City of Ripon
IT Security Policy

1.0 Overview and Purpose

In order for the City of Ripon to conduct government business as efficiently as possible, it is important to maintain the security and reliability of the City's Information Systems (computers, network, telephone, email, and other related systems). Recognizing the critical role of these Information Systems, this policy has been developed to provide clear expectations for acceptable use of the City's Information Systems.

This policy is not intended to impose restrictions that are contrary to the City of Ripon's established culture of openness, trust and integrity. The Information Technology Department is committed to protecting the City of Ripon's employees, partners and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security requires team effort and the support of every City of Ripon employee and affiliate who deals with information and/or Information Systems. It is the responsibility of every user to know this policy, and to conduct their activities accordingly.

2.0 Definitions

Information Systems	Collective term to encompass all City-owned IT Infrastructure, including computer terminals, servers, network switches, routers, firewalls, software, peripheral hardware, telephones, printers, fax machines, computer projectors, monitors, other displays, etc.
Web Browsing	Collective term for various activities such as reading websites, watching videos online, etc.
E-Mail	Electronic text, visual or audible communication to or from any user accessing the E-Mail system, including all information, data and attachments to the communication.
Blog	Short for we**blog,** an online personal journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Social Network	Collective term encompassing all websites dedicated to the sharing of personal information, photos, videos, etc.

Examples are Facebook, LinkedIn, Google+, Instagram, Vine, etc.

3.0 Scope

This policy applies to all City of Ripon Information Systems. All equipment and software are the property of the City of Ripon. This policy extends to all employees, agents, officers, contractors, temporaries, consultants, interns and any other worker regardless of employee pay, status, rank, or position, employed by the City of Ripon or any division thereof, who conducts business on behalf of the City of Ripon and to any third-party employees or contractors for the duration of their assignment with the City of Ripon (collectively, "Users").

Should an employee have any uncertainty about whether a specific action, behavior or activity constitutes a violation of this policy, they shall immediately contact their Department Head for clarification. In the event the Department Head is unable to provide clarification, the employee shall consult with the IT Administrator.

4.0 Policy Implementation4.1 General Use and Ownership

1. While the City of Ripon's IT staff desires to provide a reasonable level of privacy, users shall be aware that the data they create on City-owned systems remains the property of the City of Ripon. Inherent in the management of Information Systems is the need, from time to time, to access some or all files stored on data storage systems. Because of this requirement, IT staff cannot guarantee the privacy of information stored on any network device belonging to the City of Ripon.
2. Employees are responsible for exercising good judgment regarding "reasonable" personal use.
3. For security and network maintenance purposes, IT staff may monitor equipment, systems, files, databases, and network traffic at any time.
4. The City of Ripon reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Users are responsible for the security of their passwords and accounts. Do not share your password with anyone. Do not leave your password written on monitors, keyboards, desks, etc.
2. If another user needs access to resources to which you have access, they shall request access by contacting IT staff. It is not acceptable to log-in to a computer using your username and password to allow another individual access to information.

3. All PCs, laptops and workstations shall be secured when unattended. Securing the PC, laptop, or workstation shall be done by either logging-out, or activating the "Lock Workstation" option (Windows Key + L, or Ctrl+Alt+Del and clicking "Lock Computer").
4. Confidential Information shall only be transmitted via a secure means. Due to inherent lack of security controls, e-mail is not considered "secure means."
5. When releasing information to the public, employees shall use extreme caution to ensure that no private or confidential information is contained within documents being released. Employees of the Ripon Police Department shall refer to the Custodian of Records for clarification about whether specific information is confidential or not.
6. City e-mail accounts shall not be used when registering accounts for personal purposes (social networking, etc.) unless use of a specific service is considered "in the course of duty."
7. City e-mail accounts shall not be used for posting to newsgroups/forums, unless such posting is considered "in the course of duty."
8. If, in the course of business duties, a necessity arises, to connect personally-owned equipment or peripherals to the City of Ripon network, prior approval from the IT Administrator must be obtained. Any unauthorized equipment found connected to Information Systems will be disconnected without notice by IT staff.
9. Employees shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. In general, if an attachment is received from an unknown sender, it shall not be opened unless checked by a member of IT Staff.

4.3 Unacceptable Use

The following activities are generally prohibited.

Prohibited activities under this policy include, but are not limited to:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Ripon.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Ripon or the end user does not have an active license.

3. Physically exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. IT Staff must be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using City of Ripon equipment to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any City of Ripon account.
8. Users shall not conduct, facilitate, or participate in any behavior that disrupts, harms, or attempts to disable the whole or any part of the City's Information Systems.
9. If an employee is requested to perform an action on any Information System they feel may potentially be malicious or that may allow the third party to carry out malicious activity, the employee shall immediately contact IT staff to determine whether the action is permissible.
10. Bypassing user authentication or security of any host, network or account.
11. Providing information about, or lists of, City of Ripon employees to parties outside the City of Ripon.
12. Use of City of Ripon computer equipment, network connections, peripherals, or any other computer resource to download, view, print, or otherwise obtain pornography or other sexually explicit material.

