



BOARD OF COUNTY COMMISSIONERS

POLICY

Number: BCC-32
Cancels: ~~08/14/2021~~ 01/11/2022
Approved: 01/11/2022
Originator: Information Technology
Review: 01/11/2025

TITLE: Acceptable Use of Technology Resources

I. Objective

The purpose of this Policy is to outline the acceptable use of technology resources and tools provided by the Board of County Commissioners (BoCC). These tools include, but are not limited to, County computing equipment and software, data networks, internet access, and electronic messaging systems. Resources also include electronic data contained within or transmitted through BoCC networks and storage locations. This Policy is in place to protect the BoCC and County employees from exposing County technology resources and tools to any possibility of compromising ~~its~~their confidentiality, integrity or availability.

This Policy applies to any BoCC user. In this document, the term user refers to any County employee (permanent or temporary), contractor, consultant, vendor, volunteer, student intern, grant partner, or other person, who uses, maintains, manages, or is otherwise granted access to County Information Technology Department (ITD) resources. This includes access at a BoCC facility or elsewhere, and refers to all ITD resources whether individually controlled or shared, standalone or networked.

Employees are accountable for all activities while in possession of any of the County's technology tools and resources. Any employee found to have violated this Policy may be subject to disciplinary action, as specified by the Merit System Disciplinary Actions Policy (MS Policy 12, *Disciplinary Actions*).

II. Definitions and References

A. Definitions

1. Technology resources or Information Technology (IT) resources - All County-owned computing equipment and software, mobile devices, data networks, internet access, electronic messaging systems, and proprietary County electronic data.
2. County user - Any County employee (permanent or temporary) contractor, consultant, vendor, volunteer, student intern, grant partner, or other person, who uses, maintains, manages, or is otherwise granted access to County IT resources.
3. Incidental use - Personal use of an information technology resource before

work, after work, during breaks and lunch that does not interfere with completing work assignments.

~~3.4.~~ ITD or Information Technology Department - the Brevard County Information Technology Department.

~~4. ITD Director - the Director of the IT Department.~~

5. Malicious programs or malware - Any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.
6. Network- ~~workstations and~~ connections of ~~computer workstations devices~~ to ~~servers or any other~~ computer systems through a local or wide area network, Internet, or modem connection.

~~7.~~ Personal Identifiable Information (PII) - pursuant to Section 501.171, Florida Statutes, as may be amended, personal information means either of the following:

~~7.-~~

- a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (i) a social security number; (ii) a driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (iii) a financial account number, credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (iv) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- b. A ~~user name~~username or email address, in combination with a password or security question and answer that would permit access to an online account.
- c. The term does not include information about an individual that has been made publicly available by a federal, state, or local government entity.

B. ~~B.~~ References

1. Florida Statutes Section 119.071, as may be amended - General exemptions from inspection or copying of public record.
2. Florida Statutes Section 281.301, as may be amended - Safety and Security

Services: Security Systems; records and meetings exempt from public access or disclosure.

3. Florida Statutes Section 815.06, as may be amended - Florida Computer Crimes Act: Offenses against users of computers, computer systems, computer networks, and electronic devices.
4. Florida Statutes Section 501.171, as may be amended - Security of confidential personal information.
5. Brevard County Administrative Order AO-47, *Coordination of Public Records Requests*.
6. Merit System Policy 12, *Disciplinary Actions*.
7. Brevard County Policy BCC-22, *Records Management Program*.
8. Brevard County Administrative Order AO-31, *Email Storage & Retention*.

III. Directives

A. General Directives

BoCC aspires to maintain secure access for its officials, constituents and users to both internal and external information with regard to County government processes, including relevant information garnered from local, state, national, and international sources. In addition, the County seeks to provide an atmosphere that encourages access to knowledge and information sharing that is consistent with the mission and objectives of County government.

BoCC recognizes the importance of reliable information to ensure legal compliance, accountability, and promote open and transparent government. It is essential that users take necessary care when creating or entering data into government systems.

Use of technology resources should be consistent with the job function and specific objectives of the project or task(s) for which access to the resources was granted. All uses inconsistent with the objectives outlined below are considered to be inappropriate and unauthorized, and may jeopardize further access to services and result in disciplinary or legal action.

1. All computer information designs, programs, and data created utilizing BoCC technology resources are the property of BoCC.
2. All computer use, including Internet use, on BoCC networks is subject to monitoring, shall be monitored.

