HAMPTON VA

No. IT– 043 Replaces IT-030	Policy Name: Elected and Appointed Public Official IT Access Additions, Expirations, Departures, and Changes
Effective Date: 7-1-2011 Last Revised Date: 12-17-2014	Citywide Policy _ IT Policy X IT Procedure _
Approved By: IT Director	

I. Policy Reference: 09-005 IT Security Policy Statement

The IT department has the responsibility to manage City owned hardware, software, telecommunications services and electronic access to City provided e-mail, files, applications, and other City owned data for elected and appointed officials at the time of appointment, departure, term expiration, transfer or when there is an identified security risk to the City. Standard processes are used when there is a normal transition through the election or appointment process. Emergency procedures are used if there is an identified security risk to City systems or data. The City has the responsibility to manage a smooth transition as well as protect data as specified under state records retention laws and procedure.

II. Scope – This procedure applies to the following elected and/or appointed positions

- City Manager
- City Attorney
- Mayor
- City Council Member
- Clerk of Council
- Treasurer
- Commissioner of Revenue
- Clerk of Court
- Judges
- Credit Union Manager
- Sheriff
- Voter Registrar

III. Standard Procedure

The standard procedure is used to obtain City owned electronic devices and remove elected and/or appointed official access from the City's network and systems when there is a change due to an election or appointment process and no perceived security threat has been identified or communicated to IT. The procedure also identifies the process for providing access to new elected and appointed officials. The following steps will be taken to ensure proper access to data and applications:

1. The City Manager's Office or its designee and/or the City Attorney's Office will notify the IT Director or their designee through e-mail or voice mail followed by a written notice of the personnel changes. If the City Attorney's appointment terminates then the City Manager will notify the IT Director of the change; alternatively if the City Manager's appointment terminates the City Attorney will notify the IT Director of the change. The correspondence will at a minimum include the name, office held and the time and date of the departure. This should be received by IT as soon as possible after the information is known and in all cases prior to the change in office or appointment.
2. Prior to the date and time of expiration ("Expiration") of the term of office or appointment, the IT Department will identify and inventory all hardware, software, mobile devices and telecommunications services assigned to the individual whose term is expiring. The inventory will be shared and verified with the individual prior to departure. If an employment agreement specifies the transfer of City assets at the time of departure, these assets will be identified and documented in the inventory.
3. At the date and time of the departure of office or appointment the IT Department will suspend access to e-mail, network services, applications and files to the terminated individual. No files will be deleted, moved, accessed or tampered with at this time by any IT or other City employee. Requests for access to the information will be made to the City Manager's Office and/or the City Attorney's Office
4. At the date and time of the departure, the IT Department or their designee will terminate all telecommunications services assigned to the terminating official
5. At the date and time of the departure of office or appointment the elected or appointed individual will turn over all City owned devices and software to the IT Department or their designee. Documentation of the inventory received will be kept by the IT Department or their department designee. A copy of the documentation will be provided to the departing official. In cases where an employment agreement specifies the transfer of IT assets upon departure, or at the specific direction of the City Manager and/or the City Attorney's office, the IT Department will only obtain assets that remain as part of the City's inventory. Assets that are identified as transferring to the terminating official will be removed from the City's inventory. Documentation on the transfer of the assets will be obtained by the City and a copy will be provided to the departing official.
6. The City Manager's Office or its designee and/or the City Attorney's Office will notify the IT Director or their designee through e-mail or voice mail followed by a written notice of the replacement elected or appointed official. Information will include the name, position and official start date and time of the individual. At the specific direction of the City Manager and/or the City Attorney's office, the IT Department or their designee may take appropriate steps to allow the new replacement elected or appointed official electronic access to City provided e-mail, files, applications, and other City owned data in advance of the official start date; however any activity

predating the official start date and time for the individual shall not constitute a "Public record" or "record" as that term is defined in Virginia Code Section 42.1-77.

7. The IT Department will create a new account, e-mail and file storage space for the newly elected or appointed official. The IT department will notify the newly appointed official of instructions for gaining access and the time and date when access will be available. Newly appointed or elected officials will not have e-mail or network access prior to their official start date unless they already have city network access serving in another capacity. In those cases access will not be provided to files or applications of their new position until the official start date and time. Access to files and applications from their previous position will be reviewed to determine if access is still required for their new duties. If these files and applications are not necessary to perform their new duties then access to those files and applications will be terminated.
8. The City Manager's Office or its designee and/or the City Attorney's Office will provide the IT department with permission to grant a newly appointed or elected official access to e-mail and files belonging to their predecessor. All correspondence granting this access should be provided through e-mail or written memorandum to the IT Director or their designee.
9. IT staff will grant access to e-mail and electronic files created and owned by the official's predecessor. In addition, the IT Department will contact the replacement official and notify them of the state records retention schedule as it pertains to their predecessor's files and e-mail. The IT department will be available to assist in archiving these files at the appropriate time.
10. The IT Department or their designee will identify inventory assets and telecommunications services assigned to the newly appointed or elected official. The City Attorney's Office will notify the IT Department of any employment agreement clauses that specify the transfer of assets upon departure. The assigned inventory list will be maintained and updated as assets change. The inventory list will be provided to the appointed or elected official within 60 days of their start date and when any updates are made throughout their term in office.
11. For terminated elected or appointed officials where file and e-mail access has not been granted to their replacement, the IT department will archive the e-mail and other electronic files of the departed individual in accordance with the state records retention schedules.

IV. Emergency Procedures

There may be instances where a security risk or threat has been identified by the Police Department, the City Manager's Office and/ or the City Attorney's Office. In these cases, the Chief of Police, City Manager and/ or the City Attorney will notify the IT Director or their designee immediately of the threat and request access to data to be removed or suspended, telecommunications service suspension, and the need for inventory assets to be collected

1. These requests should go to the IT Director or any IT Manager for processing. If the request is after hours the requestor should contact 311 who will contact the engineer on call or IT Director to process the request.
2. Network engineers will suspend the network account immediately, document the request and notify their manager of the request as soon as possible. If there are other threats communicated to the engineer that require additional removal of access or investigation, the engineer will work with the police department and notify their IT manager and other appropriate IT staff as soon as possible to address the security issues.
3. If needed, telecommunications staff will suspend telecommunications services as soon as possible and notify their manager or the IT Director of the request as soon as possible.
4. If needed, IT staff will remove equipment accessible to the terminating official. If assets are in the possession of the individual at their home or on their person the IT staff will not attempt to remove this equipment in emergency situations but will provide information on the location and description of the assets to the appropriate individuals requesting the emergency removal of assets.
5. As soon as possible during and after the event, engineers will document the request and associated work through a tracking ticket, e-mail or other formal document.
6. The IT Department will fully comply and cooperate in any IT Security related investigations requested by the Hampton Police Department, the City Manager and/ or the City Attorney’s Office.