autonomous task team is to review and understand the software's functionality, address software operational issues, identify training and operational requirements, and plan for upgrades and enhancements.

The following task team(s) and sub-committee(s) have been established and are as follows:

PeopleSoft Task Team
Web Standards Sub-committee
Geographic Information Systems Sub-committee
Wireless Technology Sub-committee

4.10.5 Meeting Schedules

Information Technology Steering Committee meetings are generally scheduled on an "as-needed" basis; however, the Steering Committee shall minimally meet bi-annually to review, discuss, and address

technology-related issues facing County government. Sub-committee(s) and end-user task team(s) independently establish their meeting schedules and agendas in order to accomplish their respective goals.

APPENDICIES

- APPENDIX A Acknowledgement of Information Security Responsibility Form**
- APPENDIX B Privileged Access Agreement Form**
- APPENDIX C IT Policies and Guidelines Summary**

Washington County Maryland Information Technologies

Acknowledgement of Information Security Responsibility

Passwords

Appropriate password protection must be installed on all County computer systems to ensure the security and integrity of the information technology and/or network environment and restrict computer resources to authorized persons.

All computer users must become password owners, identifying themselves to the County network or computers via appropriate passwords.

The employee's division director and/or department head evaluates and determines the employee's need for access to the County's computer resources and specifies access privileges. The privileges are then communicated to the Information Technologies department which establishes and maintains all access privileges.

Internet/Intranet Usage

As a means to achieve its business goals, the County encourages responsible use of the Internet/Intranet including communications via the Internet/Intranet, access to information on the Internet/Intranet and provision of information to customers via the Internet/Intranet. Office use of the Internet/Intranet is a privilege, not a right; such privilege may be revoked at any time.

Information obtained or provided via the Internet/Intranet may not contain content that may be reasonably considered offensive or disruptive to any employee. Offensive content includes, but not limited to, sexual comments or images, racial slurs, gender offensive comments, or any comments that would offend someone on the basis of age, sexual orientation, religious beliefs, national origin or disability.

Voice/Electronic Mail (E-mail)

The County encourages the use of voice/e-mail as any other work tool available to employees. Users will not engage in any activities via voice/e-mail that will in any way discredit the County. The County reserves the right to retrieve any message.

Voice/e-mail may not contain content that may be reasonably considered offensive or disruptive to any employee. Offensive content includes, but not limited to, sexual comments or images, racial slurs, gender offensive comments, or any comments that would offend someone on the basis of age, sexual orientation, religious beliefs, national origin or disability.

Software

Washington County will provide copies of legally acquired software to meet all legitimate business needs and in sufficient quantities. The use of software obtained from any other source could present security and legal threats to the County, and such use is strictly prohibited. All software acquired for or on behalf of the County or developed by County employees or contract personnel on behalf of the County is and shall be deemed County property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

Privacy Rights and Monitoring

The County is a user of an array of electronic communication tools and equipment (electronic systems), including telephones, e-mail and voice-mail systems, pagers, personal digital organizers, fax machines, modems, servers, computers, county-wide computer network (Intranet) and network tools such as browsers and Internet access facilities. These electronic systems are owned and maintained by the County and as a general rule, are to be used for business purposes only.

All information contained in and communicated through these electronic systems, regardless of by or to whom sent or received, or however stored or files, is owned by the County. The County reserves the absolute right, in its discretion, to monitor, access, and disclose all information accessed by, contained in or communicated through these electronic systems. As such, employees enjoy no expectation of privacy with respect to their use of the County's electronic systems. Furthermore, from time to time, and whether as part of the County's electronic retention policy, maintenance or otherwise, the County reserves the absolute right to delete, wipe, or otherwise dispose of any information contained within the electronic systems.

Responsibility

Each employee of the County is responsible for maintaining the security of the electronic systems, the integrity of all databases, and the confidentiality of information relating to County business. Notwithstanding, the County's monitoring and retention/destruction policies, each employee is responsible for the proper use of the electronic systems and the contents of communications recorded in the electronic systems. Employees are also obligated to inform their department head and/or supervisor upon discovering foreign matters or security breaches. Each employee should also bear in mind that the ease and convenience of such electronic systems as a means of communication, either with one person or entity, or a group, does not reduce one's obligations, professionalism, and courtesy to others.

Acknowledgement

As an employee of Washington County, I, _____, recognize and understand that the purpose of the County's electronic systems, telephone, e-mail and voice-mail systems, pagers, personal digital organizers, fax machines, modems, servers, computers, county-wide computer network (Intranet) and network tools such as browsers and Internet access facilities are to support County business. I agree not to access a file or retrieve any stored communication other than where authorized unless there has been prior clearance provided by an authorized County representative (County Administrator, Division director, Department head and/or supervisor) and to use the County's technological resources in a proper, legal and ethical manner.

I am aware that the County reserves the absolute right and will exercise the absolute right to review, audit, intercept, access and disclose all matters on the County's information technology network, computers, telecommunications, e-mail and voice-mail systems at any time, with or without employee notice, and that such access may occur during or after working hours. I am aware that use of a County-provided or employee chosen password or code does not restrict the County's right to access electronic communications. I am aware that violations of the Systems and Electronic Communications Use Policy or other pertinent IT management policy may subject me to the loss or limitation of my privileges, to administrative action ranging from counseling, up to and including dismissal from County employment, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

I acknowledge that I have read and understand the County's Systems and Electronic Communications Use policy.

