Title	**Access Revocation Policy**
Type	Policy
Category	Security
Status	Approved
Approved	01/09/2013
Revised	06/16/2015
Scope	Affects all City information technology assets.

Policy

Policy Definition:
Access privileges are granted to an individual by username. He or she may use that username to access and use the resources of the city network. Complying with acceptable use of technology and information resources requires users to:

- use resources only for authorized purposes;
- protect your username and system from unauthorized use.
- access only information that is your own, that is publicly available, or to which you have been given authorized access.

Policy Provisions: City employee access to information technology systems will be granted only upon the written approval of the system owner. The level of access will be granted based on the duties to be performed and approved by an immediate supervisor.

Permanent Revocation.
The Department of Technology and Innovation (DTI) shall permanently revoke a user's access to a City information technology asset upon written notification from one of the following:

- The user's Department Management;
- The Department owning the information technology asset;
- The Human Resources Department.

The notice must state that the user shall no longer have access to the information technology asset due to promotion, transfer, reassignment, inactivity, retirement, termination, abuse, or

pursuant to a court order or other administrative, civil or criminal proceeding.

Temporary Revocation -- with notice.
DTI shall temporarily revoke a user's access to a City information technology asset:

- When DTI is requested in writing to do so by the user's Department for any reason, including but not limited to disciplinary action. The user's Department shall initiate a Computer Abuse / Security Incident pursuant to City policies and procedures. The revocation shall remain in effect until DTI is notified by the user's Department that the Incident has been closed and access is either to be restored or permanently revoked.
- When DTI is requested in writing to do so by the Department that owns the information technology asset. The Department owning the information technology asset shall notify the user's Department and shall initiate a Computer Abuse / Security Incident pursuant to City policies and procedures. The revocation shall remain in effect until DTI is notified by the user's Department **and** the Department owning the information technology asset that the Incident has been closed and access is either to be restored or permanently revoked.
- When revocation is necessary in order to preserve evidence being used to resolve an ongoing Computer Abuse / Security Incident or other administrative, civil or criminal proceeding which may or may not directly involve the subject user. The revocation shall be requested by the Incident Manger or the Information Security Manager as provided by City Incident policies and procedures. The revocation shall remain in effect until DTI is notified by the user's Department Management that the Incident or proceeding has been closed and access is either to be restored or permanently revoked.
- When an employee is not in compliance with the City's Employee Information Technology Security Certification Policy. The revocation shall be requested by the Chief Information Officer or his designee as provided by that policy. The revocation shall remain in effect until the employee successfully completes the certification or renewal process.

Temporary Revocation -- without notice.
DTI may temporarily revoke a user's access to a City information technology asset without notice:

- When the user's credentials have not been used and/or the information technology asset has not been accessed by the user beyond a maximum period of time. Time periods may vary by information technology asset and shall be published in a standard. The revocation shall remain in effect until DTI is requested to restore or permanently revoke access as provided in this policy.
- When revocation is necessary in order to perform scheduled or emergency maintenance on the affected information technology asset. Prior notice should be given whenever possible. The revocation shall remain in effect only until the maintenance is completed and the affected information technology asset is returned to service.
- By an authorized system administrator at any time in order to safeguard the reliability, availability and integrity of the City's information technology infrastructure. The system administrator shall report the revocation to the Chief Information Officer or his designee, who shall initiate a Computer Abuse / Security Incident pursuant to City policies and procedures. The revocation shall remain in effect until DTI is notified by the user's Department Management that the Incident or proceeding has been closed and access is either to be restored or permanently revoked.

Rationale

Access control and accountability are necessary in order to effectively protect City information technology assets.

See also:

- Information Technology Protection Policy.
- Computer Abuse Incident Reporting and Response Policy.