COUNTY AGENDA REQUEST

Department:	Information Systems	Presenter(s):	Russell Prince
Meeting Date:	Wednesday, January 4, 2012	Type of Request:	New Business

Wording for the Agenda:

Consideration of proposed policies for the use of County Information Systems.

Background/History/Details:

As recommended in the Strategic Technology Plan, a new comprehensive set of policies has been developed to cover the use of all County Information Systems. Several policies are being proposed to cover various County systems and uses, including an Acceptable Use Policy, Email Policy, Internet Use Policy, and a Technology Implementation Policy.

What action are you seeking from the Board of Commissioners?

Consideration of proposed policies to be approved at a future Commissioners Meeting. If the Board concurs, these policies will be scheduled for adoption at a meeting in the near future.

If this item requires funding, please describe:

None

Has this request been considered within the past two years?	No	If so, when?	
Is Audio-Visual Equipment Required for this Request?	No	Backup Provided with Request?	Yes

STAFF USE ONLY

Approved by Finance	Yes	Reviewed by Legal	
Approved by Purchasing	Not Applicable	County Clerk's Approval	Yes
Administrator's Approval	Yes		

Staff Notes:

Fayette County GEORGIA

Where Quality Is A Lifestyle

To: Jack Krakeel, County Administrator

From: Russell Prince, Chief Information Officer

Date: December 27, 2011

Subject: Information Systems Policies and Procedures

As part of the County's adopted Strategic Technology Plan, new Information Systems policies and procedures have been recommended. Attached are drafts of the new Information Systems policies to cover the following areas:

Information Systems - Acceptable Use. This policy provides detailed guidelines and procedures for the usage of the County computer systems and network resources.

Information Systems – Email Use. This policy provides detailed guidelines for the usage of the County email systems.

Information Systems – Internet Use. This policy provides detailed guidelines for the usage of the County Internet access and associated resources.

Information Systems – Technology Implementation Plan. This policy provides detailed guidelines and a format for the development of Technology Implementation Plans. These plans would be submitted to Administration and the IS Department prior to funding of large technology projects. The plans would be used to help identify the comprehensive resources necessary to successfully implement a new technology project including the required departmental resources, Information Systems resources, assigned Project managers, training, and long term funding.

If you have any suggestions, changes, or need any additional information, please let me know.

OPERATIONAL FUNCTIONS
Information Systems - Acceptable Use

PURPOSE

The purpose of this policy is to provide guidelines for the acceptable use of Fayette County computer systems and network resources. These rules are in place to protect the Fayette County Board of Commissioners and its employees. Inappropriate use exposes Fayette County to unacceptable risks including virus attacks, network security issues, loss of confidential information, and legal issues.

POLICY

There shall be a consistent and uniform use of computer systems and network resources.

PROCEDURES

Scope

This policy applies to employees, contractors, consultants, temporary employees, and other workers at Fayette County, including all personnel affiliated with third parties. This policy applies to all Fayette County information systems (owned or leased), whether on a public system (Internet), on the County's internal network (Intranet), or accessible via a remote connection (Extranet). These systems are to be used for business purposes in serving the interests of the County, and of our citizens and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every Fayette County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

General Use

1. New or modified network user accounts, email accounts, phone extensions, voice mail boxes, MUNIS logins, RightFax setup, or Internet access should be requested by entering a work order in the IS Department's work order system and attaching a User Access Form or MUNIS User Form with the necessary information and, if necessary, justification.
2. While Fayette County's network administrators desire to provide a reasonable level of privacy, users should be aware that the data they create on County systems remains the property of Fayette County. Because of the need to administer and monitor the County's network, confidentiality of information stored on any network device cannot be guaranteed.
3. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for

monitoring their users for excessive personal use of Internet/Intranet/Extranet systems. If abuse is suspected by department management, a request can be made to the IS Department for recent logs of a users Internet activity. The department head will determine if the usage is considered excessive and if disciplinary actions are required. If there is any uncertainty concerning personal use, employees should consult their supervisor or manager. The IS Department may also deem usage excessive based on resources consumed and restrict a user's access, up to and including termination of access to Information System resources.

