Taylor County
Board of County Commissioners
Policy Manual

Policy #:	Title:	Effective Date:
2010-10	**Network Acceptable Use Policy**	**07/06/10**

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment and systems at Taylor County Board of County Commissioners (TCBCC). These rules are in place to protect the TCBCC and its employees. Inappropriate use exposes the TCBCC to risks including virus attacks, the compromise of network systems and services, and legal issues.

REFERENCE

Not Applicable

POLICY

General Use and Ownership

1. While the TCBCC network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the computer systems remains the property of the TCBCC. Because of the need to protect TCBCC network and public records laws, management cannot guarantee the confidentiality of information stored on any network device belonging to TCBCC.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there are any questions please contact the Technology and Information Systems (TIS) department.
3. For security and network maintenance purposes, authorized individuals within the TCBCC may monitor equipment, systems and network traffic at any time.
4. The TCBCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either public record or confidential, as exempted by state constitution Section 119.07(6), F.S. Examples of confidential information include but are not limited to: Employee social security numbers, SHIP applicant information, emergency procedures, and public safety information. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure. The sharing of user accounts and password are not permitted without the express permission of the Director of Technology and Information Systems (TIS). Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less (Windows 9x users), or by logging-off (control-alt-delete for Win2K, XP users) when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. All hosts used by the employee that are connected to the TCBCC Internet/Intranet/Extranet, whether owned by the employee or TCBCC, shall be continually executing Department of Technology & Information Systems (DTIS) approved virus-scanning software with a current virus database.

Unacceptable Use

Under no circumstances is an employee of the TCBCC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TCBCC-owned resources.

The lists below are by no means exhaustive, but attempt to provide examples of activities of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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 TCBCC.
2. Knowingly 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 TCBCC or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should 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 a TCBCC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Port scanning or security scanning is expressly prohibited unless prior notification to DTIS is made.
9. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
13. Providing information about, or lists of, TCBCC employees to parties outside TCBCC unless done as part of an authorized public records request.

Email and Communications Activities

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, Voice over Internet Protocol (VoIP) telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. If you receive an email in which you do not recognize the sender and suspect it may have a virus attached contact the (TIS) department for further instructions before opening the attachment or email..
7. All county email correspondence will be performed using a BOCC DTIS approved email application.

Preview panels in the email application shall be turned off to help prevent virus infections.

Enforcement

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

RESPONSIBLE DEPARTMENT

Technology and Information Systems

SUNSET DATE

Sunset Date: 03/01/2019

Revision Date: 10/01/2015