Title	**Microsoft Windows and Security Updates**
Type	Standard
Related Policy	Information Technology Protection
Category	Security
Status	Approved
Approved	01/09/2013
Revised	12/24/2012
To Be Reviewed	06/18/2017
Scope	Applies to all personal computers, laptops and mobile devices that connect to the City's networks.
Standard	**Policy Definitions:** Defines the means by which critical patches will be applied to networked resources. • **Desktop Computers:** Desktop computers shall be configured so that Microsoft "Windows Update" critical updates are automatically downloaded and applied daily. • **Servers:** System Administrators will follow CABQ standards in the testing and installation of missing patches. Missing Operating and Security patches will be installed and activated by the System Administrators. Because many patches require a reboot of the system, the reboot will be scheduled as early as possible to remove the vulnerability associated with missing patch. System Administrators will follow CAB protocol prior to the reboot of system. The patches shall be installed and activated as soon as possible but within a two week period upon discovery. **Policy Provisions:** Automated updates shall be configured and pushed out via the Active Directory local Group Policies to staff desktop computers when available. DTI shall run periodic vulnerability scan to verify updates.
Rationale	Ensures that all personal computers and servers that connect to the City's networks have access to and apply current, critical Microsoft Windows updates. Limits the City's exposure to known vulnerabilities in Microsoft Windows.