15. INFORMATION TECHNOLOGY RESOURCES – ACCEPTABLE USE POLICY

15-1. PURPOSE OF COUNTY-PROVIDED INFORMATION TECHNOLOGY RESOURCES

The purpose of county-provided information technology (IT) resources (e.g. Email, software programs, facsimile, the Internet, and future technologies) is to support county agencies in achieving goals, and to improve County government in general. These resources are intended to assist in the efficient and effective day to day operations of county agencies, including collaboration and exchange of information within and between other county and state agencies, other branches of government and others. These resources also provide public access to public information.

Effective use of County-provided IT resources is important to Box Elder County. To help improve the effectiveness of your use of these resources, incidental and occasional personal use is permitted[1], as long as such use does not:

- Interfere with existing rules or policies pertaining to the agency
- Disrupt or distract the conduct of county business (e.g. due to volume or frequency)
- Involve solicitation
- Involve a for-profit personal business activity
- Have the potential to harm the county
- Involve illegal activities or violate this policy in any way
- Constitute an unacceptable use as defined in Appendix B

Note: Any resource used for personal use that incurs a cost must be reimbursed to the County.

15-2. PURPOSE OF THIS POLICY

The intent of this policy is to assure that:

1. The use of county-provided IT resources is related to, or for the benefit of, county government.
2. County-provided IT resources are used productively.
3. Disruptions to county government activities, because of inappropriate use of county-provided IT resources, are avoided.
4. The county government community is informed about confidentiality, privacy, and acceptable use of county-provided IT resources as defined in this policy.

[1] Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in such judgment by providing the above guideline. If you are unclear about the acceptable "personal" use of a county-provided resource or wish to use the resource for what may be considered as a good cause, seek authorization from the appropriate authority.

This Policy is not meant to be a straightjacket on the use of these resources. Rather, the intent is to create an environment where communication can flow freely and with a minimum of policing. This policy should not discourage county agencies from using county-provided IT resources.

Refer to the following appendices for detailed information:

Appendix A – Responsibilities
Appendix B – Unacceptable use of IT Resources
Appendix C – Overview of Technologies

15-3. PRIVACY ISSUES AND LEGAL IMPLICATIONS

The county has the right to access and disclose the contents of electronic files, as required for legal, audit, or legitimate county operational or management purposes. Do not transmit personal information about yourself or someone else using County IT resources unless you have prior proper authorization. The confidentiality of such material cannot be guaranteed. Email and other electronic files may be accessible through the discovery process in the event of litigation. Each of these technologies may create a "record" and therefore are reproducible and subject to judicial use.

15-4. RETENTION/DISPOSITION OF ELECTRONIC RECORDS

Just as with any other government record, electronic records are retained or disposed of in accordance with Government Records Access and Management Act (GRAMA). Refer to GRAMA or seek information from the County Recorder/Clerk for guidance in this area.

15-5. WARNINGS/CORRECTIVE ACTIONS

Box Elder County shall review complaints of instances of unacceptable use brought to its attention. Violators are subject to corrective action and discipline including termination.

15-A. APPENDIX A – RESPONSIBILITIES

1. Access only files, data and protected accounts that are your own, that are publicly available, or to which you have been given authorized access.
2. Use IT resources efficiently and productively. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, or other IT resources.
3. Be responsible for use of your own accounts. Under no condition should you give your passwords to another person. Guard yourself against unauthorized access to your accounts:
    - Change your passwords with regular frequency or in accordance with the County policy regarding the frequency of changing passwords.
    - Do not use obvious passwords.
    - When you are away from your desk, take precautions to protect your accounts.
4. Report to the agency's appropriate authority if you:
    - Receive or obtain information to which you are not entitled (Note: Also notify the owner or sender of such information).
    - Become aware of breaches of security, or
    - Know of any inappropriate use of County-provided IT resources.
5. Seek the advice of the authorized person responsible for any County-provided IT resource if you are in doubt concerning your authorization to access that resource.
6. Adhere to copyright law regarding use of software, information, and attributions of authorship.
7. Conduct yourself as a representative of Box Elder County as a whole. As a minimum, this means that you shall not use IT resources to:
    - Distribute offensive or harassing statements; disparage others based on race, national origin, sex, sexual orientation, age disability or political or religious beliefs.
    - Distribute incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities.
    - Distribute or solicit sexually oriented messages or images.

15-B. APPENDIX B – UNACCEPTABLE USE OF IT RESOURCES

The first and foremost rule of using these technologies is:

> *Don't say, do, write, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare.*

Any use of County-provided IT resources for inappropriate purposes, or in support of such activities, is prohibited (unless authorized through job responsibilities). The following list is currently considered unacceptable use of County-provided IT resources.