4. For security and network maintenance purposes, the IS Department may monitor equipment, systems, and network traffic at any time to ensure compliance with this policy.
5. No one shall copy, install, download, or export any software or data in violation of any copyright laws, license agreements, trade secrets, patents or other intellectual property or similar laws. This includes, but is not limited to, copyrighted software applications and downloading and/or the distribution of music, movies, "pirated" software and other electronic media via the internet that are not appropriately licensed for use by Fayette County.
6. Under no circumstances is an employee of Fayette County authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Fayette County-owned resources.
7. No one shall use any County information systems (computers, printers, scanners, email, telephones, paging, etc.) to copy, distribute, or store fraudulent, defamatory, harassing, obscene, or threatening material, or any communications prohibited by law.

Security, System and Network Activity, and Confidential Information

1. No user shall use any County computer or network resource without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the County's computer or network resources. The IS Department may use network monitoring software and systems to assure that only authorized users are connected to the County's network. Any unauthorized users discovered will be disconnected immediately, without notice, by physical disconnection, security software, configuration changes, or any combination of methods.
2. No one shall connect any computer or equipment to any County network without prior approval from the IS Department. The IS Department shall review all requests to determine if the equipment meets proper security standards and County policies before approval will be granted.
3. All computers that are connected to the Fayette County Internet/Intranet/Extranet, whether owned by Fayette County, an employee, or third party vendor, shall be continually running approved virus-scanning software with a current virus database unless otherwise authorized by the IS Department.
4. No one shall give any password for any County computer or network resource to any unauthorized person, nor obtain any person's password by any unauthorized means. No one except the system administrators in charge of County computers and network resources are authorized to issue passwords for computer and network use. Users should keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts.

User passwords should be changed every 90 days. Exceptions to this are passwords for systems that provide access to limited resources such as a public access terminal with access restricted to read-only files.

5. No one shall misrepresent his or her identity or relationship to Fayette County when obtaining or using County computers or network resource.
6. No one shall use the County's network and communication resources to attempt unauthorized access of any other system or resources not owned by the County.
7. No one without proper authorization shall install, modify or reconfigure the software or hardware of any County computer or network resource.
8. Information contained on County information systems should be classified as either confidential or not confidential, as defined by County confidentiality guidelines, details of which can be found in Human Resources Confidentiality Policies (436.xx). Employees should take all necessary steps to prevent unauthorized access to confidential information.
9. If sensitive information, such as data containing social security numbers or other confidential data, is being sent outside the County's network, email encryption should be used to protect the information. If email encryption is required, the department head should contact the IS Department concerning the licensing and cost of email encryption services.
10. Because information contained on mobile computers is especially vulnerable, special care should be exercised. All County laptops that store confidential data should have hard drive encryption software installed to protect the sensitive data in case the laptop is lost or stolen. Department heads or management should contact the IS Department concerning licensing and the cost of hard disk encryption for their department's laptops.
11. Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses, spam, or Trojan horse code. No one shall create, install, or knowingly distribute a computer virus, spyware, or other covertly destructive program on any County computer or network resource, regardless of whether any demonstrable harm results.
12. No one shall perform security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
13. Port scanning or security scanning is expressly prohibited unless prior notification to the IS Department is made.

Email and Internet Use

Detailed guidelines on the acceptable usage of County Email and Internet Access is provided in the Email Use Policy XXX.XX and Internet Use Policy XXX.XX

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

OPERATIONAL FUNCTIONS
Information Systems - E-mail Use

PURPOSE

The purpose of this policy is to provide guidelines for the secure, effective, and efficient use of the Electronic Mail (Email) Systems of Fayette County. It sets forth Fayette County's policy with regard to access to, usage, and disclosure of electronic mail messages sent or received by Fayette County employees using the Fayette County Email System.

POLICY

There shall be a consistent and uniform use of the Fayette County Email System.

PROCEDURES

Scope

This policy applies to all employees, contractors, consultants, temporary employees, and other workers at Fayette County that have authorized access to the County's Email systems. These systems are to be used for business purposes in serving the interests of the County, and of our citizens and customers in the course of normal operations.

