(IS) Information Technology Policy

Effective Date: January 2020
BOC Amended: March 2022

Policy Owner	Board of Commissioners (BOC)
Policy Reviewer(s)	IS Division Directors, IS Technology Services Managers, County Attorney, Support Services Agency Director, County Manager
Policy Approver(s)	Chief Information Officer (CIO) and Board of Commissioners (BOC)
Replaces	Electronic Communications and Security Policy (Adopted 10/25/2005) Information Technology Security Standards (Adopted 10/05, rev. 3/07, 5/09)
Related Policies	Conduct and Performance Policy (BOC Only) Adopted 11/89; Revised 6/92, 12/96, 4/06, 10/15, 1/20 No Harassment and No Discrimination Policy (BOC Only) Adopted 6/92; Revised 4/00, 4/06, 12/11
Related Standards	(IS) Technology Acceptable Use Standards (IS) Technology User Account Standards (IS) Technology Infrastructure Security Standards (IS) Network Security Standards (IS) Multi-Factor Authentication Standards
Storage Location	iCobb
IS Last Review Date	December 2021
IS Next Review Date	December 2023
IS Review Cycle	Every 2 years
Employee Acknowledgement	Annually

1. INTRODUCTION

Technology is mission-critical for the delivery of virtually all Cobb County (County) services. Information technology systems are an integral part of every agency. These resources and the data in them must be used responsibly to avoid equipment loss or data compromise. The CIO is responsible for establishing standards that protect the County's information technology resources.

The IS Department is responsible for all information technology systems and technology resources for the County. Although departments, offices, agencies, programs, and individuals may use and have responsibility for managing these resources, the County itself retains ownership.

2. PURPOSE

This policy is established to protect the County's information technology systems and technology resources and authorizes the CIO to create, maintain, and communicate information technology and security standards concerning the use, protection, and preservation of all County information technology systems and technology resources. These standards include but are not limited to: (IS) Technology Acceptable Use Standards, (IS) Technology User Account Standards, (IS) Technology Infrastructure Security Standards, (IS) Network Security Standards, and (IS) Multi-Factor Authentication Standards.

3. SCOPE

This policy applies to all County agencies, elected offices, departments, full-time, part-time, and temporary employees, volunteers, service providers, vendors, contractors, and any other applicable entities. Users who have questions regarding this policy may contact IS at 770-528-8740.

4. GOVERNING LAWS, REGULATIONS & STANDARDS

Guidance	Section
Georgia Computer Systems Protection Act	O.C.G.A. 16-9-90, et seq.
Georgia Open Records Act	O.C.G.A. 50-18-70, et seq.
Georgia Archives as adopted by County Code	https://www.georgiaarchives.org/records/retention_schedules
And all other applicable laws and regulations	

5. ROLES AND RESPONSIBILITIES

The CIO will decide when a new policy or standard needs to be developed to protect the County's technology resources. The CIO will bring policy recommendations and changes to the Board of Commissioners (BOC) for approval. The County Attorney will be consulted on policy matters as needed.

Role	Responsibilities
CIO	**Protect County IT Resources** • Recommend technology and security policies and updates to BOC for approval. • Recommend and approve technology and security standards as needed.
IS Division Directors	**Serve as owners/approvers of technology standards** • Serve as reviewers on all technology policies and standards. • Ensure that appropriate standards for information, data, equipment, and technology access are established for each of their areas of management. • Regularly review all technology policies and standards for updates.
Agency/Department Management	**Ensure compliance with policies and standards** • Protect technology resources assigned within their departments. • Identify to IS any potential risks and threats not identified.
Application Owners	**Identify to IS the required access levels for agency/department application owners.**
All County agencies, elected offices, departments, full-time, part-time, and temporary employees, volunteers, service providers, vendors, contractors, and any other applicable entities that access County technology resources	**Comply with IT policies and standards** • Read and adhere to County technology policy and standards. • Protect technology resources as assigned in the conduct of County business. • Identify to IS or Departmental Management any potential risks and threats not identified. • All employees are required to sign and acknowledge they have received and reviewed the IT policy and applicable technology standards.

6. POLICY

The following policy statements are established to protect the County's technology resources:

6.1 (IS) Technology Acceptable Use Standards *(Acceptable Uses)*

Technology resources are provided by the County for users to perform their County job responsibilities and to enhance their ability to conduct the County's business. It is the user's responsibility to use these resources for business purposes and to help protect County technology resources and information. **County technology and information is considered County property, and there should be no**

expectation of privacy when using resources such as email, files, data, etc. from County devices or through County systems.

For additional details see the (IS) Technology Acceptable Use Standards.

