IT 17.02: Server Configuration Standards

Policy Authority

BTS Administrative Rule 2.01- Security Administrative Rule
BTS Administrative Rule 2.07- Virus Prevention and Recovery

Purpose

In order to minimize the possibility of unauthorized access and/or control of City servers, certain minimum configuration standards are necessary.

Policy

City servers should be configured to the following minimum standards:

- Identify and regularly install all necessary patches and upgrades to the server's operating system and applications. Windows servers should utilize BTS's Windows Server Update Services (WSUS) for Windows updates. IT 17.03 Patch Management Standards defines the necessary intervals for patch application.
- Install and regularly update anti-virus software (utilize BTS's standard anti-virus software- McAfee and set to receive updates from the McAfee electronic Policy Orchestrator (EPO))
- Remove or disable unneeded default accounts and groups
- Set passwords in accordance with BTS's password standards in BTS Admin Rule 2.05
- Ensure each user and administrator has a unique ID in accordance with BTS Admin Rule 2.05
- Disable or remove unnecessary services and applications.
- Utilize internal Network Time Protocol (NTP), Domain Name Services (DNS) and WINS services

Additional standards for web servers include:

- Locate a web server in a Demilitarized Zone (DMZ)
- Locate a web server behind a firewall
- Ensure server sends necessary logs to central logging servers (such as Tripwire Enterprise Console and the Juniper Security Threat Response Manager).

Some critical infrastructure servers, such as domain controllers, should integrate their logs with BTS central logging servers. The Information Security Manager determines which servers are critical servers that require such monitoring.

The Information Security Manager is responsible for updating these standards to ensure the continued safety of BTS environment.

For further information on secure server configuration, please see National Institute of Standards and Technology, *Guidelines on Securing Public Web Servers,* Special Publication 800-44 Version 2.

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	3/31/09	Logan Kleier, Information Security Manager	BTS Leadership Team	3/13/09