(IS) Technology User Account 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 Infrastructure Security Standards (IS) Network Security Standards (IS) Multi-Factor Authentication Standards
Storage Location	County Intranet, County Website
IS Last Review Date	July 2023
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 that you have the appropriate access levels to access information on Cobb County Government's (County) systems and applications, and that you understand the responsibility your access level provides you, including the responsibility to comply with all standards, policies, and laws.

Access and authentication controls ensure that only known users have access to Cobb County information systems. Without these controls, the potential exists that information systems could be wrongfully accessed and that the security of those information systems could be compromised. The County is using Microsoft Active Directory (AD) to centralize account/identity management.

2. SCOPE

These standards apply to all County agencies, elected offices, Departments, full-time, part-time and temporary employees, volunteers, service providers, vendors, contractors, and any other applicable entities. 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.
NIST SP 800-171	3.5.1-3.5.11
ISO/IEC 27001:2013	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)
NIST SP 800-53 v4	AC-1~AC-25
And all other applicable laws and regulations	

4. DEFINITIONS

Authentication - A procedure to unambiguously establish the identity of a user, machine, device or application process before allowing access to an information resource. Authentication is typically with a password but other credentials such as digital certificates may be used.

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

Computing Device - Any electronic device that connects to the County's Network in any way (wired or wireless). Among the partial list of computing devices are personal computers, laptop computers, mobile devices, servers, firewalls, switches, routers, hubs, and DNS broadcasters.

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

Encryption - A process that transforms readable data into a form that appears random and unreadable to unauthorized users.

Identification - Means to distinguish individual users, machines, devices and application processes. Multiple identifiers can be associated with a given subject for different purposes. An individual user, for example, may be known by an account name in a Microsoft windows domain, by the distinguished name on a digital certificate, or by a Microsoft windows issued security identifier.

Information Security - Practice of safeguarding an organization's information from unauthorized access, modification, or destruction.

Integrity - Condition of undiminished accuracy, reliability, and protection from unauthorized access or modification.

Mobile Device - A wireless, portable device that allows a User to access data and information from the County’s internal network.

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).

User - A User includes any County elected or appointed official, employee, vendor, contractor or volunteer who utilizes the County’s technology resources.

User ID - The computer identifier unique to each User granted access to any County computing asset.

5. STANDARDS

Pursuant to the Information Technology Policy, AD accounts are the only method by which County systems may be accessed. An AD profile is required for users, service accounts and devices to access the County network. IS will limit information system access to the types of transactions and functions that authorized users are permitted to execute.

5.1 User Responsibility

5.1.1 All users are responsible for protecting and securing the network. In addition to the standards set forth herein, users must comply with all laws and County policies and standards governing the protection of computer systems.

5.1.1.1 Giving out passwords to other users, vendors, or contractors for accessing County technology resources is prohibited and may result in disciplinary actions, up to and including termination of employment. The disclosure of passwords or providing access to computer/networks/systems without authorization may separately be investigated and/or prosecuted as a criminal violation under the Georgia Computer System Protection Act.

5.1.1.2 Unauthorized use of another's computer or computer network is prohibited and may result in disciplinary action, up to and including termination of employment, as well as criminal charges.

5.1.1.3 Unauthorized use of a computer or the computer network to examine financial, personal, or medical information of another person is prohibited and may result in disciplinary action, up to and including termination of employment, as well as criminal charges.

5.1.1.4 The unauthorized creation, alteration or deletion of data or files contained on any computer or network is prohibited and may result in disciplinary action, up to and including termination of employment, as well as criminal charges.

5.2 Information Ownership and Classification

5.2.1 Information security requirements are based on the value of information in relation to the potential security threats. All computer-based information assets are placed into one of three classifications as determined by the County.

5.2.1.1 Public Information
Public information requires minimal protection. The risk to the government or our customers is negligible if this information is disclosed or modified. This includes information that is required to be public information by law.

5.2.1.2 Confidential Information
Confidential information must have one or more of the following attributes:
1. Provides information that is protected by law.
2. Provides information that is not public record.

5.2.1.3 Restricted Information
Restricted information is usually extremely sensitive and/or falls under and exception to the Georgia Open Records Act. Information in this classification must have one or more of the following attributes:

1. Outside disclosure is prohibited.
2. Outside disclosure would compromise the County's data and network security infrastructure.