Security

The Fayette County Email System is a privileged communication system that creates, stores, and forwards electronic data from one user to one or more users. Authorized users are provided a login name and preset password that allows them access to the system. Once the user logs in for the first time, they will be responsible for changing their password to a personalized password. The confidentiality of this password will be the sole responsibility of each user. No user shall divulge his password to anyone, unless requested by authorized Information Systems support personnel for maintenance of their email account. Any communications via the email system will be attributed to and the responsibility of the authorized user of the originating account. To maintain the security of the system, each user shall be required to log out of the system if they are not in physical control of the computer or leave the computer unattended. If a user fails to observe the recommended log out procedure, other users may have easy access to messages stored in their mailbox. No employee shall attempt any unauthorized access to the email system. Any employee found to have engaged in unauthorized access of the system may be subject to disciplinary action. No employee with authorized access to the email system shall allow an unauthorized employee or person not employed by the Fayette County Board of Commissioners to use the system for any reason.

Disclosure/Privacy

All Fayette County email data, including materials created, received or transmitted within the email system are the property of the Fayette County Board of Commissioners. All messages, even "deleted" messages, may be stored or archived and are subject to Freedom of Information Act (FOIA) statutes. Employees, therefore, must be aware that they should have no expectation of personal privacy in the use of these systems.
Fayette County reserves the right to access and disclose the contents of any employee's electronic mailbox. Such access may be necessary to comply with an open records request or to investigate a possible violation of email policy or system security. Any contents properly obtained under these guidelines, may be disclosed without the consent of the employee, but only to those personnel who have some reasonable need for access to the information.

Monitoring

The Fayette County Board of Commissioners, as owners of the system, reserves the right to monitor the use of the email system to ensure that only appropriate messages are being transmitted and to confirm that the systems are functioning properly. Such sampling will also allow the Information Systems Department to continually reassess the utilization of the systems and, whenever appropriate, make such changes to the systems as deemed fit.

Acceptable Use

1. The County's Email systems and associated resources are provided to conduct County business.

2. Occasional and incidental personal use shall be permitted if it does not interfere with the work of personnel, the County's ability to perform its mission, and meets the conditions outlined in County policies and procedures. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty concerning personal use, employees should consult their supervisor or manager. The IS Department may also deem usage excessive based on resources consumed and restrict a user's access, up to and including termination of access to County Email systems

3. Initial access for new users, will be authorized by the employee's Department Head. Initial training shall be provided by Information Systems or trained departmental staff if needed.

4. The maintenance of the Global Address List and Public Folders on the email system shall be the responsibility of the Information Systems Department. Requests for changes should be forwarded to the Information Systems Department.

5. It is the user's responsibility to mange their email account. Proper management is essential to assure that only necessary emails are kept and that the user's mailbox does not fill up.

6. Delivery or Read receipt requests shall not be turned on by default in Outlook. Requesting a Delivery or Read receipt on every email creates an unnecessary load on the email server. If a delivery or read receipt is necessary, they should be requested on individual emails using the "Options" settings in the Microsoft Outlook.

7. The County reserves the right to discard incoming mass mailing ("SPAM") without notifying the sender or its intended recipient.

8. If sensitive information, such as data containing social security numbers or other confidential data, is being sent outside the County's network via email, email encryption should be used to protect the information. If email encryption is required, the department head should contact the IS Department concerning the licensing and cost of email encryption services.

Unacceptable Use

1. No email shall be used to send or receive any information or software that is in violation of copyright laws.

2. No employee shall use the electronic mail system for mass distribution of personal or non-business information. This includes, but is not limited to, email chain letters, junk mail, pyramid schemes, and emails used to solicit for personal or commercial ventures, religious or political causes, outside organizations, or other non-work related solicitations.

3. Harassment of any kind is strictly prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, sexual preference, or any other attribute protected by state and federal laws shall be transmitted.

4. No County employee shall use a web-based email account, such as user@yahoo.com, user@msn.com, user@excite.com, to conduct County business. County emails will not be forwarded to any outside email account without a copy being retained on a County email server as emails from outside email systems cannot be properly archived by the County.

