IT Resources Policy

Livingston County
Information Technology (IT)
Resources Policy
(Updated: July 2007)

LIVINGSTON COUNTY
Information Technology Resources Policy

This policy sets forth Livingston County's policies with regards to information technology ("IT") resources (e.g., computer hardware and software, e-mail, electronic voice and video communication, facsimile, the Internet and future technologies), including County access to review or disclosure of electronic files, electronic mail and electronic voice and video communications through or stored on any part of the IT resources systems. This memorandum also sets forth the policies on the proper use of the IT resources systems. These policies do not constitute a contract. The County reserves the right to change them at any time. In addition, the County reserves the right to rescind any individual's privilege to utilize IT resources. This Policy applies to all full-time, part-time, temporary, volunteer and contract employees of the County, as well as anyone with access rights to the computer network/computer equipment and/or other IT resources.

I. General Policy

The IT resources are intended to assist in the efficient and effective day-to-day operations of County departments or programs, including collaboration and exchange of information within and between County departments or programs, other branches of government and outside contacts. These resources also provide public access to certain public information.

The IT resources system is to be used for County-related purposes only. The County treats all information stored through or stored in these systems including, but not limited to, voice communication and e-mail messages, as County information.

The County has the capability to access, review, copy, modify and delete any information transmitted or stored in the system, including voice and e-mail messages. The County reserves the right to access, review, copy, modify or delete all such information for any purpose and to disclose it to any party if legally compelled to do so, or if the County otherwise deems it appropriate.

Those voice or other IT resources files containing personal information of an employee as a result of an employee's making incidental use of the IT resources system for personal purposes, including the transmission of personal voice and e-mail messages, will be treated no differently than other files, i.e., the County reserves the right to access, review, copy, modify, delete or disclose them for any purpose required by law, or which the County deems appropriate in its discretion. Accordingly, employees should not use the IT resources system to send, receive or store any information that they wish to keep private. Employees

should treat the IT resources system like a shared file system -- the files or messages sent, received or stored anywhere in the respective systems will be available for review by authorized representatives of the County and, may be disclosed to third parties.

To protect the integrity of IT resources, all authorized users of IT resources shall be granted a user account and password. The password may not be disclosed to anyone other than the County's IT Administrator, and must be changed at such intervals as the Information Technology ("IT") Department deems necessary. Further, internet access is strictly limited to those users who have requested and received approval to utilize the County Internet Account from both the Livingston County Administrator and the IT Department, upon request from the Department Head. The password for internet access may **NOT** be disclosed to anyone other than the County's IT Administrator.

II. Prohibited Uses of IT Resources

As stated above, IT resources are to be used exclusively for County purposes. Notwithstanding the foregoing, the following uses of the IT resources system are strictly prohibited, and violation of these policies may result in discipline, up to and including immediate discharge and, where appropriate, civil and/or criminal liability. The list of prohibited uses of IT resources is for illustration purposes only and is not intended to be all-inclusive and individuals may be disciplined, or subject to civil or criminal liability for matters not listed below:

1. Viewing, downloading or distribution of offensive or harassing statements, transmission of defamatory, obscene, offensive or harassing messages or messages that disclose personal information without authorization.

2. Viewing, downloading or distribution of incendiary statements which may incite violence or describe or promote the use of weapons or devices associated with terrorist activities.

3. Viewing, downloading, distribution or solicitation of sexually oriented messages or images.

4. Any use of County-provided IT resources for illegal purposes or in support of such activities.

5. Any use of IT resources for commercial purposes, product advertisement or "for-profit" personal activity.

6. Any sexually explicit use, whether visual or textual.

7. Any use for religious or political lobbying.

8. Duplicating, transmitting or using software which is not in compliance with software licensing agreements and/or unauthorized use of copyrighted materials or other person's original writings.

