INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	**Onboarding and Termination of Users’ Computer Access**	Policy Number: 712
Effective:	July 29, 2016	
Supersedes:		
Approval:	Tom Shewchuk, IT Director	Page 1 of 2

Purpose

Ensures secure practices and standard methodology for establishment of network user access for new hires. Similarly standardizes termination of access upon separation of employment, while maintaining security and preventing unauthorized access to our computer systems.

Rationale

1. Access to computer systems is required for many job roles throughout the City of Ann Arbor
2. A standard, uniform process needs to be applied to establishment of computer access. Access cannot be granted until all prerequisites have been completed.
3. Access to computer systems must be terminated once employment with the City of Ann Arbor has ended (due to voluntary or involuntary separation, retirement, or death).

Onboarding Responsibilities

Information Technology is not to grant computer access until so authorized by Human Resources.

Human Resources notifies Information Technology of authorization to grant computer access via IT’s helpdesk ticket system. The new employee’s supervisor should provide HR all available information with regards to computer access needed.

IT routes the helpdesk ticket to the Infrastructure Team. A user account is created, and appropriate access and rights are granted.

Termination Responsibilities

Authorization to revoke computer access to an employee can come from a variety of sources depending on the status of the employee:

- Regular Employees: Authorization to revoke access should come from Human Resources. Revocation authorization will also be accepted by IT from any appropriate manager or supervisor of the employee in question. If notice does not come from HR, IT will notify HR.
- Temporary Employees (or other non-regular employees such as contractors): Authorization to revoke access should come from the employee's supervisor. HR is not involved in the separation process of temp employees.

Authorization to revoke access should be received by IT in the form of a help desk ticket. If there is time sensitivity to the revocation of access, other forms of communication are acceptable (phone call, email, in person visit) and need to be documented after the fact via helpdesk ticket.

IT routes the helpdesk ticket to the Infrastructure Team. Access is revoked via disabling of Active Directory user account and badge access at the appropriate time (immediately, if so requested, or at a scheduled date and time that corresponds to the employee's final departure).

At a later date, Infrastructure Team member performs additional activities to complete termination process.

- Data from network home folder is moved to a read-only archive area
- Data from Exchange mailbox is archived in PST format and copied to read-only archive data
- Helpdesk contacts separated employee's supervisor and inquires if any data retrieval should be performed from the employee's desktop or laptop. Any data identified will be provided to Infrastructure Team to copy to read-only archive area
- Infrastructure Team notifies other members of Information Technology to revoke other access
    - Jim Clare: local SQL server accounts
    - Dave Wilburn: Cityworks and Geocortex access
    - Kyle Spade: LOGOS access
    - Rick Powell and/or Scott Harrod: TRAKiT access
    - Jackie Steinaway: disables all access within CJIS applications for Police and City Attorney's Office
    - Alicia Green: disables all access within CJIS applications for 15th District Court
- Active Directory user account is held in a disabled state for 13 months. After 13 months, ID is permanently deleted.

Termination Audit Policy

Infrastructure Team conducts audits of Active Directory to ensure user access has been revoked for separated employees as follows:

- On a monthly basis, reports are run from UltiPro.
    - Any job changes are recorded in Active Directory as appropriate
    - Separation listings are reviewed. Any terminations found that have not been processed by the Termination Responsibilities in this document are followed up upon and access is revoked as appropriate.
- On a quarterly basis
    - A report is run from UltiPro to review all users within Active Directory. Any terminations shown in UltiPro that are not reflected in Active Directory are followed up upon and access is revoked as appropriate.
    - A report is run from Active Directory to review network user ID activity. Any user IDs that have been inactive for 70 or more days are handled as follows:
        - The user ID is disabled
        - The account is placed into a hold state for 13 months
        - If the user ID is still disabled after 13 months, the account is disabled, and data is archived as follows:
            - Data from network home folder is moved to a read-only archive area
            - Data from Exchange mailbox is archived in PST format and copied to read-only archive data
            - Helpdesk contacts separated employee’s supervisor and inquires if any data retrieval should be performed from the employee’s desktop or laptop. Any data identified will be provided to Infrastructure Team to copy to read-only archive area