

OFFICE OF THE MAYOR
ADMINISTRATIVE ORDER 2007 - 01

AN ADMINISTRATIVE ORDER ESTABLISHING A CITY OF ATLANTA
VENDOR ACCESS POLICY

WHEREAS, the City of Atlanta employs the use of Electronic Communications Resources to facilitate and support its daily business operations; and

WHEREAS, the City of Atlanta recognizes that Vendors often play an important role in supporting City business operations and require various levels of access privilege to the City of Atlanta's Electronic Communications Resources to fulfill their job responsibilities; and

WHEREAS, in order to protect these resources, adequate limits and controls must be established and maintained to regulate the availability of data that can be accessed, viewed, copied, modified, or controlled by Vendors; and

WHEREAS, a comprehensive and updated citywide policy will ensure that all City of Atlanta Electronic Communications resources are subject to management controls as they are utilized by City of Atlanta vendors; and

WHEREAS, the Department of Information Technology developed this policy to establish policies for Vendor access to the City of Atlanta's Electronic Communications Resources and support services; provide appropriate guidance regarding Vendor responsibilities; and the security and protection of City equipment and information.

NOW, THEREFORE, BY THE POWER VESTED IN ME, AS MAYOR OF THE CITY OF ATLANTA, pursuant to the City of Atlanta Charter, 1996 Ga. Laws, p. 4469 *et seq.*, Section 3-104 and Section 2-182 of the Code of Ordinances of the City of Atlanta, Georgia, it is hereby ordered as follows:

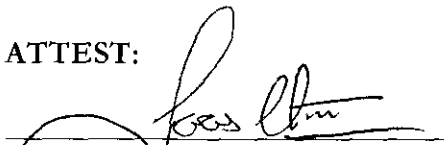
Section 1: The *Vendor Access Policy* attached hereto as Exhibit "A" is hereby enacted as the policy governing vendor access to the City of Atlanta's electronic communications resources within all City of Atlanta departments, bureaus, offices and agencies and may be amended as needed by the Chief Information Officer.

Section 2: This administrative Order will be effective on March 5, 2007 and shall remain effective until rescinded by the Mayor.

SO ORDERED, this 22 day of March, 2007.


SHIRLEY FRANKLIN, Mayor
City of Atlanta

ATTEST:


Municipal Clerk

FORIS WEBB III
DEPUTY MUNICIPAL CLERK

Scanned by VA, Date 3-23-07

Filed by _____, Date _____

EXHIBIT "A"



CITY OF ATLANTA VENDOR ACCESS POLICY

1. OVERVIEW

This Vendor Access Policy (“Policy”) sets forth the policies and guidelines to be followed at all times to minimize the security risks associated with access to the City of Atlanta’s Electronic Communications Resources by an external individual or entity.

The City of Atlanta employs the use of Electronic Communications Resources to facilitate and support its daily business operations. The City of Atlanta recognizes that Vendors often play an important role in supporting City business operations and require various levels of access privilege to the City of Atlanta’s Electronic Communications Resources to fulfill their job responsibilities. In order to protect these resources, adequate limits and controls must be established and maintained to regulate the availability of data that can be accessed, viewed, copied, modified, or controlled by Vendors.

2. PURPOSE

The objective of this Policy is to establish policies for Vendor access to the City of Atlanta’s Electronic Communications Resources and support services; provide appropriate guidance regarding Vendor responsibilities; and the security and protection of City equipment and information.

3. SCOPE

This Policy applies to all Vendors who require access at any time to Electronic Communications Resources owned or managed by the City of Atlanta.

4. RELATION TO LAWS AND OTHER POLICIES

The use and access of Electronic Communications Resources is subject to federal, state, and local laws. This Policy should be closely reviewed in conjunction with the City of Atlanta Electronic Communications Resources Policy.

5. DEFINITIONS

The following relevant terms are related to Electronic Communications Resources access, operation and security:

Authorized User

Any person who uses the Electronic Communication Resources with proper authority. The term includes employees of The City of Atlanta who have completed the required prerequisites for use and persons who are not employees and have been properly authorized to use the Electronic Communication Resources.



CITY OF ATLANTA VENDOR ACCESS POLICY

Electronic Communications

Any communications transmitted electronically via the use of the Electronic Communications Resources.

