POLICY 301 INFORMATION TECHNOLOGY RESOURCES

1. Purpose. To provide employees with a variety of information technology resources such as computers, printers, scanners, electronic mail, voicemail, Internet access, and application software in an effort to allow them to be more productive and have the information necessary to do their jobs.

2. Employee Responsibility.

2.1 Employees are responsible for appropriate use of information technology resources in accordance with this policy.

2.2 Employees are expected to adhere to the highest ethical standards when conducting County business.

2.3 All use of information technology resources must be able to withstand public scrutiny without embarrassment to Eau Claire County, its customers or its employees.

3. Management Responsibility.

3.1 Eau Claire County managers and supervisors are responsible for ensuring the appropriate use of information technology resources through training, supervising, coaching and when necessary, taking disciplinary action.

4. Appropriate Use.

4.1 The use of and access to information technology resources is limited to employees and officers of Eau Claire County and is intended for County business-related purposes only. Consequently, all data and information will be and will remain the property of Eau Claire County and will not belong to employees or officers.

4.2 Except as otherwise prohibited by this or another Eau Claire County policy, limited and reasonable use of these tools for occasional employee personal purpose that does not result in any additional cost from loss of time or diversion of resources from their intended business purpose is permitted, subject to management approval.

4.3 The use of information technology resources is a privilege and may be revoked at any time by management if use is deemed inappropriate as defined below.

5. Inappropriate Use.

5.1 Inappropriate use of information technology resources may result in the revocation of privileges, job-related discipline or both. Uses that are prohibited by Eau Claire County include, but are not limited to.

5.1.1 Accessing information resources or altering data without the explicit authorization of management;

5.1.2 Intentionally deleting or damaging files or introducing viruses;

5.1.3 Illegal activities as defined in accordance with State and Federal Law or local ordinances;

5.1.4 Wagering, betting, or selling chances;

5.1.5 Transmitting threatening, abusive, obscene, lewd, profane, or harassing material or material that suggests any lewd or lascivious act;

5.1.6 Viewing, reading, or accessing any sexually explicit sites or materials that are in any way sexually revealing, sexually suggestive, sexually demeaning or pornographic except when such access is required by job duties and approved by management;

5.1.7 Using the organization's time and resources for personal gain;

5.1.8 Solicitation, except in relationship to County-sanctioned activities;

5.1.9 Promotion of political or private causes, positions or activities;

5.1.10 Unethical use;

5.1.11 Attempts to evade, disable, or bypass any security provisions of systems or the network.

6. Internet Email.

6.1 To eliminate the potential of personal opinion from being interpreted as public policy, email addresses that reflect the name of Eau Claire County or one of its departments or agencies are reserved for official County business. Such addresses should only be given to business contacts and for business purposes.

7. Confidential Information.

7.1 Many Eau Claire County employees have access to confidential information through the course of their job. Confidential information can only be used to perform job functions. Any other use is illegal and may result in prosecution and other sanctions.

7.2 Access to confidential information outside of the strict business needs of job function is prohibited. Reasonable measures must be taken to safeguard confidential information from unauthorized access.

7.3 Confidentiality of messages cannot be guaranteed in most email systems. If a message contains confidential information, employees must use other forms of delivery.

8. Storage, Retention, and Disposition.

8.1 Employees who use electronic documents must be aware of the retention requirements for public records and the exemptions that ensure the privacy of certain documents.

8.2 It is the responsibility of the employee to determine whether a document contains official County business and whether it is subject to retention according to public record law.

8.2.1 If the document is subject to retention, the employee must determine the length of retention as required by law.

8.2.2 If the retention period is more than a few days, the document should be printed and filed in the same manner as other paper documents related to the same matter.

8.3 Eau Claire County retains exclusive ownership of all information and applications created by or stored on the information technology resources it provides. All critical business related information should be stored on the County network for backup purposes.

8.3.1 If access to the County network is not available, alternative backup procedures must be in place.

8.3.2 No personal data files such as music or pictures should be stored on the County network.

8.3.3 If personal media such as personal flash drives are used, be aware that there is no expectation of privacy if County information is stored on personal media. It is recommended that employees use only County purchased removable media.

9. Security.

9.1 The following guidelines have been established for all Eau Claire County employees given access to information technology resources.

