(IS) Multi-Factor Authentication Standards

Effective Date: January 2022

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 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) Network Security Standards
Storage Location	iCobb
IS Last Review Date	January 2022
IS Next Review Date	January 2024
IS Review Cycle	Every two years
Employee Acknowledgement	Annually

1. PURPOSE

The purpose of the Enterprise Multi-Factor Authentication (MFA) Standards is to enable a means of strong authentication for those users with access to County technology resources, confidential information, sensitive information, or have a privileged level of system support access. Multi-factor authentication (MFA) technology supports securing the modern workforce whether they are on-premise or working offsite. MFA provides an additional layer of protection to the County's network, applications, and information by requiring users to have a second source of validation, like a phone or token, to verify the user's identity before allowing them access to the network. The adoption of these standards will reduce the likelihood of unauthorized access and provide demonstrated compliance to federal and industry security standards.

2. SCOPE

These standards apply to all County agencies, elected offices, departments, agencies, full-time, part-time, and temporary employees, volunteers, service providers, vendors, contractors, and any other applicable entities. They also apply to any system that requires an additional layer of protection as determined by the Information Services Department. If you have questions regarding this standard, contact the IS Technical Operations Division Director at 770-528-8700.

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.
GTA Policies, Standards, and Guidelines	PS-21-002
NIST 800-53 Revision 4	IA-2, IA-5, IA-8, Appendix B
NIST 800-171 Revision 2	3.5.3
Georgia Archives as adopted by County Code	https://www.georgiaarchives.org/records/retention_schedules
And all other applicable laws and regulations	

4. DEFINITIONS

Confidential Information – Information the County is required or permitted to keep confidential.

Multi-Factor Authentication (MFA) – An authentication method that requires the user to provide two or more verification factors to gain access to a resource—typically at least two of the following categories: knowledge (something you know), possession (something you have), and inheritance (something you are).

Personally-Identifiable Information – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Privileged User – A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Protected Health Information – Information, including demographic data, that relates to an individual's past, present, or future physical or mental health or condition; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies an individual or for which there is a reasonable basis to believe it can be used to identify an individual.

Sensitive Information – Data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.

Single-Factor Authentication (SFA) – An authentication method for securing access to a given system that identifies the party requesting access through only one category of credentials. The most common example is password-based authentication.

5. STANDARDS

5.1 The MFA standards describe the conditions necessary to "challenge" a user for stronger authentication than single-factor authentication. Typically, this is due to the sensitive nature of the information and information system or a privileged user performing administrative functions.

5.2 MFA includes two or more of the following conditions:

1. Something you know (password)
2. Something you have (soft token, hard token, smart card)
3. Something you are (biometrics, such as fingerprints)

5.3 Users will be required to enroll in MFA when requested. Only users enrolled in MFA will have access to Webmail, VPN, or other County technology resources. Users may need to install and activate a mobile app for MFA on a County owned or personal phone. If you do not have access to a phone, then an alternative method for the user to access County resources through MFA will be evaluated on a case by case basis.

1. A user may be issued a token (a hard key) if their work location prohibits the use of phones or if connectivity is problematic.
2. If a token is lost, stolen, or damaged through negligence then the person issued the token, or their department, will be responsible to replace the token.
3. The cost of the replacement token will be $30.00.

5.4 When users try to log into systems protected by MFA, the system will "challenge" the user by requesting a secret security code. This code will be provided through the secure method chosen during enrollment.

5.5 System and business owners may conduct data classification exercises on system assets. MFA shall be applied based on the outcome of those assessments.

5.5.1 MFA is required:

5.5.1.1 When a user is asked to enroll in MFA by the County

5.5.1.2 When a user accesses the County's technology resources on a County device and/or a personal device

5.5.1.3 When a user has access to confidential information

5.5.1.4 When a user has access to sensitive information

5.5.1.5 When a user is assigned privileged access

5.5.1.6 When a person's role or job duties within the County's organization may subject them to attacks through malicious means or by bad actors

5.5.2 MFA should be considered:

5.5.2.1 When the information system contains sensitive information, such as federal tax information (FTI), personally identifiable information (PII), protected health information (PHI), and confidential information

5.5.2.2 When certain high-risk financial or administrative transactions are attempted

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.
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.
3. An acceptable balance between the costs and the risks has been determined to be acceptable to IS.
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 legacy applications will be upgraded to be MFA compliant as budget allows. New applications must be MFA compliant.

7. NON-COMPLIANCE

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 according to applicable laws and contractual agreements.

REVISION HISTORY

Version ID	Revision Date	Author	Reason for Revision
v.1.0-2022		CISO	Approval