Electronic Communications Resources

All information processing and communications facilities, including computers, facsimile machines, telephones, cellular telephones, wireless email devices, PDA's, pagers, copiers, software, on line accounts, email facilities, facilities for Internet/Intranet, Extranet access, storage media, network accounts, computer and email and instant messaging files and messages and related equipment and documentation employed or stored by the City of Atlanta; and all such information processing and communications facilities employed in the City of Atlanta's business that are connected to or able to be connected to its facilities from locations outside of the City of Atlanta's premises, including personal information processing and communications equipment and software owned or leased by City of Atlanta.

Vendor

All non-employee individuals and entities, including but not limited to service providers, independent contractors, consultants, sales representatives, and guests of the City of Atlanta who require access to the City of Atlanta Electronic Communications Resources.

6. CONFIDENTIALITY

All Vendors granted authorization to utilize City of Atlanta Electronic Communications Resources shall maintain the confidentiality of all information accessed, viewed, or copied during the course of their access privileges unless otherwise provided by law.

If there is any question regarding the appropriateness of disclosing or retaining information, Vendors shall consult with the Office of Information Security (INFOSEC).

7. IDENTIFICATION BADGE REQUIREMENTS

All Vendors granted authorization to utilize City of Atlanta Electronic Communications Resources shall obtain a temporary identification badge prior to accessing any Electronic Communications Resources located on the premises of any City of Atlanta property.

Vendors must visibly display the temporary identification badges at all times while on city property.

All temporary identification badges must be immediately returned to the Office of Information Security (INFOSEC) upon completion of the authorized access privilege utilization period or upon termination of a service agreement relationship with the City.



CITY OF ATLANTA VENDOR ACCESS POLICY

8. USAGE RULES

The City of Atlanta owns, leases or has the right to specify the use of all Electronic Communications Resources.

Prior to obtaining authorization to access any Electronic Communications resources, all Vendors shall submit a written request to the Office of Information Security (INFOSEC) for access authorization including the following:

- Name;
- Company;
- Address;
- Telephone Number;
- Nature and Scope of Access Request;
- Access Utilization Period;
- Description and Type of Non-City Equipment to be connected to any Electronic Communications Resources;
- Description and Type of Non-City Installed Software to be utilized with any Electronic Communications Resources;
- List of individuals, if more than one, requiring access;
- Certification that a Criminal Background Check has been conducted on all individuals requesting access to any sensitive information or equipment;
- Completed Authorized User Acknowledgement and Signature Sheet for Vendor Access Policy;
- Completed Authorized User Acknowledgement and Signature Sheet for Electronic Communications Resources Policy; and
- Acknowledgement that any changes to the submitted information will be updated within 24 hours.

Vendors are eligible to use the Electronic Communications Resources with proper written authorization from a department head and with the written approval of the Office of Information Security (INFOSEC).

Any Vendor given access to the City of Atlanta's equipment, internet and email resources will be considered an Authorized User and subject to the same policies as employees and must undergo the same training as specified in the City of Atlanta Electronic Communications Resources Policy.

Upon approval authorizing a Vendor to access the requested City of Atlanta Electronic Communications Resources, the Office of Information Security (INFOSEC) will provide every Vendor with a designated City of Atlanta point of contact to ensure compliance with this Policy.



CITY OF ATLANTA VENDOR ACCESS POLICY

Vendor access as an Authorized User must be uniquely identifiable and subject to recordation. At a minimum, all Vendor access occurrences must be entered into a log and readily available to the Office of Information Security (INFOSEC) or designated City personnel upon request. Logs must include, but are not limited to, occurrences such as Vendor access times and dates, personnel changes, password changes, project milestones, and business deliverables.

Vendors are prohibited from copying City of Atlanta Information onto their personal computers or devices without prior, written approval from the Office of Information Security (INFOSEC) or designated City personnel.

All software that the Vendor uses to provide service to the City of Atlanta must be properly inventoried and licensed.

Vendor must follow all applicable City of Atlanta change control processes, procedures and policies.

All Vendor maintenance equipment on the City of Atlanta network that connect to the outside world via the network, telephone line, or leased line, and all City Information Resource Vendor Accounts will remain disabled except when in use for authorized maintenance.

Vendors shall comply with all federal, state, and local auditing requirements, including available access to the Vendor's work product and records.