Under no circumstances is an employee of the City of Ripon authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City of Ripon-owned computer, telephone or network equipment.

4.4 Social Networking as representatives of The City of Ripon

1. Employees shall not, generally speaking, engage in Social Networking activity in such a manner that they represent or appear to represent of the City of Ripon. Exceptions may be made by Department Heads, when such activity is desired and beneficial as public interaction. In cases where such activity is

approved, the Department Head and employee shall establish guidelines as to appropriate behavior, extent of information released, etc.

5.0 Appropriate use of the City E-Mail System

5.1 E-Mail as a transmission system

The E-Mail System shall be used for transmission and shall not be used for the storage of information. The E-Mail System is provided by the City to Users as a convenient and efficient method of rapidly communicating transitory information in an electronic format. Users shall be permitted to retain messages in e-mail for short periods to make day-to-day business communications easier and more efficient, however e-mail shall not be used to store messages long-term, once the business or project to which they pertain is completed.

5.2 Automatic Forwards

Automatically forwarding business-related E-Mails from Users' City E-Mail accounts to their personal E-Mail accounts is not allowed. Users are also prohibited from forwarding business E-Mails containing confidential information. Users are cautioned that any business E-Mail forwarded to a personal account may subject that personal account to a Public Records Act request.

5.3 Prohibited E-Mail Activities (in addition to those set forth in Section 4.3)

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or amount or size of messages.
3. Unauthorized use, or forging, of E-mail header information.
4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6.0 Mobile Devices

6.1 Security

When any device, whether personally or City-owned, accesses City services, such as E-mail, care shall be taken to provide an appropriate level of security for the information being accessed. Devices shall be secured with a password, and shall be equipped with some form of "remote-wipe" capability in the event the device is lost or stolen.

6.2 Personal use of City-Owned Devices

The same guidelines that apply to personal use of IT Assets apply to City-Owned mobile devices. Occasional, reasonable personal use is acceptable. IT Staff is not expected to assist or configure the City-owned device for applications or services which are strictly used for personal purposes. An example would be that IT staff is not expected to configure a Facebook account on a City-owned mobile device, or to recover personal photos stored on a City-owned device when a device is upgraded/replaced.

The device will remain the property of the City, and is to be returned to the IT division upon discontinuing use, whether leaving City employment, migrating to a new device, or otherwise.

6.3 Use of Personal Devices to access City Services

Use of personally-owned devices (smartphones, tablets, etc.) may be configured to access City services. IT Staff will provide assistance in the configuration of the device to the extent required to access City services. IT staff will not provide any other configuration of personal devices.6.4 In the event of loss/theft

In the event the personally-owned device is lost, stolen or otherwise compromised, the owner/assignee shall notify IT Staff immediately, to ensure accounts are secured against unauthorized access.

7.0 Enforcement

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

Offenses of insufficient gravity to merit termination will be handled on a case-by-case basis after coordination between the employee's supervisor and IT Administration.

8.0 Electronic Data Retention Policy

8.1 File and Application Server Backups

The City of Ripon IT Department maintains an ongoing backup system to provide disaster-recovery abilities. This backup system backs up data stored in department-common and user-specific data share locations, as well as server configurations and databases.

Because backups are focused on providing disaster-recovery protection, the ability to restore individual files or records from within a database will vary from system-to-system. Caution shall be used when deleting files.

8.2 Disk use quotas/limits

In general, the IT Department does not enforce disk-use quotas or limits. From time to time, staff may request users to review the data they store to ensure all data is necessary, current, and needs to be maintained. Should the need arise to reduce disk space consumed by user files, a member of IT Staff will consult with all users involved. IT Staff SHALL NOT ENGAGE IN DELETION/PURGING OF FILES without consulting Users before and during the process.

8.3 Files are stored until a User deletes them.

IT Staff shall not engage in purging/deleting files without User consultation. Responsibility shall be upon the User to determine which files are no longer needed. Any deletion/destruction of files shall be carried out in accordance with all relevant laws and sections of the government code, as well as according to the City of Ripon records retention policy.

8.4 E-Mail Messages

It is the City's policy that City E-mail and E-mail systems are intended to be a medium of communication. Employees shall exercise care and discretion in deleting messages which are no longer relevant/pertinent to active city business.

E-Mail messages shall be maintained only so long as to be useful as reference in ongoing communications and city business. Once the relevant business or project is completed or concluded, e-mail messages that need to become a retained record shall be printed and delivered to the City Clerk's office for filing as an official city record. Messages which do not need to be retained as a record shall be deleted promptly.

