RICE COUNTY

Security and Acceptable Use Policy

EFFECTIVE July 25, 2006

Introduction: Rice County Security Policies and Guidelines

The public places considerable confidence in Rice County to ensure the integrity, accuracy and security of information stored, managed and shared by the County. In addition, the County is responsible to manage and protect this information according to county, state and federal regulations including Minnesota's Government Data Practices Act, [Chapter 13] and Federal HIPAA Regulations. These policies and guidelines have been developed to help ensure the proper management and security of this information. Failure to comply with any of the provisions can have employment consequences and will be managed in accordance with Rice County personnel policies.

Purpose: Rice County recognizes that phone and computer systems are becoming increasingly interconnected and sophisticated in their ability to create, disseminate and store information, along with an increased potential for the inappropriate release of non-public data.

The information systems operated by Rice County for the conduct of business are the property and work environment of Rice County, and all Rice County policies relating to personal conduct apply to access to and use of these resources.

Security Principles: The County's basic security principles are to protect the confidentiality, integrity, and availability of the County's information and information resources. The County is entrusted with these assets and is accountable for their protection.

- Confidentiality means that information deemed sensitive or confidential is protected such that it is unavailable to those who do not have the necessary approvals to access it.
- Integrity means that information is correct and has not been altered or corrupted in some way during transmission, processing, or while in secure storage.
- Availability means that access to information and information systems is not denied to authorized users.

Security is critical to the success of technology initiatives, and as such will be given important consideration in systems design and use.

Scope

Applicability to Individuals: The following policies and guidelines apply to any individual ("User" or "Authorized User") that has been granted privileged access to County information, the information systems that contain or transmit that information (which includes but is not limited to computers, data and telephone networks, fax machines, printers and associated equipment and software), and the physical locations that house that information. This applies to protected information in all forms – verbal, written and electronic. Note that this includes both Rice County employees as well as non-employees with such access.

Applicability to Physical Facilities/Locations: These policies and guidelines apply, but are not limited to, the security of County information technology facilities, off-site data storage, computing systems, telecommunications, applications and related services and Internet-related applications and connectivity, regardless of the location or personnel responsible.

User Requirements

Information security is responsibility of all Users of Rice County information and information systems. Authorized Users are responsible to:

- Read and understand these policies and guidelines and updates as directed;
- Participate in training on the policies and guidelines as directed;
- Apply policy and guidelines to protect information according to its confidentiality;
- Protect against unauthorized disclosure, disruption, and corruption (intentional or otherwise);
- Use and disclose information only according to departmental policies or as directed by an immediate supervisor; and,
- Demonstrate compliance with the policies and guidelines at all times.

Security Controls

Access Authorization: Individuals are required to follow established Rice County access authorization procedures before gaining system access. See the IT department if you need assistance gaining authorized access to a Rice County system.

Passwords: Passwords used with Rice County Information Systems must follow the policies below. Passwords cannot be shared across multiple users or across multiple computer systems, unless expressly approved by the Rice County Information Security Committee and the IT Director.

Passwords will expire every 120 days, and a new password must then be selected. They should be of sufficient complexity so that they are not easily guessed. This includes characteristics such as:

- Passwords must use at least eight (8) alphanumeric characters. Whenever possible, Rice County information systems will be configured to require a minimum of eight (8) characters.
- Passwords cannot be reused within one year. When possible Rice County Information Systems will be configured to prevent re-use of a password within one year.
- Passwords should be in phrases, such as 'ilikeworking4ricecounty'. Passwords should not be obviously related to the user. This includes such items as spouse, children, pet names, nicknames, license numbers or phone numbers.

Users should take care to ensure privacy for themselves and others when entering passwords to ensure the passwords are not accidentally disclosed to those nearby.

Password notification must be handled in a secure manner and passed directly to the User or his/her supervisor, or through voicemail, but never through email. The initial password will be set to expire upon first login, requiring the User to change the password upon first login to ensure that the User is the only person with knowledge of the password.

In event of a suspected disclosure of a password, immediately contact the IT Department so that the password can be changed.

Information Requests: Rice County maintains public access points for information about the County, and for access to County records and information. These systems shall only be operated by persons specifically authorized and trained to place or remove data on such a system. Release of data to the public in other formats should be carried out through authorized channels.

New/External Software and Equipment: In order to prevent the loss, corruption or unauthorized disclosure of County information through the introduction of incompatible or non-policy-compliant equipment and software, software viruses, or other security vulnerabilities, Users are prohibited from:

- Downloading or installing any software or other materials from the Internet or other external or internal sources without the authority of the Rice County IT Director. This includes but is not limited to commercial software, shareware, freeware, or Internet-loaded plug-ins and patches.
- Modifying the hardware or software configuration of any computer or communications equipment except under the authority of the IT Director. This includes, but is not limited to the addition or removal of a modem to a computer or terminal, any hardware or peripheral (laptop, printer, scanner, disk drive, tape drive, memory), and any software or software configurations.