5.3 User Authentication

5.3.1 Authentication establishes whether you are authorized to access the County technology resources you are attempting to use. Currently, authentication is accomplished by the following:

Information that only you know and can enter into the computer system when prompted. For example, a Login ID and password.

5.3.2 When you are granted a Login ID and access to the County's technology resources, you are responsible for all transactions, inquiries, emails, and activities performed with your Login ID. You will secure your Login ID to prevent unauthorized use.

5.3.3 Multifactor authentication is required for users accessing County technology resources, sensitive information, or have a privileged level of system support access. Such users are subject to the (IS) Multi-Factor Authentication Standards.

5.4 Login ID

5.4.1 To access the County technology resources and business applications that are integrated with Active Directory, you must have an assigned Login ID and associated password.

This standard will be used for all new users. Existing users will continue to use their current Log-in ID.

Some business applications may require a unique login and password. Contact your supervisor or manager for more information.

5.4.2 Privileged User Login IDs
A privileged account is an information system account with authorizations of a privileged user.

Privileged User Login IDs must be separate from your normal user ID.

5.4.3 Shared User Login IDs
Shared Login IDs may exist for individuals or applications. Shared Login IDs may be requested by your Department Manager and approved by IS.

5.4.3.1 Shared User Login IDs may be established for use by more than one person if all of the following criteria are met:

1. Use of an individual Login ID has a negative impact on productivity.

2. All users have the same access authorizations, same job functions, use the same workstation, and the workstation is logged off after working hours each day.

3. Users with a shared login report to the same manager/supervisor. If there are multiple shifts using the same Login ID, each shift may have a separate manager/supervisor responsible during that shift.

4. Information displayed on the workstation is not confidential or restricted information.

5. The manager retains responsibility for the proper use of the Shared Login ID and changes the password in accordance with the password reset process.

6. When an authorized user of a Shared Login ID is performing an update function, the workstation must not be left unattended at any time. The workstation must be restricted physically to prevent unauthorized access.

7. Access is restricted to those applications/information necessary to perform the required job function.

8. Access to the Internet or e-mail may be restricted.

Note: If unable to meet one or more of the above criteria, exceptions may be approved by the IS Technical Operations Division Director.

5.4.3.2. Shared Service Account IDs

1. Service Account IDs that are not associated with a specific user or group of users may be defined for use by special processes such as network monitoring, batch processing, application interfaces and operations management.

2. Service Account IDs must have appropriate compensating controls such as restricted account privileges, non-interactive sign on, no VPN privileges, or locking the ID to a specific workstation implemented to ensure access is limited to the authorized processes.

5.4.4 Non-County Employees

5.4.4.1 IS may establish Login IDs for use by non-employee users. Access is granted as needed by Department request via the (IS) Contractor/Vendor Access Request form, which is located on the County Intranet.

5.4.4.2 When non-employee access to County technology resources is no longer needed, the County IS Project Manager or the Department Business Implementation Manager sponsoring the access is responsible for notifying IS immediately.

5.4.4.3 IS will review non-employee access IDs quarterly and may cancel or suspend Login IDs for non-employees if not used for a period of more than 90-days.

5.5 Password Requirements

5.5.1 Your passwords used to authenticate access to the network shall:

1. Be a minimum of eight (8) characters long, one of these must be a special character.
2. Be a mix of three of the four following classification types: alpha (a-z), numeric (0-9), upper/lower case (A/a), and special characters (#, !, %, $, etc.).
3. Be changed at a minimum of once every ninety (90) days. Additionally, shared login passwords shall be changed each time a member of the staff who knows the password leaves the Department or employment of the County. Exceptions to the 90-day requirement may be granted on a per case basis with the approval of the CIO.
4. Not be identical to the previous ten (10) passwords.
5. Not be the same as the User ID.
6. Not be a dictionary word or proper name.
7. Be changeable by the person to whom the Login ID belongs (via password reset self-service), except for vendors only connecting via VPN.
8. Be changed immediately upon installation of the application, device, or operating system for vendor-supplied default and/or blank passwords.