Employees shall take care in exercising regular maintenance of e-mail inboxes, with specific emphasis on deleting messages which are no longer current and relevant. Employees must remember that there is no expectation of privacy covering e-mail inboxes, contents of email inboxes can be accessed via discovery in the course of legal proceedings. Employees shall furthermore be advised that any information contained in a City of Ripon E-Mail account must be disclosed to any member of the public, should that member of the public make a properly formed request, under the California Public Records Act.

8.5 Interface with the Public Records Act

All "public records" (which generally means any writing, whether electronic or paper, that contains information relating to the conduct of the public's business) are governed by the mandatory public disclosure requirements of the Public Records Act and its exceptions (Gov't. Code §§ 6250 et seq.). Because information on the E-Mail System is automatically purged, the City considers

every E-Mail to be a preliminary draft (not retained in the ordinary course of business).

8.6 Retention of Electronic Data and Databases

With the increased use of electronic data, attention to the retention requirements for electronic records becomes extremely important. Other than Revenue Procedure 91-59, which recognizes electronic data interchange records and specifies that these records may be retained in electronic form unless a visible record is requested by a tax auditor, no other law at this time requires an organization to maintain both the electronic and hard copy form of the same information. You may, therefore, maintain records in any form unless the law either specifies the form or restricts the forms that can be used.

1. Databases

Databases consist of electronic files and fields of data that provide useful information to the organization. Typically, databases are modified over time through the addition, deletion, or modification of records. Reports are periodically prepared to reflect information from the databases that may be useful for specific purposes. Due to the large volume of information maintained in databases, reports rarely reflect all the information found in the database. Backups of databases, which are stored on City servers, are performed daily and would be used to restore the databases in case of accidental erasure or disaster.

Databases maintained by the City could include financial information, mailing lists, customer information, employee information, work order tracking, marketing information, records management information, etc. Since reports typically do not reflect the entire content of the database, the electronic form of the database contains different information than the visible reports. Electronic databases are often more useful than the paper reports, so visible reports are not equivalent to electronic databases.

For records retention purposes, a database is an official record of the organization. The retention period is established as “until superseded (SUP)" to reflect that only the current version needs to be maintained. Daily digital backup tapes are destroyed after four (4) days; weekly backup tapes are destroyed every three (3) weeks; and monthly backup tapes are destroyed on a rolling twelve (12) month cycle. Periodic reports, which are produced in hard copy format from a database and used for administrative, fiscal, legal or historical purposes, shall not be considered official records. These reports must be maintained for the requisite retention period according to the particular records series they are assigned.

2. Word-processing Files

Many organizational documents are prepared using word processing. A draft of the document is generally typed into the word processing system from hand-written notes or other materials, or transcribed from automated dictation devices. The word processing document is then printed and revised until the final printed version is accepted by the author.

For records retention purposes, the original notes and recorded media from dictation are non-records or work-in-progress. This version shall be destroyed in a relatively short period of time after the final draft has been accepted. Similarly, successive drafts of a document and the successive revisions of the electronic word processing file are non-records or work-in-progress. *Only the final approved, paper record shall be considered an official organization document.*

If the final product of the word processing process is a communication in an electronic mail system, the communication will only become an official record of the organization if the formalization process discussed above is followed.

For operational reasons, you may want to maintain some of the electronic-word processing files for extended periods of time to facilitate the revision of drafts. These decisions shall be made based upon the importance of the final document produced and the likelihood of revision or use of the material for other purposes. The word processing operator shall then destroy the computer version when it is no longer needed.

Word processing computer information is treated differently than databases. The computer information from a word processing file is printed letter-for-letter onto a final paper document, which in many instances is then signed. In essence, the paper document "mirrors" the information in the word processing systems and may contain authorizing signatures, so only the most useful version — the printed, paper version — becomes the official record and is retained in the normal course of business.

9.0 Revision History

1.0 Original Policy Created

2.0 June 24, 2009 – D. Brannon

Material from SANS Institute sample policy incorporated and updated.

Obsolete/deprecated material removed.

Definitions updated as appropriate.

3.0 April 30, 2013 – D. Brannon

Merged "Overview" and "Purpose;" added "Definitions"

Removed obsolete information; updated with new terms.

Added section 4.0 – Mobile Devices

3.1 Minor formatting updates; expanded definitions; edits for brevity and removal of superfluous language; incorporation of section 8.0 – electronic data retention and 5.0 – e-mail.

4.0 Incorporates comments and input from City Council, City Attorney, City Administrator and IT Administrator.

5.0 Simplified section 8.4, Unified directive to seek clarification from Department Head, misc. grammatical & language fixes.

5.0.1 Spelling Correction

Kevin Werner
Deputy City Administrator - City of Ripon