(IS) Technology Infrastructure Security Standards

Effective Date: January 2020

Owner	Information Services (IS) Director, IS Division Directors
Reviewer(s)	IS Division Directors and IS Technology Services Managers
Approver(s)	IS Director and IS Division Directors
Related Policies	(IS) Information Technology Policy Adopted 1/20 Conduct and Performance Policy (BOC Only) Adopted 11/89; Revised 6/92, 12/96, 4/06, 10/15, 1/20
Related Standards	(IS) Technology Acceptable Use Standards (IS) Technology User Account Standards (IS) Network Security Standards Cobb County Business Continuity Plan (Accessible by BCP owners and designees only)
Storage Location	iCobb
IS Last Review Date	December 2019
IS Next Review Date	December 2021
IS Review Cycle	Every two years
Employee Acknowledgement	Annually

1. PURPOSE

The purpose of these standards is to ensure proper measures are in place to prevent damage or unauthorized physical access to Cobb County Government's (County) technology infrastructure.

2. SCOPE

These standards apply to designated Information Services (IS) staff and other Departmental staff responsible for areas where County IT infrastructure is housed. If you have questions regarding these standards, contact the IS Technical Operations Division Director at 770-528-8740.

These Standards also apply to physical areas that include but are not limited to:

1. Data centers or other facilities for which the primary purpose is the housing of IT infrastructure.
2. Server rooms and switch/wiring closets within shared purpose facilities for which one of the primary purposes is the housing of IT infrastructure.

3. GOVERNING LAWS, REGULATIONS, & STANDARDS

Guidance	Section
ISO 27001:2013	A.11 (A.11.1, A.11.2)
NIST SP 800-171	3.10.1–3.10.6
NIST SP 800-53 v4	PE-2–PE-6, MA-5, PE-8, CP-2, CP-6, CP-7, PE-1, CP-8, PE-19–PE-16, MA-2–MA-6, AC-19, AC-20, MP-5, PE-17, MP-6, MA-2, MP-5
And all other applicable laws and regulations	

4. DEFINITIONS

Controls - Administrative, technical, or physical measures and actions taken to try and protect systems, including safeguards and countermeasures.

Onsite Contractor - A Contractor who performs all daily work at a Cobb County facility.

Offsite Contractor - A Contractor who performs some or all of the contract work at a non-Cobb County owned facility.

5. STANDARDS

Pursuant to the Information Technology Policy, IS will protect and monitor the physical facility and support infrastructure for information systems by use of the following controls and security measures. 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 IS Director 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 IS Director that the selected security methods or tools provide the same or higher security levels as the Cobb County standards.

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.

5.1 Physical Access Controls

Physical access controls help ensure that all computing equipment is properly safeguarded and available for its intended purpose. These standards are applicable only to areas where information processing equipment and data are located and supplement any security standards for the building.

5.2 Physical / Environmental Controls

Application servers, file and print servers, and telecommunications equipment shall be located in rooms that meet the following physical control standards:

5.2.1 IS must designate an owner who is responsible for authorizing and periodically reviewing who has access to each data center or other IT infrastructure facility.

5.2.2 IS will restrict physical access to personnel with a business need to be in the data center, IT infrastructure facility, or switch and wiring closets.

5.2.3 IS will review, approve, and coordinate credentials for IT infrastructure facility access.

5.2.4 IS will establish and maintain a list of authorized personnel, append newly authorized personnel to the list, and remove those personnel who have lost authorization from the list.

5.2.5 IS will review card access logs quarterly.

5.2.6 IS will maintain visitor logs for the data center, the TMC backup data center, and 911 data center. The facility visitor log should be visibly posted (eg. on a door or wall). Printable copies of the IS-Facility Visitor Log can be found on iCobb. IS will annually review and retain all visitor logs according to the County’s retention guidelines.

5.2.7 IS will distribute keys, cards and combinations to authorized personnel only.

5.2.8 IS or Property Management is responsible for switch and wiring closet access.

5.2.9 IS will handle and protect equipment to ensure risks are reduced, preventing potential environmental threats and hazards.

5.2.10 IS will determine and implement protection against natural disasters or malicious attacks, as well as accidental incidents, per the County's Business Continuity Plan.

5.2.11 IS or their designee will place power equipment and cabling in sa locations to prevent environmental and/or man-made damage and destruction.

5.2.12 IS may install an uninterruptible power supply (UPS) to ensure a constant and steady supply of electricity.

5.2.13 IS will not allow rooms to be used for unrelated purposes, such as storage of janitorial supplies, office supplies, volatile chemicals, etc.

5.2.14 IS shall equip spaces designated for technology assets with appropriate environmental controls, including considerations for temperature, humidity, protection against water damage, and emergency lighting

5.3 Disposal of Technology Assets Containing County Data

Please contact the IS Call Center at 770-528-8740 for current disposal instructions.

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

6. EXCEPTIONS

Exceptions to these standards must be justified and approved in advance. The County may deviate from the standards when:

1. Written justification is provided to the IS Director by the Agency/Department Director; and
2. A cost/benefit analysis has been performed by IS and the requesting Department showing:
   a) the available compliance options, and
   b) the risk of noncompliance; and
3. An acceptable balance between the costs and the risks has been determined to be acceptable to IS; and
4. The acceptance of risk has been formally recommended by the IS Director and approved by the County Manager as needed.

Note: Certain legacy applications may use older security and communication protocols which do not fully comply with advanced security practices. These systems will be upgraded as budget allows

7. NON-COMPLIANCE

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

Violations of these standards may include 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 networking resources and facilities.
3. Termination of employment; and/or
4. Legal action

Revision History

Version ID	Date of Change	Author	Rationale
v.1.0-2020		IS-Technical Writer	BOC Approval