HAMPTON VA

No. IT– 031	Policy Name: Procedures for Disabling Accounts
Effective Date: 7-1-2011 Last Revised Date: 7-5-2014	Citywide Policy _ IT Policy _ IT Procedure X
Approved By: IT Director	

Procedures for Disabling Accounts

The following processes permit an orderly transition for the affected Department, while maintaining the integrity of the data sources in the event any Litigation actions are encountered. Additionally, this process also ensures a clean Records Retention copy is maintained for those users requiring extended retention.

- Ticket is created specifying the department, requestor and user of the affected e-mail. Only department heads or their designee can request and e-mail account to be disabled or terminated. Departments have the option of having another individual in the department be the recipient of e-mails during a transition period. Transition periods are normally set at 30 days.
- IT identifies from the department whom they want to receive any e-mails addressed to the departing user.
- The departing user's account is then disabled, and set to be deleted within 30 days or earlier.
- The departing user's e-mail address is moved as an alias onto the individuals e-mail account identified by the department. (They will then receive all new e-mail addressed to the departing user)
- The departing user's exchange account is exported to a pst file, and provided to the department IAW their guidance.
- The departing user's Z drive folder can be either copied or provided to the Department's Representative, depending upon whether Litigation action is expected.
- Tech Support can then assist the Department's Representative with configuring Outlook rules to have incoming e-mails addressed to the departing member placed into whatever folder they would like. Additionally, a rule can be created to automatically send out an Out of Office Reply to the sender of an e-mail addressed to the departing user's account.
- Depending upon Records Retention requirements, Tech Support may need to clone the individual's hard drive. Department heads, council members, the Mayor, City Manager and Assistant City managers all must have their hard drive data retained at time of departure and retained based on records retention guidelines.
- Tech Support can remote into the departing person's PC, and assist the Department's Designated Representative with gaining access to any files on the PC that the departing user may have had.
- It then becomes the responsibility of the department to destroy the copied PST file and any Z drive folder information IAW the City's Record Retention policy. IT Engineering will then either destroy the original e-mail account at the end of 30 days, or hold a copy of the exported PST file in a secured location, if we are advised of potential Litigation action by the department/City Attorney's office. Department heads, City Manager, Assistant City Managers, Council Members and the Mayor's mail will be hold a copy of the exported PST file in a secured location and retain based on records retention guidelines.

- Departing individuals with access to other applications will also have their accounts disabled or terminated. This includes but is not limited to the following:
    - New World
    - Infinium
    - HITS
    - Laserfiche
    - Salesforce & Basic Gov
    - Remote Access (VPN, GoToMyPC or vWorkspace)
    - UseDirect
    - CivicPlus
    - GIS
    - Microsoft Office 365
    - Other City Applications known to IT

The Tech Support will notify other areas in IT and/or department contacts of the departing employee.