CITY OF ATLANTA	*Control ID*	NIST 800-53
	Effective Date	06/27/2016
	Version Number	5.0
	Revision Date	08/28/2020
Access Control Policy	*Approved By*	Gary Brantley, **Chief Information Officer**
	POC for Changes	**AIM Office of Information Security**

DocuSigned by:
Gary Brantley
5978BF2984D145A...

9/14/2020

Gary Brantley, Chief Information Officer, City of Atlanta **Date Signed**

1.0 Purpose

The purpose of this Access Control Policy ("Policy") is to establish the guidelines to be followed at all times to minimize the security risks associated with unauthorized access to the City of Atlanta's ("City") Information Technology Assets by an internal or external individual or entity. This includes City of Atlanta ("City") employees and vendors that are not authorized to access certain Information Technology Assets. The City of Atlanta Access Control policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish an access control capability throughout the City of Atlanta and its related entities to help the organization implement security best practices with regard to logical security, account management, and remote access.

2.0 Objective

The objective of this Policy is to establish criteria for Access to the City's Information Technology Assets and support services, provide appropriate guidance regarding Authorized User responsibilities; and the security and protection of City equipment, information and/or data.

3.0 Scope

This Policy applies to all City employees, contractors and vendors that provide IT services to the City and all other authorized Users who require access at any time to Information Technology Assets owned or managed by the City.

4.0 Applicability to Laws and other City Policies

The use and access to City Information Technology Assets is subject to applicable federal, state, and local laws. All Authorized Users of City Information Technology Assets that fail to comply with this policy shall be subject to disciplinary action, up to and including dismissal, in conformance with the provisions of the Code of Ordinances of the City of Atlanta, Georgia. Violations of this Policy may also serve as grounds for revocation of privileges to access City Information Technology Assets. In addition, if applicable, violations of this Policy may be referred to the appropriate authorities for criminal or civil prosecution.

5.0 Confidentiality

All users granted authorization to utilize City Information Technology Assets shall maintain the confidentiality of all information accessed, viewed, transferred, or copied during the course of their privileges unless otherwise provided by law.

If there is any question regarding the appropriateness of disclosing or retaining information, employees as well as vendors shall contact their supervisor or the Atlanta Information Management Office of Information Security (AIM OIS).

6.0 Identification Badge Requirements

All users granted authorization to utilize City Information Technology Assets on-site (i.e., any City premise or property) shall obtain an identification badge prior to accessing any Information Technology Assets. Employees and Vendors must visibly display the identification badges at all times while on-site.

- All identification badges must be immediately returned to the City upon completion of the authorized access privilege utilization period or upon termination of relationship with the City.
- Employees and Vendors are prohibited from 'tailgating" through any door that requires badge access. Employees and Vendors for their own safety need to ensure that they utilize their own badge for entry into secure areas. In the event of an emergency, this will aid in determining the whereabouts of all authorized users. Employee or Vendor signature at the end of this document is an acknowledgement that they will abide by these badge usage requirements.
- If an Employee or Vendor forgets their badge, they must sign in and out with the receptionist to ensure that they are accounted for.

7.0 Usage Rules

The City owns, leases, or has the right to specify the use of all of its Information Technology Assets.

Prior to obtaining authorization to access any Information Technology Assets, all Vendors shall read and sign this Policy and then submit the signed copy to the AIM OIS for access authorization.

8.0 Connection of Non-City Equipment - Bring Your Own Device (BYOD)

Employees and Vendors are prohibited from connecting any non-City equipment, including but not limited to, desktops, laptops, notebooks, tablets, hand-held computers, servers, or any related devices to the City network or cloud solutions like O365 without express written authorization from the AIM OIS. Employees and Vendor's non-City computer equipment that is authorized to connect to the City network must meet the following minimum requirements:

- Must have anti-virus and anti-malware protection software installed and running on the portable computing device at all times.
- Must have the latest anti-virus and anti-malware signatures running on the portable computing device at all times.
- Must have the latest service pack and security patches applied on the portable computing device.
- Local Administrator password must meet the requirements of the City's Universal Password Policy.
- Must encrypt any City sensitive information contained on the portable computing device with City approved standard encryption software (i.e., minimum of 256-bit AES encryption).

