BTS-2.07 - Virus Prevention & Recovery

VIRUS PREVENTION & RECOVERY

Administrative Rule Adopted by Council
ARC-BTS-2.07

Purpose

Computer viruses can be transferred by disk, local and wide area networks, connections to the internet, email and by a variety of other means. Computer viruses can quickly spread to destroy or corrupt data. Overall service to internal and external customers of Bureaus and Offices can be drastically affected by contracting a computer virus. Diligence demands stringent efforts to safeguard City owned and managed systems and data from viruses.

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

Administrative Rule

All systems connected to City owned networks must have BTS approved virus 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 virus prevention software, operating systems, operating system patches and equipment in accordance with City standards and to institute measures to ensure that virus prevention methods remain current.
- Maintain procedures for proactively preparing for and reactively responding to, virus 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 virus outbreaks, minimize impact and to effectively restore services in a timely manner.
- Implement technologies as funding is available and establish policies and procedures that limit the methods of connections for networked devices (laptops, PDA's, etc) that do not meet minimum security standards and specifications.

Bureau & User Responsibilities

- Comply fully with all virus security actions, warning and notices as issued by the Bureau of Technology Services.
- Do not open email file attachments from an unknown or untrustworthy source or from known sources when the messages appear suspicious in nature.
- Report all suspected virus incidents or missing/malfunctioning virus protection software immediately to the Bureau of Technology Services Helpdesk.
- Logoff all personal computing systems from the City network at the end of each normally scheduled work day so as to ensure current virus signature updates.
- As noted in BHR Administrative Rule Section 4.08, do not download and/or install software on City computers without prior approval from BTS.
- Do not connect any non-BTS supported computer or network device to the City network without prior validation and authorization from BTS.
- Do not circumvent, disable or remove any BTS virus protection software, systems or patches.
- Fund replacement of bureau owned aging equipment (servers/workstations) when it no longer supports BTS standard operating systems versions, virus protection software or patches (virus or application) required to maintain adequate virus 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 virus 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 computers to minimize the risks of viruses.

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.