Title	**Patch Management and Vulnerability**
Type	Standard
Related Policy	Information Technology Protection Policy
Category	Security
Status	Approved
Approved	08/07/2012
To Be Reviewed	08/05/2015
Scope	Applies to IT equipment on the City of Albuquerque's network.

Standard Definitions

The City of Albuquerque shall promote a secure computing environment for all staff and business partners. Computing systems (including but not limited to: desktop workstations, laptops, hand-held, personal digital assistants, servers and network devices) are an integral part of the operations of the City and as such are vital to the City's mission. Computer viruses, worms, Trojans, to name a few, constitute a major threat to the integrity and performance of the computing operations, including access to critical data and the availability of the City's network. This Patch Management and Vulnerability standard will help ensure that all vulnerable computing platforms are hardened against attack and protected by antivirus software at all times.

Standard Provisions

- Any computer or network device connected to the City network, including wireless, the Any Connect (VPN) or dial-up connections, must be protected against attack by viruses, worms and Trojans. This standard applies to all devices connected, by any means, to the City network including those owned by the City, private individuals such as staff, vendor and business partner.
- All antivirus software and Security patches shall be actively managed to ensure that the latest virus signatures and security updates are installed. It is strongly recommended that the antivirus software and security updates be configured to obtain these updates automatically.
- The City reserves the right to review any device attached to the network (public or non-public) for adequate virus protection. The City reserves the right to deny access to the network to any device found to be inadequately protected. Additionally, the City reserves the right to disable network access to any device that is insufficiently protected, or currently infected with a virus. Network access may be restored when the device has been cleaned and current antivirus software and applicable operating system and application patches have been installed.

Standard

A Patch and Vulnerability Group (PVG), this group is tasked to implement the patch and vulnerability management program. This group functions are as follows;

1. Create a System Inventory (using existing inventories).
2. Monitor for Vulnerabilities, Remediations, and Threats.
3. Prioritize Vulnerability Remediation.
4. Create an Organization-Specific Remediation Database.
5. Conduct Testing of Remediations.
6. Deploy Vulnerability Remediations.
7. Distribute Vulnerability and Remediation Information to Local Administrators.
8. Perform Automated Deployment of Patches.
9. Configure Automatic Update of Application Whenever Possible and Appropriate.
10. Verify Vulnerability Remediation Through Network and Host Vulnerability Scanning.
11. Vulnerability Remediation Training.
12. Provide Security Metrics for Patch and Vulnerability Management

The PVG will be led by the IT Security Officer. The IT Security Officer will appoint members as required. These members should have a knowledge of vulnerability and patch management, as well as system administration, anti-virus, intrusion detection, and firewall management.

The PVG will be responsible for creating procedures to achieve the functions listed above.

Rationale

The City currently have around 8000 network end points and supports around 5,000 users. Ensuring that the City's and citizens data and is safe is an important function. By following the NIST-Special Publication 800-40 will ensure that this is achieved.