Remote Access

Remote Access of County email is supported using the following methods:

a. *Outlook Web Access* – County email can be accessed via a web browser on any Internet enabled computer using the following address: https://email.fayettecountyga.gov/exchange. The user must login using his network username and password.
b. *Microsoft Mobile Activesync* – Smart Phones and other devices that are compatible with Microsoft's Mobile Activesync can also access the County email system (e.g. iPhones, Andriod phones, etc.). Generic instructions for this type of setup can be obtained from the Information Systems Department. Access to email

from personal devices is considered a "user managed" service, meaning that the user is responsible for providing Internet connectivity for the device, installing any required software, and paying any associated fees.

Support for email access using personal computers or devices is limited to general assistance and written instructions.

Violations

Violations of any policy guidelines are subject to the Fayette County's disciplinary procedures, up to and including dismissal. Violators may be subject to loss of access to Internet and email systems. Violators of the policy may also be subject to law-enforcement referrals if laws have been violated. If necessary to support appropriate disciplinary measures, information about email messages and usage will be recorded and provided to the appropriate department head, supervisor, or the Human Resources Department. Any investigation will be maintained as confidential to the greatest extent possible, while recognizing specific legal requirements for public access to information and the need to investigate all complaints thoroughly.

OPERATIONAL FUNCTIONS
Information Systems – Internet Use

PURPOSE

The purpose of this policy is to provide guidelines for the acceptable use of the County's Internet access and associated resources. These rules are in place to protect the Fayette County Board of Commissioners (FCBOC) and its employees. Inappropriate use exposes Fayette County to unacceptable risks including virus attacks, network security issues, loss of confidential information, and legal issues. Adherence to this policy will prevent the unauthorized and unethical use of the County's Internet access.

POLICY

There shall be a consistent and uniform use of the County's Internet resources to prevent the unauthorized and unethical use of the Internet.

PROCEDURES

Scope

This policy applies to all employees, contractors, consultants, temporary employees, and other workers at Fayette County that have access to the County's Internet resources. These systems are to be used for business purposes in serving the interests of the County, and of our citizens and customers in the course of normal operations.

Acceptable Use

1. The County's Internet access and associated resources are provided to conduct County business.
2. Occasional and incidental personal internet use shall be permitted if it does not interfere with the work of personnel, the County's ability to perform its mission, and meets the conditions outlined in County policies and procedures. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for monitoring their users for excessive personal use of Internet resources. If abuse is suspected by department management, a request can be made to the IS Department for recent logs of a users Internet activity. The department head will determine if the usage is considered excessive and if disciplinary actions are required. If there is any uncertainty concerning personal use, employees should consult their supervisor or manager. The IS Department may also deem usage excessive based on resources consumed and restrict a user's access, up to and including termination of access to County Internet resources.

3. Authorization for County Internet access shall be provided by the Information Systems Department. Internet access should be requested by entering a work order in the IS Department's work order system and attaching a User Access Form with the necessary information and justification.
4. No one shall give any username or password for a County computer or Internet access to any unauthorized person, nor obtain any person's password by any unauthorized means. (This includes family and other household members if work is being done at home.) No one except the system administrators in charge of County computers and Internet access are authorized to issue passwords for computer and Internet use. Users should keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts. User passwords should be changed every 90 days.

Unacceptable Use

The following activities are prohibited, although some employees may be exempted from these restrictions during the course of their legitimate job responsibilities
(example: Law Enforcement staff my need to access inappropriate web sites for investigative reasons). The list below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. Access to streaming audio and video sites, including but not limited to Internet radio/television sites, news sites, etc., consume excessive network bandwidth and are not permitted on the County's network. Requests for temporary exceptions for video training purposes shall be reviewed by the IS Department. Requests should be sent to the IS Department via a work order stating the request, justification, and time frame needed.
2. For its own protection, the County reserves the right to block all Internet communications from sites that are involved in extensive spamming or other disruptive practices, even though this may leave the Internet users unable to communicate with such sites.
3. Under no circumstances is any user of the County's Internet access or resources authorized to engage in any Internet activity that is illegal under local, state, federal, or international law.
4. Unauthorized downloading or uploading of copyrighted material for which Fayette County or the end user does not have an active license is strictly prohibited. This includes, but is not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and copyrighted software.
5. Browsing, downloading, posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material deemed offensive or dangerous is strictly prohibited.
6. Posting or sending sensitive or confidential information outside of the County without management authorization is prohibited.
7. County Internet users shall not use County Internet resources to post commercial announcements or advertising material.
8. County Internet access and resources shall not be used to promote or maintain a personal or private business.

