

Board of County Commissioners

Escambia County, Florida

Title: Information Technology Use Agreement (ITUA)
Date Adopted: September 21, 2017
Effective Date: September 21, 2017
Reference:
Policy Amended:

Information Resources are provided by the Escambia County Board of County Commissioners (BCC) to support the business of local government. The term "Information Resources" includes all BCC hardware, software, data, information, network, computing devices, phones, and other information technology. To use BCC Information Resources, you agree to adhere to the provisions of this Policy Agreement (Agreement) which are established to ensure security and inform you of the conditions of use.

A. Purpose

The purpose of this Agreement is to set forth the policies and procedures with respect to Internet, Computer, E-mail, and Information Resources, and to give specific and general authority to the Escambia County Information Technology Department (IT) with regard thereto. This Agreement is designed to protect the County, its employees, and its resources from the risks associated with the usage of Information Resources. The provisions of this Agreement are applicable to the County, its elected officials, officers, employees, and all Users of all County Information Resources.

B. Appropriate Use

1. Use for BCC Business

I understand that Information Resources are to be used primarily for the business of the BCC with exceptions limited to those provided by BCC Ethics Rules, Social Media Policy, and my department's policies. I understand that not all personal use of e-mail and the Internet is forbidden. Reasonable personal use is a privilege and is permitted consistent with the provisions of this Agreement and other applicable County policies. Non-County business related e-mail and internet usage is permitted, provided such use is brief, does not interfere with work, does not subject the County to any additional costs, and is otherwise consistent with the requirements set forth in this Agreement. With prior permission of his or her supervisor, an employee is permitted to briefly visit non-inappropriate sites during non-work time such as during break or lunch time. I understand that abuse of this privilege resulting in excessive or disruptive personal use or access to inappropriate sites may result in revocation of personal use privileges and disciplinary action.

2. Approved Information Resources

I shall only use Information Resources owned, licensed, or being evaluated by the BCC to conduct BCC business. I shall not use my personal Information Resources for BCC government business at BCC facilities (excludes personal cell phones and tablets when authorized by your department). I shall not use Information Resources provided by a third party to conduct BCC business unless authorized by the BCC Information Technology (IT) department.

3. Protecting from Misuse & Damage

I shall use care in protecting against unauthorized access, misuse, theft, damage, or unauthorized modification of Information Resources. I shall not leave a workstation without first ensuring it is properly secured from unauthorized access. I shall use good judgment to safely transport and store Information Resources in and away from the workplace. I understand that while I am actively logged in to any BCC Information Resource device, I am solely responsible for all activity and all use of the BCC Information Resource. If I fail to secure my workstation and unauthorized access occurs, I understand that I will be deemed responsible for that access and that I may be subject to disciplinary action for the failure to secure Information Resources whether such failure results in unauthorized access.

4. Public Disclosure & Monitoring

I understand that any information created, accessed, or stored on Information Resources may be subject to public disclosure. The BCC reserves the right to monitor all use of Information Resources, including my e-mail and Internet use, and I have no right or expectation of privacy with respect to my use of Information Resources. Computer Passwords are for security purposes only and are no guarantee of the privacy or confidentiality of any user's utilization of County Information Resources.

C. Prohibited Activities

I understand that activities prohibited by this Agreement may not be permitted without the prior written approval of the IT Director. Prohibited activities include:

1. Unauthorized Disclosure of Confidential Information

I shall not disclose confidential information to unauthorized parties. Confidential information includes but is not limited to social security numbers, driver's license numbers, financial account information, credit card numbers, and personal health information. I acknowledge that certain information is confidential or discretionary by law, and it is my duty to protect that information from unauthorized disclosure.

2. Unauthorized Software

I shall not download or install any software outside of the BCC standards. Privately purchased or downloaded software without a legitimate BCC purpose or authorization is forbidden. Banned software includes, but is not limited to, sniffers, password crackers, games, screen savers, and peer to peer.

3. Violation of Law

I shall not use the Information Resources to violate any law, including copyright or other intellectual property law. I shall not copy, share or distribute software without authorization.

4. Unauthorized Use

I shall not permit unauthorized users to use the Information Resources that the BCC has provided me. I shall promptly report any unauthorized use to my manager or the IT Director.

5. Access

I shall not share my password or access code to BCC Information Resources with any other person. I shall not use another person's password or access code. I shall not access or attempt to access information for which I have no authorization or business need. I shall connect to the BCC network only through approved services (e.g. – Citrix and VPN are approved; a direct dial-up connection to a work PC modem is prohibited). I shall not access another person's email, workstation, or social media/networking account/address, if not specifically authorized to do so.