Vendors are prohibited from connecting and using personal portable computing devices including but not limited to, storage devices (i.e., jump drives, portable drives, etc.), wireless and wired routers, switches, hubs, access points, network appliances, or any device capable of receiving, storing, managing, transmitting electronic data, receiving email, or browsing Web sites on the City network without express written authorization from the AIM OIS**.**

9.0 Access Control Requirements (NIST Access Control based)

Access Control Policy (AC-1) All of City of Atlanta business systems must develop, adopt or adhere to a formal, documented access control policy that addresses

purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Account Management (AC-2) All of City of Atlanta business systems must:

- Identify account types (i.e., administrative, shared, service, individual, group, system, application, guest/anonymous, and temporary accounts).
- Establish conditions for group membership in and application directory/database or Active Directory.
- Identify authorized users of the information asset and specify access privileges.
- Document an appropriate approval process for requests to create accounts. The process should specify the allowable privileges for the accounts and include a justification for these privileges.
- Communicate user account policies and procedures including authentication procedures and requirements to all users of an information system. Users shall be responsible for maintaining the security of their user authentication credentials.
- Assign credentials to users that are unique in order to maintain accountability.
- Change default/generic credentials, such as “root” or “admin” prior to a system being put into production.
- Disable user credentials immediately upon the account owner’s termination from City of Atlanta or when the account owner no longer needs access to the system or application.
- Establish the default access method for files and documents as role-based access control (RBAC), however, other methods to securely access files and documents may be used.
- Restrict access to confidential information to authorized individuals who require access to the information as part of their job responsibilities.
- Disable user credentials that are inactive for a maximum of forty-five (45) days except as specifically exempted by a security administrator.
- Delete all accounts that have been disabled for greater than 365 days.
- Establish user credentials for a non-employee/contractor with a defined expiration date.
- Retain information on system/application logon attempts.
- Disallow the use of guest/anonymous accounts.
- Specifically authorize and monitor the use of administrative, shared, service, and temporary accounts.
- Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred or information assets usage or need-to-know/need-to-share changes.

- Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
- Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated mission's/business functions.
- Review accounts on a periodic basis or at least quarterly.

Access Enforcement (AC-3) City of Atlanta business systems must enforce approved authorizations for logical access to the system in accordance with applicable policy. The combination of a unique user credential and a valid password shall be the minimum requirement for granting access to an information system when IDs and passwords are used as the method of performing identification and authentication.

Information Flow Enforcement (AC-4) City of Atlanta business systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Network must connect to external networks or information systems only through managed interfaces approved by City of Atlanta management. These managed interfaces must consist of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels, web content filters, data loss prevention) arranged in accordance with an effective, security architecture. Protective controls shall at a minimum include the following:

- Authentication to ensure that routing tables do not become corrupted with false entries.
- Email should correspond to data leak prevention (DLP) rules to maintain compliance, identify, and monitor the safe handling of specific categories of confidential data as defined in the Data Classification policy.
- Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to conduct business.

Separation of Duties (AC-5) City of Atlanta business systems must have:

- Separation of duties for individuals as necessary, to prevent malevolent activity without collusion.
- Document separation of duties.
- Implements separation of duties through assigned information asset access authorizations.
- Monitor and review system usage for activities that may lead to business risks by personnel who are able to quantify and qualify potential threats and business risks.
- Enforce separation of duties from critical IT roles.

Least Privilege (AC-6) City of Atlanta business systems must employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

- Access to confidential data shall be controlled through various appropriate access control mechanisms.
- Require that users of information system accounts, or roles, with access to sensitive, use non-privileged accounts or roles when accessing non-privileged functions.
- Restrict privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties.
- Prevent non-privileged users from executing privileged functions: including disabling, circumventing, or altering implemented security safeguards and countermeasures.

Unsuccessful Logon Attempts (AC-7) To the extent possible, an information system shall limit unsuccessful logon attempts to five (5) during a 120-minute period before the user's account is disabled. The locked-out duration shall be at least thirty (30) minutes unless the end user successfully unlocks the account through a challenge question scenario or a system or security administrator or an authorized service desk staff member re-enables the user's account.

System Use Notification (AC-8) City of Atlanta business systems must:

- Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
- Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.

Previous Logon Notification (AC-9) Where supported, information systems shall notify the users, upon successful logon (access) to the system, of the date and time of the last logon. Users are notified of the number of unsuccessful logons since the last successful logon.

Concurrent Session Control (AC-10) City of Atlanta business systems must limit the number of concurrent sessions for each system account to **2** for information assets.

Session Lock (AC-11) City of Atlanta business systems must prevent further access to the information asset by initiating a session lock after **15 minutes** of inactivity or upon receiving a request from a user. In addition, City of Atlanta business systems

must retain the session lock until the user reestablishes access using established identification and authentication procedures.