9. Excessive Internet usage that disrupts the County's Internet access is strictly prohibited and may result in temporary or permanent termination of the user's Internet access. County related business that may consume excessive bandwidth (such as large software downloads) should be scheduled after hours as to not negatively impact the other County Internet users.

Blogging/Social Networking

1. Blogging or posting on Social Networking sites by employees, whether using Fayette County's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Fayette County's systems to engage in this activity is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Fayette County's policy, is not detrimental to Fayette County's best interests, and does not interfere with an employee's regular work duties. As with any type of Internet access on the County's network, this activity is subject to monitoring.
2. Fayette County employees and other individuals covered by this policy are prohibited from revealing any Fayette County confidential or proprietary information, or any sensitive material prohibited by the Fayette County Human Resources Confidentiality Policies (436.xx) when engaged in blogging or posting on social networking sites.
3. Employees shall not engage in any blogging or posts that may harm or tarnish the image, reputation and/or goodwill of the FCBOC and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging, posting, or otherwise engaging in any similar conduct. Employees may also not attribute personal statements, opinions or beliefs to Fayette County when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Fayette County. Employees assume any and all risks associated with blogging.
4. It is recommended that employees refrain from identifying themselves as an employee of the FCBOC on their personal social networking site. By identifying oneself as an employee of a company, a social networker becomes, to some extent, a representative of that company, and everything he/she posts has the potential to reflect on the company and its image. If an employee does identify themselves as a Fayette County employee, however, they shall place a disclaimer on personal posts or on their site so that it is clear that the opinions expressed are solely those of the author and do not represent the views of the FCBOC.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Fayette County's trademarks, logos and any other Fayette County intellectual property may also not be used in connection with any blogging activity or social networking sites.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Blogging - Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Spam - Unauthorized and/or unsolicited email.

Spyware - Spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

Trojan - A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can take control of a system and carry out its chosen form of damage.

OPERATIONAL FUNCTIONS
Information Systems – Technology Implementation Plan

PURPOSE

To provide guidelines for the procurement and implementation of technology systems or services to assure that the appropriate resources are available and that the proper responsibilities have been defined.

POLICY

There shall be a consistent and uniform method for the procurement and implementation of technology systems or services.

PROCEDURES

A. Definition

Technology plans are required for all county projects that include the purchase, installation, and support of computer equipment or software. Departments who seek funding and/or technical assistance with such projects must first complete a technology plan in accordance with the template provided. This process results in 1) a complete understanding of the projects to be undertaken by all departments involved and 2) a logical organization of all technology projects and resources. This includes all projects from small-scale software installations, such as those that affect only individual PC's, to County-wide long term or CIP-funded technology projects. Each technology plan will be reviewed by the Information Systems Department and will accompany the respective department's budget request. If there are technology projects planned but not included in a budget (such as grant-funded projects, for example), technology plans are required but will be reviewed only by the Information Systems Department before project commencement.

B. Objectives

Continued growth and innovation in the County's Information Systems environment requires proper management. As multiple departments initiate more and more IS projects, it is important that we understand what resources will be required for both implementation and long-term maintenance. With this planning process in place we will be able to:

- To enable the organization to best manage the funding and use of vital technology resources,

- To identify opportunities to leverage I.S. investment across departments,

- Prioritize projects based on their feasibility and importance to the organization,
- To ensure that related technology projects are carried out in the proper order,
- To enable the Information Systems Department to plan appropriately for upcoming projects so that adequate resources can be made available
- Improve the potential success of each project,
- Evaluate and potentially reduce the risk associated with each project,
- Initiate only those projects for which there are or will be adequate resources, and
- Schedule projects in a manner that avoids situations where limited resources are exhausted on a few projects and other projects do not get the attention required.
- To assure technology projects' alignment with the County's mission.

C. Template / Requirements

The technology plans will vary in both length and detail depending upon the complexity of each project, however, each plan must include the following components. Please include the following sections in your plan.