9. Installing or downloading personal or non-approved software on any IT system, including but not limited to internet file sharing software, screen savers and screen wallpaper;

10. Use of IT resources for the purpose, or which have the effect of, damaging the business or reputation of the County;

11. Wasting IT resources by, for example:

A. Placing a program in an endless loop;

B. Printing unnecessary amounts of paper;

C. Disrupting the use or performance of County-authorized IT resources or any other computer system or network;

D. Storing any information or software on County-provided IT resources which are not authorized by the IT Director;

E. Listening to Internet radio stations, as they create huge amounts of network traffic;

12. Security violations including, but not limited to:

A. Accessing accounts within or outside the County's computers and communications facilities for which you are not authorized or do not have a business need;

B. Copying, disclosing, transferring, examining, renaming, or changing information or programs belonging to another user unless you are given express permission to do so by the person responsible for the information program;

C. Knowingly or inadvertently spreading computer viruses;

D. Distributing "junk mail" such as chain letters, advertisements or unauthorized solicitations;

E. Misuse of another's password, negligent or intentional disclosure of the assigned password or any attempt to defeat the password

security;

F. Transmitting confidential or proprietary information without proper security and authority;

G. Disabling, tampering, modifying or failure to utilize the anti-virus program(s) installed by the County;

H. Allowing others access to our network through your account log-in and password.

III. Suggested Practices

It is suggested that employees undertake the following practices with regards to the use of the County's IT resources.

1. Confidential County Information: County employees must exercise a greater degree of caution in transmitting confidential information on the computer system than they make with other means of communicating information (e.g., written memoranda, letters or telephone calls) because of the reduced human effort required to redistribute information electronically. Confidential information should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information and should not be sent or forwarded to other employees inside the County who do not need to know the information.

Always use care in addressing e-mail messages to make sure that the messages are not inadvertently sent to outsiders or the wrong person inside the County. In particular, exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information. Individuals using lists should take measures to ensure that the lists are current.

2. Viewing and Protecting Electronic Files: In order to guard against improper dissemination of confidential information, employees should not access their computer for the first time each day in the presence of others. Confidential information should not be left open on the screen when a computer is unattended. In addition, do not leave floppy disks or back-up tapes containing confidential information out in the open. Keep them locked in drawers or filing cabinets.

3. Passwords: Employees must use passwords as made available by the County IT resources system to protect against unauthorized access to files on which they are working. (Note, however, that individual passwords do not prevent authorized County representatives from accessing those files). Access passwords should never consist of names, birth dates or

words that can be found in the dictionary. Passwords should combine letters and numbers and be routinely changed. Never disclose personal or system passwords to anyone other than authorized County representatives.

4. Attorney-Client Privileged Communications: Some of the e-mail messages or memoranda sent, received or stored on the system may constitute confidential, privileged communications between the County and its attorneys. Upon receipt of a message or memorandum from counsel or creation of a message to counsel, do not forward it or its contents to others inside the County without counsel's authorization. Never forward such messages or their contents to any third parties.

5. Copyrighted Information: Use of the computer system to copy and/or transmit software programs, documents or other information protected by copyright law is prohibited by federal law and may subject you and the County to civil and criminal penalties. Never copy software programs of any kind without express authorization from the IT Director. Never download copies of any software programs from any other employees or third party without approval from the IT Director.

6. Installation of Software: Since some software programs may be incompatible with the IT system or may contain viruses, do not install any software into the County IT system without prior approval of the IT Director.

7. E-Mail Etiquette: Please note that your e-mail and voice mail messages may be read or heard by someone other than the persons to whom they are sent and some day may be disclosed to outside parties or to a court in connection with litigation. Accordingly, please create and send messages that are courteous, professional and business-like.

IV. Use of the Information Services Department

You should contact the IT Network Manager if:

1. You receive or obtain information to which you are not entitled;

2. You become aware of breaches of security;

3. You learn of inappropriate use of County-provided IT resources;

4. Any threats to or against a County employee or County property should immediately be reported to the Livingston County Administrator and IT Director.

Please seek the advice of a person in the IT Department if you are in doubt concerning your authorization to access any particular IT resource.

To ensure that employees comply with these policies, the IT Department may conduct periodic audits of the IT system, including individual personal computers, floppy disks or back-up tapes. An employee's failure to comply with these policies may lead to disciplinary action.

Each County department or program shall review complaints or instances of unacceptable use brought to its attention. Violators are subject to corrective action and discipline, up to and including discharge, and may also be subject to civil prosecution or prosecution under state or federal statute.