Vendors shall not access any Electronic Communications Resources outside the nature and scope of its original approved access request without approval from the Office of Information Security (INFOSEC).

Designated City of Atlanta personnel must identify, clear, accompany and supervise any Vendor who requires access to any City of Atlanta data centers, wiring closets, or protected areas.

9. CONNECTION OF NON-CITY EQUIPMENT

Vendors are prohibited from connecting any non-city equipment, including but not limited to personal computers, notebooks, tablet PCs, hand-held computers, PDA's, or servers to the City of Atlanta network without express written authorization from the Office of Information Security (INFOSEC).

Vendor's non-city computer equipment that is authorized to connect to the City of Atlanta network must meet the following minimum requirements:

- Must have anti-virus software installed and running on the computer at all times.



CITY OF ATLANTA VENDOR ACCESS POLICY

- Must have the latest anti-virus signatures running on the computer at all times.
- Must have the latest service pack and security patches applied on the computer.
- Must be added to the domain.
- Must have the Domain Admin group added to local Administrator group.
- Local Administrator password must meet the requirements of the City of Atlanta Electronic Communications Resources Policy.
- Must disable personal firewall while on the City of Atlanta network.
- Must encrypt any City sensitive information contained on the computer with City approved standard encryption software.

Vendors are prohibited from connecting and using personal portable devices including but not limited to, storage devices (i.e., jump drives, portable drives, etc.), wireless/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 of Atlanta network without express written authorization from the Office of Information Security (INFOSEC).

10. SERVER DEPLOYMENT

All production, development, or test servers installed on the City of Atlanta network by a Vendor must meet Department of Information Technology (DIT) Server Configuration Standards, as well as the following minimum requirements:

- Must have anti-virus software installed and running on the server at all times.
- Must have the latest anti-virus signatures running on the server at all times.
- Must have the latest service pack and security patches applied on the server.
- Must be added to the domain.
- Must have the Domain Admin group added to local Administrator group.
- Local Administrator password must meet the requirements of the City of Atlanta Electronic Communications Resources Policy.
- Application Service accounts must meet the requirements of the City of Atlanta Electronic Communications Resources Policy.

11. REMOTE ACCESS/VPN

Vendors are prohibited from accessing City of Atlanta Electronic Communications Resources remotely without express written authorization from the Office of Information Security (INFOSEC).

Vendor remote access level must be clearly stated, identifiable, logged, auditable, and limited only to the authorized systems in which the Vendor must have access in order to perform its assignments.



CITY OF ATLANTA VENDOR ACCESS POLICY

Vendor remote access time (logon hours) must be clearly stated, logged, and auditable.

Vendor network/VPN accounts must be disabled immediately upon completion of the authorized access privilege utilization period or upon termination of a service agreement relationship with the City.

Vendor's activities on the network must be entered into a log and available to City personnel upon request. Logs must include, but are not limited to, connection times, disconnection times, systems accessed, files accessed, tasks performed, or any other activities performed while on the network.

Vendors are prohibited from remotely installing, configuring, or modifying systems or applications on the City of Atlanta network without express written authorization from the Office of Information Security (INFOSEC).

Installing Telnet, FTP, or SMTP services is prohibited on any servers and workstations on the City of Atlanta network.

12. REPORTING, VIOLATIONS AND ENFORCEMENT

Vendors have a duty to report all resources problems, security incidents, suspected and known violations of this Policy or the Electronic Communications Resources Policy to the Office of Information Security (INFOSEC) within 48 hours so that prompt remedial action may be taken. This obligation includes reporting of any suspected malicious code.

13. UNAUTHORIZED USERS

Any use of the Electronic Communications Resources or Facilities by any person who is not an Authorized User is strictly prohibited. Any such unauthorized use will be referred to appropriate governmental authorities for action and will be prosecuted vigorously by the City of Atlanta.

EFFECTIVE DATE:



**CITY OF ATLANTA
VENDOR ACCESS POLICY**

AUTHORIZED USER ACKNOWLEDGEMENT AND SIGNATURE

I hereby acknowledge that I have received a copy of the City of Atlanta Vendor Access 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 the Policy's requirements and 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, service agreement relationship with the City, or possible civil and criminal penalties.

Name of Authorized User (Print)

Title

Company

Signature of Authorized User

Date