1. Project Description

This section of the plan provides an opportunity to introduce the technology project and review its purpose. The project's mission and objectives should be clearly stated, and should indicate how this plan aligns with the department's business plan. Reference to applicable master plans should be included in this section if appropriate.

2. Identification of Business Process

Use this section to explain how this function is currently carried out and how it will be improved with the implementation of the proposed technology solution. For example, perhaps more revenue could be generated with a technology solution in place, activities could be completed in less time, long-term costs could be reduced, information could be more readily available to the public, etc.

3. User Involvement In The Construction Of This Plan

This section should include a description of how the end users have contributed to the planning process and how they will participate as the project evolves. Business processes are best understood by the people who employ them on a daily basis. These users are crucial to identifying what must be accomplished and, thus, the end users of a proposed system should be included in the planning and implementation phases of all IS projects. The success of any solution will depend very heavily upon the satisfaction of the users who are required to use the system as a part of their job function.

4. Identification of Stakeholders

Identify who will be impacted by this project. Public citizens are likely to always be a stakeholder. Other likely examples include other departments, local businesses, and other government agencies. This section should explain who the stakeholders are and specify how they will be impacted.

5. Technical Requirements

In this section identify what new hardware, software and technical consulting services will be required for this project, as well as what will be expected of existing hardware and/or software. Include specific brand names and models when possible. A basic description of the type of hardware and/or software will suffice when specifics are unavailable for planning purposes.

6. Security

Identify both physical and electronic security requirements. Include identification of individual personnel who should or should not have access to the solution or specific components within the solution, whether any data involved is private, whether there are any public safety considerations, whether there is legislation that enforces specific security restrictions, etc. It is essential that each plan clearly identify all security concerns so that adequate security measures can be planned and implemented.

7. Budget

This section should include the details behind the budget request or grant allocation. Include specific funds, account numbers and line items. If known, list all hardware, software, training, engineering and consulting services, and all other expenditures that will be required to carry out this project.

8. Future Budget Impact

In addition to the items listed in the previous "Budget" section, identify how this will impact future budgets. Most technology projects will carry a support and maintenance cost into future years, additional computers will increase Computer Replacement Plan contributions, etc. If you plan to establish a replacement fund for this particular technology solution so that it can be replaced when it becomes obsolete, include details here.

9. Training

Formal training is a required component of all new information systems. Indicate in this section how the training will be conducted and by whom.

10. Request For Proposals

Indicate whether an RFP will be written for the selection of this technology solution, and, if so, specify the timeline for RFP construction, release, review and selection. Also, identify who will participate on the RFP review team. Outline in detail the selection criteria that will be used in choosing the solution which best meet the needs of this project. Likely examples include cost, scalability, compliance with technology standards, provider's experience with this product in the municipal market, provider's financial stability, etc.

11. Timeline

Use this section to identify project milestones that, when complete, will mark successful progress during the course of implementation. Include projected dates when each milestone is likely to be accomplished. (Note that only technology projects for which there are adequate human resources available will be approved. Adjustments to project schedules and timelines may be made in order to accommodate any deficiency in human or other resources.)

12. Assignments

The names of individuals assigned to specific roles should be included here. At minimum, the following roles will be required:

- Staff Project Leader - the individual in the originating department who will be the main point of contact and will take responsibility for managing the department's role in this project.

- Information Systems Project Manager - the Information Systems staff who will be the main point of contact for coordinating the technology implementation, handling the technology issues, and will ensure that Information Systems requirements are carried out according to this plan, and

- Budget contact - the individual in the originating department who will make funding decisions and assignments as payments are required for this project.

Additional assignments may be required depending upon the size and nature of the project.

D. Submission Procedure

Completed Technology Plans should be submitted to the Information Systems Department. Information Systems staff will review each plan and analyze the following:

- Completeness according to these guidelines,

- Adherence to county technology standards,

- Adherence with Information Systems Department policies,

- Accuracy of cost estimates,

- Impact on other IS projects, and

- Feasibility of project schedule in accordance with other IS projects.

Upon such review, Information Systems staff will determine whether changes to the plan are required and, if so, work with originating department staff to adjust the plan accordingly. If satisfactory, Information Systems staff will approve the plan. The originating department will be required to include approved Technology Plans with related budget requests.