B. Use of County Computing Equipment and Software

1. No BoCC owned or leased computing equipment shall be used for purposes other than official business and following the appropriate usage procedures.
2. When using assigned technology resources, access to these resources must

be gained securely using previously assigned user accounts and passwords. The Information Technology Department is responsible for assignment, management and auditing of user credentials.

3. Products that are not appropriately licensed for use by the County or those that violate the rights of any person or organization 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", personally owned or other software, shall not be installed or used on County equipment.
4. Unauthorized copying of copyrighted material, including, but not limited to, digitization, copying or distribution of photographs from magazines, books, Internet web pages or other copyrighted sources, copyrighted music, copyrighted digital media files, and the installation of any copyrighted software for which the County or the end user does not have an active license, is prohibited.
5. Use of software shall be in a manner which is prescribed and permitted by the accompanying documentation and licensing agreement(s).
6. Computer equipment, ~~system files, or software programs~~ shall not be removed from County property, ~~reproduced, or used in any way to duplicate software~~, unless specifically authorized by department or office management.
7. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws is illegal, and all users shall consult the appropriate management prior to exporting any material that is in question.
8. Intentional introduction of malicious programs into the network or any computing device (e.g., viruses, worms, Trojan horses, root kits, email bombs, etc.) is prohibited.
9. Storage of personal content or information, such as music, photos, or other documents that are not related to County business, is prohibited. The Information Technology Department is not responsible for the loss or backup of such ~~content~~content, and the content may be subject to immediate deletion.

C. ~~C.~~ Use of BoCC Data

It is the duty of each user to protect BoCC data that is designated as sensitive or confidential by the Department Director of the department or office that owns the data, as delineated in Brevard County Policy ~~BCC-#22~~BCC-#22, *Records Management Program*, and Brevard County Administrative Order ~~AO-#47~~AO-#47, *Coordination of Public Records Requests*. As such, County users will abide by the following policy:

1. BoCC users must use BoCC secure, private network storage service to store and transfer BoCC data. No public cloud storage services, such as Dropbox, Google Drive, or personal Microsoft OneDrive, may be used for this purpose unless approved by the ITD Director, or their designee. BoCC OneDrive is acceptable and recommended for individual storage.

2. Only storage dedicated to department shared drives and individual BoCC OneDrive are routinely backed up.- **Local machine storage is not backed up.**
3. All email and data made or received pursuant to law or ordinance or in connection with the transaction of official business of the County transmitted over the County network is considered County data and shall be transmitted only to individuals who have a business need to receive them. Users shall have no expectation of privacy in personal communications over County computers or networks, including facsimile machines.
4. For security and network maintenance purposes, authorized employees within the Information Technology Department may monitor and audit County data systems on a periodic basis to ensure compliance with this Policy.
5. County users must promptly report the theft, loss, or unauthorized disclosure of BoCC proprietary information to management as soon as they become aware of the transgressionincident.

D. ~~D.~~ Use of Electronic Messaging and Internet

1. Users' communications on County electronic systems shall be professional and courteous. Users must exercise good judgment in their communications.
2. Email and Internet access are provided for County business use; incidental use for informal and/or personal purposes may be permissible only within reasonable limits. Departments or offices may have more stringent policies regarding such use(s) and said policies should be consulted for specific guidance.
3. The County's email system is not intended as a document management or document retention system. Users must follow guidelines provided in Brevard County Administrative Order AO-#31,- Email Storage & Retention, on proper email management and retention.
4. Users shall not use County network or computerIT resources for commercial financial gain or to conduct and/or support personal business ventures.
5. Users shall not send email messages to all County users without specific authorization by the County Manager's Office. Email messages shall not be sent to large distribution lists, entire Departments, Offices, or Programs without authorization by the Department Director. Discretion should be used when sending emails to a large number of users. Authorized messages with broad distribution shall minimize the size of the message, limit the size and number of attachments, and restrict the use of embedded images. Any announcement which any user wishes to make utilizing County email that is not strictly related to County business shall be approved in advance by his or her Department Director.

E. ~~E.~~ Unacceptable Use

Information technology resources shall not be used for purposes other than those that support official County business. However, incidental use of BoCC email and internet may be permissible, as outlined in this document. Access to and use of

BoCC's technology resources is a privilege, shall be treated as such, and shall be used in a manner that respects the public trust and abides by established policy and regulations. Further, access to the technology resource infrastructure ~~both within BoCC and beyond~~ requires that each and every user accepts responsibility to protect the rights of other County users and the public they serve.

