HAMPTON VA

No. IT– 048	Policy Name: Office 365 Administrator Rights
Effective Date: 10-20-2015 Last Revised Date: 02-02-2016	Citywide Policy_ IT Policy _ IT Procedure X
Approved By: IT Director	

Office 365 Administrator Rights Procedure

Background

The Office 365 platform provides e-mail and other online services to all City employees in a shared environment. The Office 365 contract and services are managed, licensed and deployed through the City's IT Department. The Hampton Police Division (HPD) has a need to perform some administrative tasks in the Office 365 environment to support e-mail and exchange services for HPD users. This procedure identifies the types of permissions, process for allocating permissions and auditing of administrative activities on the Office 365 platform.

Scope

Applies to all City Departments. HPD administrative permissions for Office 365 only apply to activities and needs of HPD personnel and users. HPD users granted administrative permissions shall utilize the functions inherent in the permissions to change, update, view or provide any services only to HPD employees. The IT Department will use the Office 365 administrative functions to provide service and service changes to all other users in the City.

Office 365 Administrator Responsibilities

1. Administrators will follow all IT security policies and procedures at all times when utilizing the City network and network services
2. Administrators will support and enforce all security and best practices in IT Security
3. Administrators will immediately notify the IT Department and IT Director of any security breach or employee misuse of O365 or City network resources
4. Administrators will keep up to date with changes in the O365 environment and proactively utilize online training, forums, knowledge bases and other materials.
5. All changes need to have a documented business or technical reason for implementation

Levels of Permission

Administrators will only be granted the permissions necessary to perform their primary job functions and no more. Below are the administrator options that the City utilizes to manage O365:

1. User Administrator – Resets passwords, monitors service health, and manages user accounts, user groups, and service requests. The user management admin cannot delete a global admin, create other admin roles, or reset passwords for billing, global, and service admins.
2. Exchange Administrator – Has administrative access to Exchange Online through the Exchange admin center (EAC), and can perform almost any task in Exchange Online
3. Billing Administrator - Makes purchases, manages subscriptions, manages support tickets, and monitors service health. (For IT Staff Only)
4. Global Administrator - Has access to all administrative features. Global admins are the only admins who can assign other admin roles and conduct global or group searches.

The Process

1. Granting Administrator Privileges - Administrators will be granted permission levels based on their job function, skill level and department needs.
   a) Administrators must possess appropriate technical experience and prerequisites to perform the administrative functions on the permission level.
   b) All Administrators will be approved by the IT Director. Administrators supporting the HPD will be approved by the IT Director and the Police Chief
   c) Administrator Training & Knowledge Transfer
      i) Administrators will complete a knowledge transfer prior to being given administrative privileges.
         - The IT Sr. System Engineer will provide any documentation and a knowledge transfer session for each administrator.
         - The IT Sr. System Engineer will provide documentation that the administrator has completed the training and all appropriate documentation and information has been communicated.
   d) Users needing Office 365 Administrative Privileges will complete the attached Office 365 Administrator Request form. The form should be sent to the Telecommunications and Network Manager who will coordinate training. After knowledge transfer is complete the IT Director (and Police Chief for HPD requests) will sign off on the request and rights will be granted.

2. Removing Administrator Privileges -Administrator privileges may be removed for any reason by management. Generally, privileges may be removed for the following reasons:
   a) The administrator is no longer employed by the City of Hampton
   b) The administrator moves to another position or department in the City. Administrators may re-apply for privileges if their new position requires administrator duties.
   c) The administrator's job duties change where administrator functions are not necessary to perform the job.
   d) The administrator is on leave (annual, LWOP, sick, disability, etc.) for more than 30 days. Administrator privileges will be reinstated after the employee returns to work assuming they have the same position and duties. The 30 day period can be extended with approval of the IT Director and the Police Chief for HPD employees.
   e) Administrators on temporary assignment (generally 30 days or longer) that does not require administrator functions during that time. Administrator privileges will be reinstated after the assignment period.
   f) The administrator has been found to have violated any City IT Security policy or procedure or has not reported a known violation by another administrator.
   g) Any other act, utterance, failure to act, or activity that would deem the administrator to be a security risk or unable to perform the administrator function.

3. All changes will be documented.
   a) User Requested Changes - Administrators will document all user requested changes in the IT360 ticket system. Documentation should include the request date, the nature of the request, the user e-mail & contact information and other pertinent information. Documentation will be completed within 3 business days of the request completion.
   b) New User Accounts - Administrators will document all requests for new accounts in the IT360 ticket system. Documentation should include the request date, the nature of the request, the user network account & contact information and other pertinent information. New user accounts will be documented in the IT360 system 3 days prior to implementation to allow for the management of O360 licenses across the City.
   c) Other Changes - Other changes will also require documentation that should occur prior to the change being made. If there is an impact to users or other administrators they will be notified prior to the change. The change will include the date of the change, nature of the change and impact of the change. Changes that impact all City users or general system features or functionality will be approved by the IT Director.
   d) Emergency Changes –In rare occasions emergencies arise that require changes to the system or user accounts where time is not available to document the changes on the schedule identified above. Administrators will document emergency changes as soon as feasible after the change. The same information will be required for emergency changes as for all other changes.

4. Audits
   a) Audit reports of administrator logs and activities will be produced on a periodic basis to ensure compliance with procedures and be available for any security audit, FOIA and e-discovery requests.
   b) Audit reports will be archived by the IT Department for a period of 3 years as per the Library of Virginia Records Retention County & Municipal Government Schedule No. 33 Series No. 000161.
   c) Audits of specific administrator changes can be viewed at any time by the IT Director or by other department heads, the City Manager or Assistant City Managers upon request.
   d) Audit reports can be shared with department heads or their designee on a per request basis or for any investigation, litigation or FOIA requests.

Additional Documents/ Forms

Please refer to the supplement “Office 365 Administrator Rights Request Form”