6.1.1 Access to County Technology Resources

6.1.1.1 Per technology audit requirements, user access will be validated annually for each software application.

6.1.1.1.1 Where IS maintains the User Access List for applications, IS will provide a report to the Department annually. The Department will review the report and validate that each user still requires access to the application. The Department will return the updated report to IS.

6.1.1.1.2 Where the Department maintains the User Access List for their applications, the Department will validate annually that each user still requires access to the application and provide a User Access List to IS.

6.1.2 Email

6.1.2.1 The County retention period for email in the Outlook system is 5 years. Departments, agencies, and employees are responsible for the retention of emails or records in compliance with all applicable laws and regulations, including the Local Government Record Retention Schedules.

6.1.2.2 The County archives all incoming and outgoing email onto a separate storage system. Archived emails will be retained for 10 years unless on administrative or legal hold. Prior to initiating the first 10-year purge (2030), IS will seek approval from the County Attorney.

6.1.2.3 To the extent required by law, including, but not limited to the Georgia Open Records Act, O.C.G.A. § 50-18-90 et seq., each individual County department and agency shall be responsible for complying with all applicable laws and regulations, including the Local Government Record Retention Schedules.

6.1.3 Personal Devices

6.1.3.1 Users may utilize a personal device to access the County's technology resources if they have approval from their Department Director or designee and the CIO. Although use of a personal device for County business purposes may be efficient, it is not the preferred method and may subject information on that device to Georgia's Open Records Act.

6.1.3.2 Users are responsible for ensuring their personal devices and connections to the County's technology resources are in compliance with the County's security standards. These standards can be found on iCobb in the (IS) Technology Acceptable Use Standards, the (IS) Technology User Account Standards, and the (IS) Multi-Factor Authentication Standards.

6.1.4 Internet Websites

All County domain names must be approved by the CIO and Communications Director. The domain name registration is controlled and maintained by the County Webmaster. Submit domain name requests to web@cobbcounty.org.

6.1.4.1 Elected Officials may obtain and maintain their own domain names. They should provide the domain name information to the IS webmaster at web@cobbcounty.org to ensure IS has a complete list of Cobb County domain names. IS does not maintain elected officials' domain security or websites.

6.1.5 Privileged or Confidential Information

Pursuant to the Conduct and Performance Policy (BOC Only), an employee who deals with plans, programs, and other information of significant interest may only release information the employee has authority and responsibility to release to persons authorized to receive such information. (Go to iCobb > Policies to access the policy).

Agency/Department Heads, Division Managers, other supervisors, and Department representatives who are entrusted with confidential employee information must hold that information in the strictest confidence. Unless the information needs to be conveyed for a business purpose, the information should not be discussed.

Privileged or confidential information must be submitted via secure methods. See (IS) Technology Acceptable Use Standards section 5.6 "File Transmissions" for details.

6.2 (IS) Technology Acceptable Use Standards *(Prohibited Uses)*

Users who access the County's technology resources will not:

6.2.1 Create, send, copy, or forward any fraudulent, defamatory, obscene, threatening, intimidating, offensive, harassing, discriminatory, or disruptive messages, e-mails, or chain messages. Such prohibited uses include any communication which violates County policy, standards, and/or state or federal law. If a user receives material believed to be in violation of the County's No Harassment and No Discrimination Policy (BOC Only), the user should report the incident as advised in the No Harassment and No Discrimination Policy (BOC Only). (Go to iCobb > Policies to access the policy.)

6.2.2 Create, send, copy, or forward any messages, e-mails, or chain messages that violate the County's Conduct and Performance Policy (BOC Only). (Go to iCobb > Policies to access the policy.)

6.2.3 Access, view or download any non-business-related information from any website, chat room, newsgroup, messaging, e-mail or any other electronic location of an adult nature (obscene, sexual, or pornographic) unless pursuant to County business (i.e., law enforcement, public safety, sheriff, judicial).

6.2.4 Transmit any messages anonymously or using an assumed name; attempt to obscure the origin of a message or misrepresent a user's job title or position with the County; and/or allow any other person to utilize a user's protected information to access County resources or information.

EXCEPTION: The following groups are exempt:

- Law enforcement investigation units
- IS staff for cyber security training purposes

6.2.5 Engage in any illegal acts involving electronic communications, including criminal acts outlined in the Georgia Computer Systems Protection Act, O.C.G.A. Sec. 16-9-90, et seq. Criminal acts contained in that statute include: computer theft (unauthorized use with the intention to take, appropriate, obtain, or appropriate the property of another); computer trespass (unauthorized use with the intention of deleting a program or data, of interfering with the use of a program or data, or

of altering, damaging, or causing a malfunction of a computer, computer network or computer program); computer invasion of privacy (use with the intention to examine employment, medical, salary, credit, or other financial or personal data without authority); computer forgery (creation, alteration, or deletion of data contained in any computer or computer network); and computer password disclosure (unauthorized disclosure of a password for accessing a computer/computer network).