1. Each person granted access to BoCC network resources shall be responsible for the content, syntax, and format of all text, audio, or images that he/she may place upon or send over the network. All users shall conduct themselves with the same integrity in electronic interactions as they would in face-to-face dealings with one another and shall not:
 - a. Make unauthorized use of any technology resource.
 - b. Make unauthorized copies of any software, license codes, information, communication, data, or digital media.
 - c. Seek personal benefit or permit others to benefit personally from the use of BoCC technology resources or confidential information acquired through the use of those resources; nor operate or request others to operate any BoCC technology resource for personal business.
 - d. Knowingly ~~or intentionally~~ include, directly or indirectly, a false, inaccurate, or misleading entry in any record or report, or enter information in a computer file or database that is known to be false and/or unauthorized.
 - e. Divulge assigned login credentials to anyone. In the case of requiring access to another user's data, please contact the ITD help desk for assistance.
 - f. Provide any non-authorized person access to information or permit such persons the use of BoCC technology resources.
 - g. Intentionally use irresponsibly, destroy, alter, dismantle, or disfigure the County's information technologies, properties, or facilities, including those owned by third parties.
 - h. Make any modification to BoCC computer equipment, systems files, or software, including the installation of any non-standard software on any BoCC workstation, without approval from the ITD Director, or their designee.
 - i. Add, move, or change any networking or computer equipment.
 - j. Connect any personal computer, laptop, or mobile device to the County network unless using an approved user account; exceptions to this may be requested through the ITD Director, or their designee.
 - ~~k. Change computer information without being the data owner or having proper authority to change that information.~~
 - l.k. Make copies of County electronic data files without a valid business reason or expressed written approval from the Department Director, or

their designee.

~~m.l.~~ Transmit personal information without encrypting the information as required per HIPAA regulations or Section 501.171, Florida Statutes, as may be amended.

~~n.m.~~ Send electronic communications which hides the identity of the sender or misrepresents the sender as someone else.

~~e.n.~~ Jeopardize security, confidentiality, or potentially subject the County to litigation as a result of violating any County policy or local, state, or federal law relative to privacy, public records, copyright, or patent.

~~p.o.~~ Store personal content or documents on County equipment.

2. BoCC technology resources shall not be used for procuring, transmitting, retrieving or storing any material or communications that violate County discrimination, sexual harassment, or workplace violence policies.

~~3.~~ BoCC technology resources shall not be used to access, transmit or retrieve offensive material, or otherwise send or receive offensive material. ~~Offensive material includes, but is not limited to, sexual comments or images, or any comments, pictures, or video that would be offensive on the basis of age, sexual orientation, gender, race, religious beliefs, national origin, or disability.~~

~~4.3.~~ No abusive, threatening, profane, or offensive language or pictures ~~(including all pornography)~~ shall be transmitted through or stored on the BoCC network unless required by business necessity ~~(e.g., investigative case evidence)~~ and authorized in writing by the Department Director, or their designee.

~~5.4.~~ Illegal material, ~~such as child pornography,~~ from any source, with the singular exception of job requirements related to the fulfillment of law enforcement or legal responsibilities, is prohibited.

F. ~~F.~~ Enforcement and Exceptions

1. Violators of this policy may be subject to disciplinary action ~~up to, and including, employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil,~~ as established by Section 815.06, Florida Statutes, as may be amended, Merit System Policy 12~~1~~– *Disciplinary Actions*, and other applicable laws and regulations.

2. ITD will be responsible for monitoring and auditing technology resource usage ~~on request. Upon identifying any policy violation, a report will be submitted to the ITD Director for appropriate action.~~

3. A report or complaint of a possible violation of this Policy will be investigated by the ITD, in collaboration with the Brevard County Human Resources Office, the department or office having ownership of the technology resources used, and/or with consultation from other departments or offices, as appropriate.

IV. Reservation of Authority

The authority to issue and/or revise this policy is reserved to the Board of County Commissioners.

ATTEST:

Rachel M. Sadoff, Clerk

~~Kristine Zenka~~ Thad Altman, Chair
BOARD OF COUNTY COMMISSIONERS
BREVARD COUNTY, FLORIDA

As approved by the Board on: _____