(IS) Network Security Standards

Effective Date: January 2020

Owner	Chief Information Officer (CIO) and IS Division Directors
Reviewer(s)	IS Division Directors and IS Technology Services Managers
Approver(s)	CIO and IS Division Directors
Related Policies	(IS) Information Technology Policy Adopted 1/20; Revised 3/22 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) Technology Infrastructure 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 two years
Employee Acknowledgement	Annually

1. PURPOSE

The purpose of these standards is to ensure security is a key consideration in network management and in the transfer of information in and out of Cobb County Government (County).

2. SCOPE

These standards apply to Information Services (IS) technical staff and managers and other Departmental staff responsible for vendor software or equipment which connects to or resides on the County network. If you have questions regarding these standards, contact the IS Technical Operations Division Director at 770-528-8740.

3. 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.
ISO27001: 2013	A.13.1, A.13.2
NIST SP 800-171	3.13.1-3.13.16
NIST SP 800-53 v4	XX-1 controls, SA-5, CM-2~CM-9, AC-5, SA-9, SA-10, AU-4, AU-5, CP-2, SA-2, SC-5, CA-2, CA-6, SA-4, SA-11, AC-19, AT-2, AT-3, IR-2, IR-8, MA-3, MP-7, SC-42, SI-1, SI-3, SI-5, SI-7, SA-8, SC-2, SC-3, SC-7, SC-18, CP-9, AC-3, AC-17, AC-18, AC-20, SC-8, SC-15, CA-3, MP-5, AU-10, IA-2, IA-8, SC-7, SC-8, SC-13, AC-3, AC-22, SI-4, SI-7, SI-10, AU-2, AU-3, AU-8, AU-11, AU-12, AU-14, AU-6, AU-7, AU-12, CM-6, CM-11, PE-6, PE-8, SC-7, SI-4, SI-6, SI-7,
And all other applicable laws and regulations	

4. DEFINITIONS

Authorization - The identification of which IT resources, User, machine, device, or application process is entitled to access.

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

Data - Local Agency and/or County information that is stored, processed or transmitted in electronic, optical, or digital form.

Firewall - A rule-based hardware or software control device that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Network Devices - Exclusively, routers, switches, hubs and bridges (including physically cabled and/or wireless connectivity).

Risk - The capability and likelihood of a threat or vulnerability compromising the confidentiality, integrity, and availability of information and systems. Risk analysis evaluates the probability of a vulnerability or threat resulting in an unfavorable business impact.

Voice Applications - Exclusively, Private Branch Exchanges (PBX's); Centrex services; IP Telephony systems; voicemail systems; call accounting systems; call center systems; and cellular devices.

5. STANDARDS

Pursuant to the Information Technology Policy, 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.

Architectural designs, software development techniques, and systems engineering principles will be employed to promote effective information security within organizational information systems.

5.1 Firewall

5.1.1 IS Technical Operations shall be responsible for the review, approval, configuration, and security of all firewall designs.

5.1.2 All internal/external firewalls must be County-owned, installed, and administered by IS Technical Operations. In special cases, written authorization for exceptions to these standards may be granted as agreed upon by the CIO (see section 6 “Exceptions” for details).

5.1.3 All external access to the County network must be via a firewall.

5.1.4 IS Technical Operations will monitor the status and activity of all firewalls and remediate any issues that may be detected.

5.1.5 IS Technical Operations will conduct monthly backups of all firewall configurations. In addition, backups will be performed prior to making any firewall configuration changes.

5.1.6 IS Technical Operations will develop and maintain documentation for baseline configuration and hardening standards.

5.2 Network

5.2.1 IS Technical Operations shall be responsible for the review, approval, configuration, and security of all network devices for use on the County network.

5.2.2 IS Technical Operations must review and approve all site network designs prior to implementation.

5.2.3 IS Technical Operations shall review and approve all facility data communications wiring prior to installation.

5.2.4 IS Technical Operations shall provide the following:

1. IP address or address ranges
2. Subnet masks
3. Network device names
4. Protocols/Ports (ie: SSL/443)

5.2.5 Privileged access to all technology resources shall require an administrative account separate from your normal user login ID. Please refer to the (IS) Technology User Account Standards.

5.2.6 IS Technical Operations shall review, approve, and implement all switch and router configurations.

5.2.7 IS Technical Operations will monitor the status of all network devices and remediate any issues that may be detected.

5.3 Voice

5.3.1 IS Technical Operations shall be responsible for the monitoring, administration, and security of the following:

1. Voice over IP (VoIP) system and associated network devices
2. Collaboration Tools such as telephones, softphones, and meeting applications
3. Call recording applications and solution designs
4. Call center management applications

5.4 IP Addressing

5.4.1 IP address ranges are controlled and managed by the IS Technical Operations Division. Reserved IP addresses are only for special business cases. Reserved IP addresses may be issued from IS Technical Operations after review and approval.

5.4.1.1 In special cases written authorization for exceptions to these standards may be granted as agreed upon by the CIO (see section 6 “Exceptions” for details).

5.4.2 The MAC address and location of the equipment must be provided prior to an IP address being assigned.

5.4.3 When equipment with a reserved IP address is moved or removed from service the Department/Designee must notify IS Technical Operations immediately.

5.5 Vendor Equipment

5.5.1 The County’s endpoint protection software must be loaded on all vendor supplied devices that are attached to the County network. In special cases, written authorization for exceptions to these standards may be granted as agreed upon by the CIO (see section 6 “Exceptions” for details).

5.5.2 Vendor equipment cannot be connected to the network without a security review.

5.5.3 If vendor equipment is to be connected to the County's network, a change control must be submitted prior to allowing the equipment to connect to the network.

5.5.4 IS Technical Operations shall monitor the equipment to ensure the proper endpoint protection updates and security patches are installed.

5.6 Information Transfer

5.6.1 IS Technical Operations will use subnetworks for publicly accessible systems that are physically or logically separated from internal networks to provide a level of separation for security.

5.6.2 IS Technical Operations will deny network communications traffic to the network by default. Any deviations must be considered under the exception protocol.

5.6.3 IS will coordinate with Departments to provide a level of data transmission security required by the system or application. There are multiple protocols available (i.e. VPN, secure ftp) to securely transfer the data. Contact the IS Call Center at 770-528-8740 for assistance.

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 CIO 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 CIO 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 inappropriate.

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 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

Revision History

Version ID	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