6. Remote Control

I shall not use any remote-control software or service on any internal or external host or systems not specifically approved by agency management, IT support, and the IT Director.

7. Circumvention of Security Measures

I shall not bypass or attempt to bypass measures in place to protect Information Resources from security threats and inappropriate use. I shall not disable software on computing devices designed to protect Information Resources.

8. Unauthorized Devices

I shall not place unauthorized computing or network devices on the BCC network (e.g. – computers, access points, etc.).

9. Unjustifiable Use of Resources

I shall not intentionally sustain high volume transactions or network traffic for non-business purposes. I shall not send or reply to messages that would negatively impact the performance of the email system (e.g. – “replying to all” on a message received in error or distributing chain letters). I shall refrain from actions that hinder others' use of Information Resources or that may increase BCC costs.

10. Harassment

I shall not use Information Resources to harass, intimidate, or threaten another person.

11. Inappropriate Material

I shall not use Information Resources to access or distribute any obscene, sexually explicit, pornographic, abusive, libelous, defamatory, or any other material deemed inappropriate for the workplace.

12. Disruptive Material

I shall not use Information Resources to access or distribute any material that is disruptive, offensive to others, harmful to morale, abusive, or that contains ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement to others based on race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs. I shall not use Information Resources in any manner which reflects unfavorably upon the image of the County.

13. Identity

I shall not use Information Resources to impersonate another user or to mislead a recipient about one's identity.

14. Official Position

I shall not use Information Resources to communicate the BCC's official position on any matter, unless specifically authorized to make such statements on behalf of the BCC.

15. Solicitation

I shall not use Information Resources to solicit or proselytize others for commercial ventures, religious or political causes, or other non-work-related solicitations.

D. Storage of Information

I shall store BCC owned information only on BCC provided storage media. Storage of BCC information on non-BCC owned PCs, laptops, flash drives, CDs and other forms of media is prohibited. I shall not store BCC owned information resources on the Internet without express agency authorization. With appropriate authorization, I may access and store BCC email messages on my personal cell phone or tablet. The storage of personal or non-business music and video files on BCC provided storage is forbidden.

1. Adherence to Security Guidance

I shall ensure that security fixes and updates for my BCC provided resources are implemented consistently and promptly, as directed by IT.

2. Spam/Phishing Awareness

I shall be aware of the characteristics of spam and phishing messages. I shall recognize and dispose of spam/phishing messages appropriately. I shall never provide my login ID and password in response to an email or phone solicitation unless I have verified that the request is from the BCC or IT. I shall not risk a malware infection by navigating to links embedded in spam messages.

3. Violations & Uncertainty

I shall report violations of this Agreement to my manager or the IT Director upon learning of such violations. If I am uncertain whether an activity is permissible, I will refrain from the activity and obtain authorization from my manager before proceeding.

4. Violation of Policy Agreement

I am aware that any inappropriate use of Information Resources or my failure to comply with this Agreement may result in disciplinary action, up to and including immediate dismissal from employment, criminal prosecution where the act constitutes a violation of law, and an action for breach of contract if applicable. Additionally, users found to be in violation may be no longer permitted use of Information Resources.

5. Information Technology

The County Information Technology Department shall have the discretionary authority, as set forth herein, to audit, inspect, and/or log Information Resources and block non-work-related Internet access, consistent with this Agreement.

- a) Logged and Blocked Access. IT maintains the right to utilize software to identify and/or block access to Internet sites containing sexually explicit or other material deemed inappropriate for the workplace and to log all aspects of use of the County's Information Resources.
- b) Direct monitoring of Internet and e-mail usage may be conducted by IT at the request of any supervisor, the County Administrator, any County Official, the Human Resources Department, or the County Attorney's Office.

6. Communication of the Policy to Employees and Users of Information Resources

I understand this policy will be updated, as necessary, the BCC will make reasonable efforts to inform me of the changes. The Information Technology Department shall be responsible for ensuring that the Policy is updated from time to time as necessary. The Human Resources Department (HR) shall be responsible for communicating this Policy Agreement to all BCC elected officials, officers, and employees, and providing copies of this Policy Agreement to newly hired employees (including seasonal, recreational program employees). A copy of the signed Agreement shall be included in each employee's official HR file.

7. Receipt and Acknowledgement

I have been provided with a copy of the Information Resources Use Agreement. I have read the Agreement and agree to abide by its policies. I understand that I have no expectation of privacy in any usage of Information Resources. I understand that violation of the terms of this Agreement may result in disciplinary action, up to and including termination of my employment. Violations of local, state, and federal laws may carry additional penalties.

Printed Name: _____ Signature: _____

Job Title/Department: _____ Date: _____