Employee Signature

Date Signed

Adopted: 11/21/2006

Washington County Maryland Information Technologies

Privileged Access Agreement

Introduction

Privileged access enables an individual to take actions which may affect computing systems, network communications, or the accounts, files, data, or processes of other users. Privileged access is typically granted to Information Technologies (IT) staff functioning as system administrators, network administrators, account administrators, data custodians or other such employees whose job duties require special privileges over a computing system or network. Additionally, privileged access is typically granted to agents, or affiliates that function as a technical partner and are responsible for the implementation of information systems and the technical management of data resources.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices, and operational guidelines pertaining to the activities of the computing systems in which they have privileged access.

In particular, the privacy of restricted information holds important implications for computer system administration at Washington County government (WCG). Individuals with privileged access must comply with applicable policies, laws, regulations, procedures, while pursuing appropriate actions that may be required in order to provide high quality, reliable, and timely computing services and technical support.

General Provisions

1. Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have read and signed this agreement.
2. Privileged access may be used only to perform assigned job duties.
3. If methods other than using privileged access will accomplish an action. Those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.
4. Privileged access may be used to perform standard system related duties only on machines and networks whose responsibility is part of assigned job duties. Examples include:
 - installing system or application software to include fixes, patches and/or upgrades;
 - restoring and/or relocating individuals' files;
 - performing repairs required to return a system to normal function, such as fixing databases, tables, files or file processes, killing and restarting runaway processes, or shutting down and rebooting servers;
 - running security checking programs;
 - monitoring the system to ensure reliability and security.
5. Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorized account management activities or under exceptional circumstance. Such actions must follow any existing organizational guidelines and procedures. Examples include:
 - disabling an account apparently responsible for serious misuse such as:
 - attempting to compromise an administrator account

- using a host to mount attacks on other hosts or engaging in activities designed to disrupt the functioning of the host itself
 - using a host in such a manner which violates applicable Information Technology Management (ITM) policy and/or any management policy specified therein.
 - disconnecting a host or subnet from the network when a security compromise is suspected.
6. In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.
7. Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.

Acknowledgement

I acknowledge that I have read and understand the Privileged Access Agreement and the overarching Information Technology Management (ITM) Policy, to include but not limited to the Application Change Management Policy, the Data Management Policy, the Systems and Electronic Communications Use Policy, the Access Control Policy and the Network and System Security Policy.

I agree to comply with the provisions of this Privileged Access Agreement and the overarching Information Technology Management (ITM) Policy, to include but not limited to the Application Change Management Policy, the Data Management Policy, the Systems and Electronic Communications Use Policy, the Access Control Policy and the Network and System Security Policy.

Signature

Printed Name

Date Signed

Adopted: 11/21/2006

IT Policies and Guidelines Summary

Name	Quick Summary	Effective Date
Application Change Management Policy	Specifies procedures and prerequisites for managing the application change and acceptance process for enterprise and departmental software systems and/or applications. Examples of managed change include: major and minor software releases, service packs, and patches/fixes	21-Nov-06
Data Management Policy	Describes proper management, use, and protection of restricted and unrestricted data. Outlines responsibilities of Data Proprietors, Data Users, and Data Custodians. Describes and recommends specific procedures that provide for responsible data stewardship.	21-Nov-06
Hardware Management Policy	Describes an orderly approach to budgeting, purchasing, installing, maintaining, upgrading and/or replacing computer hardware and related technology.	21-Nov-06
Software Management Policy	Describes an orderly approach to budgeting, purchasing, installing, maintaining, upgrading and/or replacing computer software and related technology. Topic such as software ownership, licensing, registration, auditing, violations and federal law are also reviewed.	21-Nov-06
Telecommunications Management Policy	Establishes and defines areas of responsibility for the provision and management of telecommunication services that support the business operation of County government.	21-Nov-06
Systems and Electronic Communications Use Policy	Requires users to respect the rights of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Lists specific examples of prohibited “misuse”, specifies the County’s rights with respect to privacy and system monitoring, and reviews remedies for policy violations.	21-Nov-06
Access Control Policy	Establishes access control practices, personnel security procedures and defines the areas of responsibility for the identification, authentication, and authorization of County information system users. Password requirements are also specified.	21-Nov-06
Network and System Security Policy	Defines goals, roles, responsibilities, procedures and practices for maintaining security for the County’s network and system resources, and highlights general security procedures for all County system users to follow.	21-Nov-06
Documentation and Equipment Information Policy	Defines responsibilities, requirements, procedures, and practices for managing and maintaining system resource documentation and accurate equipment information and inventory.	21-Nov-06
Information Technology Steering Committee	Defines the focus, responsibilities and membership for the Information Technology Steering Committee.	21-Nov-06
Acknowledgement of Information Security Responsibility Form	Confirms information security responsibilities for system users and the County’s absolute right to monitor, audit, review, access and disclose all matters on the County’s information technology infrastructure at any time, with or without notice.	21-Nov-06
Privileged Access Agreement Form	Individuals with privileged access to systems must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws and/or regulations.	21-Nov-06