Computer Viruses: Files introduced into the Rice County information systems environment are required to be scanned for viruses before being opened or used. This includes files introduced through all external means, including computer disks, "jump" drives, Internet download and incoming email file attachments. Contact the IT Department if you need assistance with virus scanning.

Users should contact the IT Department immediately if a computer virus is suspected or confirmed to have infected their computer system. Only the IT Department Staff should attempt to destroy or remove a virus.

Unattended Computers: Users will either log off or lock their system when they will be away from the computer for any length of time. As a precaution, automatic logouts or password-protected screensavers shall be enabled after a period of 15-minutes of inactivity. Where possible, applications must be configured to log off the user after not more than 60 minutes of inactivity. Users are NOT permitted to change or disable the automatic logouts or screensavers without prior permission from their supervisor.

Preventing Disclosure: Users should be aware that potentially sensitive data may be displayed on a computer screen they are using, and should be alert to ensure that unauthorized individuals cannot read or modify data through a valid system login or session. Users may consider monitor placement or other solutions such as anti-glare screen guards to prevent unauthorized disclosure to individuals nearby.

Users should take care when printing sensitive, proprietary or otherwise controlled information, to retrieve the printed material in a timely manner to ensure that it is not available for unauthorized use or disclosure, and should not make extra copies of any Rice County or client information beyond what is required to perform official duties.

Remote Access and Wireless Access: In order to prevent unintended security vulnerabilities, as well as to ensure compatibility and proper configuration, remote access and/or wireless access to the County's internal network is only allowed through methods approved by the Rice County Information Security Committee, the User's department head, and in coordination with the Rice County IT Director.

Users provided such access must acknowledge the additional risks associated with it and are required to take every effort to protect the network, data and computing assets of Rice County, and acknowledge such efforts by signing an applicable access agreement. See the acceptable use policies below for further information about these types of access.

Security Incident Response

Users that become aware or have knowledge or suspicion of a compromise or attempted compromise of Rice County information systems or access controls are required to immediately report that knowledge or suspicion to their supervisor or a Rice County IT staff member. This will increase County system integrity by ensuring that even seemingly minor or trivial actions or system changes will not grow into major problems.

Policy Compliance

Responsibility: Supervisors are responsible to oversee use and to determine if uses of electronic systems are appropriate to assigned work, and to ensure compliance with this and other applicable Rice County policies.

Monitoring: The use and content of Rice County information systems can and will be tracked randomly and as deemed necessary under administrative procedures; externally under subpoena in reply to a request for public data or due to other legal actions; due to the unexpected absence of an employee; or for other business or technical reasons.

Disciplinary Action: Disciplinary action for intentional or unintentional violation of these guidelines is covered by the Rice County Personnel Policies.

Introduction: Rice County Acceptable Use Policies and Guidelines

The following policies and guidelines are in addition to those above, and further address appropriate use of Rice County information and information systems and the conduct of Users of those resources.

Careful Use: Rice County provides information systems including telephone, fax, Internet access and e-mail to efficiently conduct the business of the County. Use of these systems is granted by the department head with regard to job function.

Once given access, users are expected to use these systems in a responsible manner at all times, in a manner consistent with these and other applicable departmental and County policies and as directed by your immediate supervisor. All usage should be able to withstand public scrutiny without embarrassment to the County. Users with requirements that are outside of those typically provided are required to provide a business case to support their requests.

Personal Use: Limited personal use of Rice County information systems is permitted, provided such use:

- Does not impair the employee's workplace performance and production;
- Is done on the employee's personal time;
- Does not interfere with business usage;
- Does not contain harassing or threatening material;
- Is not performing work for profit, for personal gain, promotional use or solicitation;
- Does not incur direct additional County costs (for example by using County material such as printer paper, or through long-distance telephone use or cell phone use); and
- Does not contain abusive, profane or offensive language.

Personal use of e-mail and the Internet must not exceed 30 minutes per day. See your supervisor if you have any questions as to what constitutes limited personal use. Personal use of the Internet for streaming video, audio or instant messaging is strictly prohibited.

Use as a Privilege: Rice County can prohibit the use of any/all of this equipment or set limitations on its usage. The use of Rice County electronic communication and information systems is a privilege and not a right, and may be revoked at any time.