1. Illegal Use. Any use of county-provided IT resources for illegal purposes, or in support of such activities. Illegal activities shall be defined as any violation of local, state, or federal laws.
2. Commercial Use. Any use for commercial purposes, product advertisements or "for profit" personal activity.
3. Sexually Oriented. Any sexually oriented use, whether visual or textual. You shall not view, transmit, receive, save, or print any electronic files which may be deemed as sexually oriented.
4. Religious or Political Lobbying. Any use for religious or political lobbying, such as using Email to circulate solicitations or advertisements.
5. Copyright Infringement. Duplicating, transmitting, or using software not in compliance with software license agreements. Unauthorized use of copyrighted materials or another person's original writings.
6. Unnecessary Use of IT Resources. Wasting IT resources by intentionally:
   - Placing a program in an endless loop.
   - Printing unnecessary amounts of paper.
   - Disrupting the use or performance of county-provided IT resources which are not authorized by the agency.
   - Storing any information or software of county-provided IT resources which are not authorized by the agency.
7. Security Violations.
   - Accessing accounts within or outside the county's computers and communication facilities for which you are not authorized.
   - 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 user responsible for the information or programs.
   - Violating the privacy of individual users by reading Email or private communications unless you are specifically authorized to maintain and support the system.
   - Representing yourself as someone else, fictional or real.
8. Viruses. Knowingly or inadvertently spreading computer viruses. "Computer viruses" are programs that can destroy valuable programs and data. To reduce the

risk of spreading computer viruses, do not import files from unknown or disreputable sources. If you obtain software or files from remote sources, follow proper procedures to check for viruses before use. You should adhere to any county-specific policy in this area.

9. Junk Mail. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations.
10. Confidential Information. Transmitting classified information under the Government Records Access and Management Act without proper security.[2]

[2] Use caution when sending classified information. Always display "Confidential" on the screen when sending classified information. Confirm that encryption has been enabled. Inform the recipient of the information's classification, their responsibility to keep it private, and their responsibility to dispose of it in a secure manner at the end of its retention period.

15-C. APPENDIX C – OVERVIEW OF TECHNOLOGIES

The following are examples of technologies that this policy governs. As new technologies gain popularity and use, they too will be governed by this policy. This overview will increase understanding of these technologies as they relate to creating electronic records. Each of these technologies creates an electronic record. This is what separates these from other forms of communications such as a telephone conversation. An electronic record is reproducible and therefore deserves special recognition.

15C.1 EMAIL

Email is a major means of communication in county government and offers an efficient method of conducting county business. Email, as defined in this document, consists not only of the county-provided Email system, but also the act of sending and receiving Email through the Internet.

There are a number of characteristics that distinguish Email from other means of communication, such as paper records, telephones, and information stored on electronic media such as diskettes. Awareness of these characteristics should guide your use of Email.

1. Backups. As part of standard computing and telecommunications practices to prevent loss of data, Email systems and the systems involved in the transmission and storage of Email messages usually are "backed up" on a routine basis. This process results in copying data, such as the content of an Email message, onto stored media that may be retained for periods of time and in locations unknown to the sender or recipient of a message. The frequency and retention of backup copies vary from organization to organization. While it may be difficult and time consuming, it should be assumed backup copies of Email messages exist and can be retrieved, even though the sender or recipient has discarded his/her copy of a message.
2. Special Status. While password protecting your Email account is beyond usual measures taken to protect access to paper records and telephones, it does not confer a special status on Email records with respect to applicability of laws, policies, and practices.
3. Monitoring. In the course of their work, managers, supervisors, network and computer operations personnel or system administrators may monitor the network or Email system. It should be assumed that the content of Email messages may be seen by these authorized individuals during the performance of their duties.
4. Forgeries. No system of communication is completely secure, including Email. An Email message can be forged, and it can be distributed beyond the address list originally defined by its author.

5. Viruses. Executable files (e.g., *.exe, *.com) can be transmitted via Email. You must always check executable files attached to Email messages for viruses before they are executed on county-provided IT resources.
6. Legal Implications. Email and other electronic files may be accessible through the discovery process in the event of litigation.

15C.2 FACSIMILE (FAX)

Fax machine, in the past, simply created a paper copy of the original message. With today's technology, this is becoming less and less true; an electronic copy may be created. The same rules governing acceptable use of other county-provided IT resources also apply to the use of fax technology. The faxed message may be "backed up" onto other storage media. As with other technologies, the content of faxed messages may be seen by authorized individuals during the performance of their duties.

Use of fax technology does not always require a password for access. Recipients should not assume that the sender is always as reported. A fax should always be perceived as a non-private communication method. Remember, anyone at the other end may read your fax.

15C.3 INTERNET

The Internet provides the ability to communicate, collaborate with others and access information throughout the world. However, there is little in the way of hierarchy or control of the information available. Increased access to computers and people all over the world also brings the availability of controversial material that may not be considered of value to an individual or the county, and may violate this policy.

Even if you are able to encrypt your data, anything you transmit over the Internet is subject to interception, reading, and copying by other people. This includes Email, personal information and passwords that are transmitted when you log into an account or log into another computer.

15C.4 VOICE MAIL

Voice mail is a means of communication that is in and of itself unique. It is similar to a telephone conversation, but it creates a "record." This should always be remembered by anyone using this technology. The sender must remember that the message can also be saved, replayed, and shared with others that the sender did not intend. It also can be used in litigation. The same rules of password protection and confidentiality that concern other technologies also apply here.

15C.5 EMERGING TECHNOLOGIES

This policy does not address the specific details of technologies that are yet to be invented or implemented with State and County government. This policy should be sufficient to allow you to determine the acceptable use of any new or emerging technology. If you have any questions regarding appropriate use of a particular technology not specifically covered in this policy, please contact the appropriate individual in the County agency.