6.2.6 Use another person's login credentials.

6.2.7 Access or download gambling sites.

6.2.8 Send information that violates or unlawfully infringes on the rights of any other person (including but not limited to copyrights and software licenses).

6.2.9 Download, install or run security programs or utilities, such as, password cracking programs, packet sniffer, or port scanners that reveal or exploit weaknesses in the security of technology resources.

EXCEPTION: The following groups are exempt:
- Law enforcement investigation units
- IS staff for cyber security training purposes

6.2.10 Open email attachments or click on hyperlinks sent from unknown or unsigned sources through any platform (email, instant message, social media, etc.). Attachments/links are the primary source of computer viruses and should be treated with utmost caution.

6.2.10.1 Users are encouraged to use the phish alert button to report suspicious emails to the IS Department. If using your mobile device, forward the suspicious email to PhishAlert@cobbcounty.org.

6.2.11 Use their County passwords for other non-County accounts or logins. In the event that other services are compromised, it could leave County accounts compromised as well.

6.2.12 Circumvent County security measures.

6.3 (IS) Technology User Account Standards

6.3.1 Information system accounts are the only method by which County systems may be accessed.

6.3.2 An active directory profile is required for users, service accounts, and devices to access the County network.

6.3.3 Department management will determine and notify IS of required individual access levels.

6.3.4 IS will limit information system access for each account to the types of transactions and functions that the authorized user is permitted to execute.

For additional details see the (IS) Technology User Account Standards.

6.4 (IS) Technology Infrastructure Security Standards

6.4.1 IS will protect and monitor the physical facility and support infrastructure for information systems by use of physical access controls, environmental controls, and security measures.

6.4.2 Certain Agencies/Departments and Elected Offices in the County have special networks or subsystems attached to the County network. In these cases, they may have a security administrator with special privileges agreed between them and the CIO to protect information and ensure the security of the County network. Examples are: TMC, Superior Court Clerk, Sheriff's Office, etc. Also, if the administrator desires to deviate from Cobb County security protocols and standards there must be agreements between Agency, Director, Elected Official, and the CIO that the selected security methods or tools provide the same or higher security levels as the Cobb County standards.

6.4.3 Water System industrial systems (e.g. SCADA, plant controls, etc.) are managed by the Technology Support Group (TSG) within the Water System's Water Protection Division. The operations and security of these industrial systems are governed by TSG's Industrial Network Policy and Standards.

For additional details see the (IS) Technology Infrastructure Security Standards.

6.5 (IS) Network Security Standards

6.5.1 IS will monitor, control, and protect County communications (i.e. information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

6.5.2 IS will employ architectural designs, software development techniques, and systems engineering principles to promote effective information security within County information systems.

For additional details see the (IS) Network Security Standards.

6.6 (IS) Multi-Factor Authentication (MFA) Standards

6.6.1 Only users enrolled in MFA will have access to Webmail, VPN, or other County technology resources.

For additional details see the (IS) Multi-Factor Authentication Standards.

7. STANDARDS

Standards supporting and providing additional information to this Information Technology Policy include:

1. (IS) Technology Acceptable Use Standards
2. (IS) Technology User Account Standards
3. (IS) Technology Infrastructure Security Standards
4. (IS) Network Security Standards
5. (IS) Multi-Factor Authentication Standards

These standards are located on iCobb. Users are responsible for familiarizing themselves with them.

8. NON-COMPLIANCE

Since it is impossible to specify every instance that might result in a violation of the Information Technology Policy or Related Standards as listed in section 7 and on the chart on page 1, a standard of reasonableness will apply to determine whether a user's use of technology is inappropriate.

Violations of this policy may result in one or more of the following:

1. Disciplinary action according to applicable County policies;
2. Temporary or permanent revocation of access to some or all computing and technology resources and facilities, including access to the County's technology resources through a personal device;

3. Termination of employment; and/or
4. Legal action

ACKNOWLEDGEMENT

I acknowledge I have read and understand the **IS Information Technology Policy** and applicable related suite of technology standards. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or County policy.

_____
Employee Name

_____
Employee Signature Date

Revision History

Version	Revision Date	Author	Reason for Revision
v.1.0-2020		IS Technical Writer	BOC Approval
v.2.0-2022	January 2022	IS Technical Writer	Update