5.5.2 Your passwords used to authenticate access to County technology resources should **not** be:

1. Easily guessed.
2. Reset by anyone other than the appropriate system administration personnel or their designees. This does not prohibit you from resetting your own PC password using password self-service or changing your password using the password reset option on your PC.
3. Written down or otherwise recorded and stored near the access device to which they pertain.
4. Displayed in plain text.

5.5.3 You may be required to change the default password upon your first log in.

5.5.4 IS will prohibit password reuse for a minimum of ten iterations.

5.6 System Sign-On and Session Management Control

5.6.1 IS shall properly authenticate all access to County technology resources that store County information. Access is managed through the use of Login IDs, passwords, and multi-factor authentication.

5.6.2 IS will monitor attempts to sign on to County technology resources with invalid passwords. A system log will be maintained to allow timely review and follow-up of all attempts. If there is unusual activity during sign on, IS will notify the offender's manager/supervisor.

5.6.3 IS will suspend your user ID until it is reset by an administrator or the employee can use self-service to reset their own password if the number of invalid login attempts exceeds the system specified parameter. Instructions for resetting your password if you are locked out are stored in Support Central knowledge base (IS call center ticketing system).

5.6.4 IS password management systems will be interactive and mandate strong passwords.

5.6.5 You must log off or lock the keyboard before leaving the area of your workstation to prevent unauthorized access.

5.6.6 You must not create processes that automate or eliminate the need to enter your password or shared Login IDs.

5.7 Network Monitoring Devices

5.7.1 Only IS Technical Operations staff is authorized to use network monitoring devices, scanning and intrusion/detection software for network and server support. If you are found using these tools without proper authorization you will be subject to disciplinary action up to, and including, termination of employment.

5.7.2 Pursuant to section 6.4.2 of the (IS) Information Technology Policy, Departmental Administrators may be authorized to scan their department’s network or sub-systems but should not scan networks or sub-systems not under their purview.

5.7.3 IS will control and restrict any use of software programs capable of overriding system and application controls.

5.8 Remote Control Access to County Workstations

5.8.1 Remote control software allows an authorized IS or departmental support person to take control of another network-connected workstation. Remote control access is allowable when remote control is needed to perform business duties, job functions, or support activities. The authorized IS or departmental support person will notify you if she/he is going to use remote control access to take control of your workstation.

5.8.2 Prior to connecting to your workstation, each authorized IS or departmental support person using remote control access will identify himself or herself to you (and provide user ID and manager/supervisor name if requested), identify the reason he or she wants to take remote control of your workstation, and identify what he or she intends to do. You will be asked to give approval for the remote-control access prior to connecting.

5.8.3 Your passwords must remain confidential during the remote-control access session. The authorized IS or departmental support person using remote control will request that you enter all IDs and passwords when necessary.

5.9 Security Requirements

5.9.1 IS uses Active Directory controls for the assignment of user rights. The (IS) New Employee Access Request form is used to request user rights and is located on the County Intranet.

5.9.2 Department Managers are responsible for requesting individual user rights for employee access to technology resources and business applications.

5.9.3 The County will disable local administration rights for end user devices by default. Any exceptions shall be reviewed and approved by the IS Technical Operations Division Director.

5.9.4 IS will grant the lowest level of security privileges required to perform your job function. Department Managers are responsible for identifying employee job functions and associated privileges.

5.9.5 Managers must notify IS within 5 days of being notified that an employee will be missing work for any reason for more than 30 consecutive calendar days. The employee’s account will be disabled. Once the employee returns, their account can be reactivated by them or their manager by contacting the IS Call Center.

5.9.6 If an account has not been used for 31 days or more IS will disable the account. The account can be reactivated by the user or their manager by contacting the IS Call Center.

5.9.7 Vendor accounts are automatically set to expire after 30 days and can be requested to be extended by the vendor’s Cobb County contact.

5.9.8 IS will disable access rights upon notification of termination of employment unless otherwise directed by the CIO.

5.9.8.1 IS will employ processes to remove temporary and emergency accounts after a 90-day review. A similar process will exist for disabling inactive accounts after 90 days unless otherwise directed by the CIO.

5.9.9 IS will control network connection of County-owned mobile devices through mobile device management and/or access control.

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: Some existing 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
v.3.0-2023	July 2023	Cyber Security Technology Services Manager	Security Update