Inappropriate Use: Use of Rice County information systems for purposes other than official business or as permitted for limited personal use as outlined above is inappropriate. This includes but is not limited to participation in illegal activities, gambling, commercial activities, accessing sexually explicit or violent material; using the systems to harass or disable other systems, creation or distribution of virus or destructive programs, distributing pirated software or stolen data. Exceptions will only be granted with supervisory approval when such access and usage is required by a job assignment.

Content: Each user is responsible for the content of all text, audio and video they send over the Internet or phone systems. All messages should contain the user's identity, and should be written with the same professional manner as any hard-copy correspondence.

Users should demonstrate respect for intellectual property and ownership of information by stating authorship whenever possible. Users should respect their co-worker's right to privacy and to a workplace free from intimidation by their conduct when using these systems.

Rice County authorizes and maintains e-mail and servers for staff use. The use of County information systems, including email systems, for the development of documents, messages and other electronic files constitutes the creation of public documents that should be used in fulfillment of the governmental mission of the County. Personal and non-governmental-related information should not be stored on Rice County servers.

Records Retention: Rice County will establish and maintain a records retention policy consistent with MN statutes that all Rice County staff should receive training in and review periodically.

No Privacy: Users have no expectation of privacy in using Rice County information systems. Use of these systems to develop, store, or communicate information using these systems cannot be considered private or personal. Since records retention policies may apply to electronic communications, users should assume that even deleted email messages are retrievable at a later date.

Accountability: Ultimately, responsibility for the content of a message or transmission that does not conform to these guidelines is with the individual who creates that message and sends it.

Software Licenses: Rice County purchases software licenses for installation on all Rice County authorized systems. Installation on systems at non-Rice County facilities (including Rice County staff home systems) is not permitted.

In order to eliminate unlicensed or improperly licensed software on Rice County systems (and any corresponding legal liabilities), software licenses and pertinent information (such as sales receipts or paid invoices that represent proof of license) should be stored and maintained in a central location for all software owned by the County.

New Systems: All acquisitions of computing hardware, software, and services should be made in a coordinated fashion with the Rice County IT department. In addition to information protection, this effort promotes assurance: of compatibility with existing systems and infrastructure; that the business requirements of Rice County users are met; that acquisitions are obtained from reputable vendors; and, that appropriate anti-virus controls are in place and current.

This includes, but is not limited to all hardware, software and services such as printers, computers, CD drives, scanners, and PDAs; software such as Photoshop, Adobe Acrobat, Clipart, and drivers; services such as development, installation, maintenance and support.

Individual departments are responsible to:

- Complete requests for business requirements/functions (using required forms);
- Review requests with IT staff to determine requirements;
- Determine if specialized hardware or software is required;
- Assist with locating funding sources for the equipment.

The IT Department is responsible to:

- Assist departments in defining hardware/software requirements;
- Discuss equipment/software features and costs;
- Discuss the physical planning of the equipment/software;
- Discuss department's requirements for specialized hardware/software;
- Generate purchase orders and place orders for equipment/software.

Any hardware, software or service that has not been reviewed and authorized as the policy specifies will be disconnected and/or removed and will not be supported.

In addition, vendors, consultants or other agency representatives outside of Rice County must work in a coordinated fashion with the Rice County IT department in an approved secure manner. When possible, production changes should be installed and tested in a test environment prior to being installed into a production environment.

Remote Access and Wireless Access: Any form of remote access to a network increases the vulnerability of the network by creating a possible avenue for unauthorized persons to gain access and damage or otherwise compromise the systems and information on the network. Because of this, Rice County will only provide Users with remote access to its internal network through properly authorized and secured methods, and only with the prior approvals in the security policy presented above. Neither remote access nor wireless access is typical and therefore requires a business case and the completion by the User of a Rice County Remote Access Agreement or Wireless Access Agreement.

Support for remote access will be provided during normal business hours (Monday through Friday, 8:00am to 4:30pm). If issues arise with remote access outside normal work hours, they will be addressed the next business day. Any problems with Rice County access surrounding the connection will require the Rice County computer be brought to the Rice County office for resolution during normal business hours.

Rice County IT staff is not responsible for set up, installation, configuration or resolution of problems with the modem or broadband hardware, software or connection, or for off-site support for the modem or broadband connection.

Rice County Security and Acceptable Use Policy Signatures

I acknowledge that I have received training and read the Rice County Security and Acceptable Use Policy regarding the use of electronic systems at Rice County. I also acknowledge that I have had the opportunity to ask questions regarding the Security and Acceptable Use Policy.

Note: * is required field. Without this information the form will not be processed.

*_____ _____

User's Signature and Printed Name Date

*_____

Company Name (Third Party Vendors Only)

I acknowledge that I have made this Policy regarding the use of electronic systems available to the above-named person for review.

*_____ _____

Rice County Contact: Signature and Printed Name Date