BTS-2.07 - Malware Prevention & Recovery

MALWARE PREVENTION & RECOVERY
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.07

Purpose
Malicious software (malware) can be transferred over the Internet, by portable storage device, local area networks, email and other means. Malware can quickly spread to destroy or corrupt data. Overall service to internal and external customers of the City can be drastically affected by becoming infected by malware. Diligence demands stringent efforts to safeguard City owned and managed systems and data from malware.

This policy applies to all computers, systems, portable storage devices and network devices connected to City networks to ensure effective malware prevention, detection and eradication.

Administrative Rule
All systems connected to City owned networks must have BTS approved malware protection software, operating systems, operating system patches, applications and application patches installed, operational and up-to-date at all times.

Responsibilities

Bureau of Technology Services Responsibilities
- Procurement, installation, maintenance and monitoring of malware prevention software, operating systems, operating system patches and equipment in accordance with City standards and to institute measures to ensure that malware prevention methods remain current.
- Maintain procedures for proactively preparing for and reactively responding to outbreaks to minimize City impact and restore full operations as quickly and securely as possible.
- Isolate or quarantine systems and/or network segments to prevent and/or contain malware outbreaks, minimize impact and to effectively restore services in a timely manner.
- Implement technologies and establish policies and procedures that limit the methods of connections for networked devices (portable computing devices, etc.) that do not meet minimum security standards and specifications.
- For systems considered to be not commonly affected by malicious software, the Information Security Office shall perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

Bureau & User Responsibilities
- Comply fully with all malware security actions, warning and notices as issued by the Bureau of Technology Services.
- Do not open email file attachments from an unknown source or from known sources when the messages appear suspicious in nature.
- Report all suspected malware incidents or missing/malfunctioning malware protection software immediately to the BTS Helpdesk.
- Attach all City virtual or physical computing systems to the City network at least weekly to ensure current malware signature updates.
- As noted in BHR Administrative Rule Section 4.08, do not download and/or install software on City devices without prior BTS approval.
- Do not connect any non-BTS supported device to the City network without prior BTS validation and authorization.
- Do not circumvent, disable or remove any BTS malware protection software, systems or patches.
- Fund replacement of bureau-owned aging equipment (servers/workstations) when it no longer supports BTS standard operating systems versions, malware protection software or patches (malware or application) required to maintain malware security on such equipment.

Supporting Practices

With assistance from the Bureau of Technology Services, Bureau and Office managers shall ensure that employees are provided with information on safe practices for malware protection and that these safe practices are observed at all times.

As per BHR Administrative Rules Section 4.08, City employees are reminded of the expectation to observe safe practices regarding the use of devices to minimize malware risks.

History

Originally published as PPD number ARC-BIT-2.03, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-2.07.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.
Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.
This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.
This rule was reviewed as part of a periodic review and remains unchanged. April 30, 2018.