9.1.1 Employees may only access information resources explicitly authorized by management.

9.1.2 Employees are responsible for properly safeguarding logins and passwords and are held accountable for any activity that occurs under their login name and password. Any unauthorized activity must be immediately reported to management.

9.1.3 Employees may not use logins and passwords belonging to others to seek information, hide their identity, or misrepresent someone else.

9.1.4 Employees may not intentionally engage in any activity that is likely to prevent others from accessing and using any information technology resource.

9.1.5 Anyone receiving electronic communications in error will notify the sender immediately. The communication may be privileged, confidential, and/or exempt from disclosure under applicable law. Such privilege and confidentiality will be respected.

10. Downloading Software.

10.1 Unless authorized by the Information Systems Director, employees will not download software residing on the Internet or bulletin boards. This includes but is not limited to games, screensavers, wallpaper, graphics, utilities, demo disks, and third-party software.

10.2 Downloading software presents a significant risk of virus infection and license fee liability. Resolving these problems can be expensive and time consuming, therefore the unauthorized copying, downloading, or importing of software by any method is strictly prohibited.

10.3 If downloading is properly authorized, employees must follow designated procedures for file transfer, virus scanning and licensing.

11. Copyrighted Material.

11.1 Material on the Internet may be copyrighted. Duplicating and distributing copyrighted material without express written consent of the owner is against the law and is prohibited.

11.2 Employees should not assume that software is available for public use free of charge simply because there is no copyright or other intellectual property notice on or in the software. U.S. copyright law, and that of many other countries, no longer requires a copyright notice as a prerequisite to copyright protection.

12. Anti-Virus Measures.

12.1 All computers with Internet access will have virus protection software installed prior to the connection being established. Even though this software will detect many viruses, it will not detect them all. Therefore, it is very important **not** to access email or email attachments from senders you are not familiar with or appear suspicious. Simply opening a file can cause a virus to invade the network.

13. Software Use.

13.1 All software used on Eau Claire County computers must be legally licensed and purchased through or authorized by the Information Systems Department. Running software that is not licensed is illegal and can subject the user and Eau Claire County to substantial penalties under the law.

13.2 No personal software, even if purchased by employees specifically for their office computer, may be installed without prior authorization from Information Systems.

14. Hardware Use.

14.1 All hardware connected to Eau Claire County computers or networks must be purchased through or authorized by the Information Systems Department. Attaching hardware that is not approved can cause compatibility problems or breech the security of the network.

14.2 No personal hardware, even if purchased by an individual specifically for their office computer, may be installed without prior authorization from the Information Systems Department.

15. Network Use.

15.1 All hardware belonging to outside vendors, contractors or interns must be checked and approved by the Information Systems Department prior to being connected to the Eau Claire County network. Attaching hardware that has not been authorized can breech the security of the network and cause significant damage Use of Eau Claire County equipment by outside vendors, contractors or interns will be reviewed on a case-by-case basis and must be approved by the department head and the Information Systems Director.

16. Personal Digital Assistants.

16.1 Personal Digital Assistants (PDA's) are small handheld computers capable of running applications that range from calendaring and note taking to information retrieval and update.

16.2 All requests to purchase PDA's or attach employee-owned PDA's to the Eau Claire County network must include written justification and a description of the hardware and software required.

16.3 The department head and the Information Systems Director must approve each request.

16.4 The Information Systems Department will be responsible for installation and implementation of the required hardware and software.

17. Privacy and Monitoring.

17.1 The information technology resources provided for employees are the exclusive property of Eau Claire County as are all documents, applications, communications, and messages created using those resources.

17.2 Utilizing information technology resources should **not** be considered private or secure.

17.3 Eau Claire County reserves the right to access the contents of documents, applications, communications, and messages and to fully cooperate with local, state and/or federal officials in any investigation concerning or relating to any electronic communications transmitted to or from any Eau Claire County facility.

17.4 Eau Claire County will monitor the use of information technology and retains the right to limit its use. Hardware and software tools exist that will log destination and duration of Internet access by user, examine the content of files and email, and scan network and local disk drives. Eau Claire County will implement these tools to perform periodic and random audits of information technology usage. Management may use the results to identify and prevent potential problems.