Session Termination (AC-12) City of Atlanta business systems must have:

- Network-connected single-user systems, such as laptops and PCs, shall employ City of Atlanta- approved hardware or software mechanisms that control system booting and that include a time-out- after-no-activity (for example, a screen saver).
- This time-out system must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. For some higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by City of Atlanta policy, industry standard (e.g., PCI DSS) or other regulations.
- An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the City of Atlanta Network.

Permitted Actions without Identification or Authentication (AC-14) City of Atlanta business systems must identify specific user actions that can be performed on the information asset without identification or authentication. In addition, City of Atlanta business systems must document and provide supporting rationale in the security plan for the information asset, user actions not requiring identification and authentication.

- Users may access public websites or publicly available information on accessible information systems without identification and authentication.
- System/business owners, in collaboration with service provided must identify, provide justification, and develop supporting documentation for user actions that can be performed on systems not requiring identification and authentication.

Remote Access (AC-17) City of Atlanta business systems must:

- Document allowed methods of remote access to the information assets.
- Establish usage restrictions and implementation guidance for each allowed remote access method.
- Monitor for unauthorized remote access to the information asset.
- Authorize remote access to the information asset prior to connection.
- Enforce requirements for remote connections to the information asset.
- Access to City of Atlanta's internal networks via external connections from local or remote locations including homes, hotel rooms, wireless devices and off-site offices shall not be automatically granted with network or system access. Systems shall be available for on- or off-site remote access only after an explicit

request is made by the user and approved by the manager for the system in question.

- Access shall be permitted through a City of Atlanta-managed secure tunnel such as a Virtual Private Network (VPN) or Internet Protocol Security (IPSec) that employs FIPS 140-2 compliant encryption techniques for encryption and secure authentication. Virtual private networks (VPNs) shall require user authentication and encryption strength compliant with the City of Atlanta encryption standard.
- Systems containing confidential data must ensure that the information system is configured to employ automated mechanisms to monitor and control remote access methods.
- Each user who remotely accesses an internal network or system shall be uniquely identifiable. Account passwords shall not traverse the network in clear text and must meet minimum requirements of the City of Atlanta password policy.
- All users wishing to establish a remote connection via the Internet to the City of Atlanta's internal network must first authenticate themselves at a firewall or security device.
- Remote access for system administration functions that originate from networks external to City of Atlanta's network, such as the Internet, must be accomplished, at a minimum, using multi-factor authentication (MFA). It is recommended that all other remote access to systems, specifically those with either confidential data, be achieved using MFA (Multi-Factor Authentication) technologies.

Use of External Information Systems (AC-20) City of Atlanta business systems must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to:

- Access the information asset from the external information systems.
- Process, store, and/or transmit organization-controlled information using the external information systems.
- Access to an external system is only permitted when an approved information system connection or processing agreements with the organizational entity hosting the external information system are in place.
- Access to restricted or highly restricted information from external information systems, other than through a virtual desktop infrastructure is prohibited.

10.0 Reporting, Violations and Enforcement

If an account or password is suspected to have been compromised, the Authorized User must report the incident immediately to the AIM Service Desk or AIM 0IS and change their password or request to have their password changed. All Authorized Users are responsible for the enforcement of this Policy. All department heads and supervisory personnel are responsible for ensuring that their directives are implemented and administered in compliance with the approved Policy.

Any violation of this policy may result in disciplinary action, up to and including termination of employment. City of Atlanta reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. City of Atlanta does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties.

Accordingly, to the extent permitted by law, City of Atlanta reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

11.0 References

The following are references applicable to this policy:

NIST Special Publication 800-53 Revision 4 - National Institute of Standards and Technology (U.S. Department of Commerce) Security and Privacy Controls for Federal Information Systems providing a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the U.S. from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors. This policy complies with Revision 4, Technical Controls, Access Control Family, April 2013 (Updated 1/22/2015).

AUTHORIZED USER ACKNOWLEDGEMENT AND SIGNATURE

I hereby acknowledge that I have received a copy of the City of Atlanta Access Control Policy ("Policy"), dated as of ; that I ——————— have read the Policy; that I understand the Policy; and that I am bound by and will abide by Federal, State and Local laws and ordinances, the Policy's requirements, any applicable supplements and any additional or amended policies and procedures issued from time to time.

I further acknowledge that I understand that any violation of this Policy may subject me or my company to immediate termination of the authorized access privilege utilization period, relationship with the City, or possible civil and criminal penalties.

_____

Name of Authorized User (Print)

_____

Title

_____

Company

_____

Signature of Authorized User

_____

Date