IT 17.07: Anti-Malware Management Standards

Policy Authority

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

Purpose

Anti-malware software provides a defense mechanism to limit the City's exposure to certain threats which may damage the City's information technology systems. Effective management of these devices requires procedures on the authorized use and modification of these devices.

Scope and Responsibilities

In order to accomplish the aforementioned purpose, certain anti-malware management procedures must be established including:

- Scope
- Roles and Responsibilities

Scope
BTS provides anti-malware software to any Bureau of Technology Services managed workstations and servers.

Roles and Responsibilities
There are multiple groups within BTS that are responsible for maintaining a functional and up to date anti-malware infrastructure. These groups' roles and responsibilities are described below:

Information Security- Sets all policies related to the deployment of anti-malware software and hardware within the City's environment.

Production Services- Maintains the central anti-malware infrastructure including the policy server(s) that contains the central repository for anti-malware software and reporting. Troubleshoots server issues and remediates infected or unprotected servers. Deploys anti-malware software on BTS maintained servers and workstations. Provides regular application and operating system software patches to the policy server(s) in accordance with BTS Patch Management Standards. Provides operational guidance to Information Security on performance and policy tuning necessary to maintain an optimally configured infrastructure.

Desktop Support- Troubleshoots end user malware issues and remediates infected or unprotected workstations. As necessary, maintains distributed anti-malware infrastructure in partnership with Production Services. Provides operational guidance to Information Security on performance and policy tuning necessary to maintain an optimally configured infrastructure.

Support Systems- Maintains an up to date installation package for deployment on new workstations. Coordinates testing of software upgrades on BTS maintained workstations. The City's anti-malware software includes updates to the management agent, signature updates and engine updates.

Police IT- Maintains a central anti-malware infrastructure in support of Portland

Police Bureau IT infrastructure; including testing and deployment of anti-malware software on servers and workstations within this environment. Coordinates policy changes in this infrastructure with Information Security.

All parties are responsible for maintaining a working knowledge of the City's anti-malware software and hardware and should periodically receive formal training on the operation and capabilities of this infrastructure.

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	12/15/09	Logan Kleier, Information Security Manager	Bureau Leadership Team	12/15/09