BTS-2.07 - Malware Prevention & Recovery

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Policy category: Information Security

Policy number: BTS-2.07

MALWARE PREVENTION & RECOVERY

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority

ARB-BTS-2.07

Search Code, Charter, Policy

Keywords

Search

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 Chief Technology Officer November 15, 2013.

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.

Revised by Chief Technology Officer October 10, 2018.

This rule was reviewed as part of a periodic review. September 1, 2021.

Related documents

BTS-2.07 Malware Prevention & Recovery Administrative Rule 109.4 KB

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 and valuable City information. Essential services for internal and external customers of City Technology Resources can be drastically affected by malware infections. To maintain high availability of City Technology Resources r continuous efforts must be applied to prevent malware infections.

This policy applies to all devices connected to City networks and hosted (SaaS) City Technology Resources to ensure effective malware prevention, detection and eradication.

Devices may be City-managed or personal, smartphones, computers, portable storage devices, and network devices.

Any device or network connection that does not meet City security standards will disconnected and prevented from accessing City Technology Resources.

Administrative Rule
All systems, devices, City-owned or personal, or Hosted Technology Recourses connected to City-owned and managed networks must have Bureau of Technology Services (BTS) approved malware protection software, operating systems, operating system patches, applications and application patches installed, operational and up to date.

Responsibilities

Bureau of Technology Services Responsibilities
1. 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.
2. Maintain procedures for proactively preparing for and reactively responding to security incidents to minimize City impact and restore full operations as quickly and securely as possible.
3. Isolate or quarantine systems and/or network segments and Internet-based services to prevent and/or contain malware outbreaks, minimize impact and to effectively restore services in a timely manner.

4. Implement technologies and establish policies and procedures that limit the methods of connections for connected devices (smartphones, computers, tablets, etc.) that do not meet City minimum security standards and specifications.
5. For systems considered to be not commonly affected by malicious software, the Information Security Office must perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue to not require anti-virus software.

Bureau & Authorized User Responsibilities

1. Comply fully with all malware security actions, warning and notices as issued by BTS.
2. Do not open email file attachments from an unknown source or from known sources when the messages appear suspicious in nature.
3. Immediately report all suspected malware incidents or missing/malfunctioning malware protection software to the BTS Helpdesk.
4. Attach all City virtual or physical network and computing systems to the City network at least weekly to ensure current device security and malware signature updates.
5. As noted in BHR Administrative Rule 4.08, Information Technologies, do not download and/or install any software (including free or trial software) on City devices without prior BTS approval.
6. Do not connect any non-BTS supported device to the City network without prior BTS validation and authorization.7. Do not circumvent, disable or remove any BTS malware protection software, systems or patches.
7. Do not circumvent, disable or remove any BTS malware protection software, systems or patches.
8. 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.

Use of personal and non-City devices to access City Technology Resources

1. Personal devices may connect to cloud hosted City Technology Resources, such as Microsoft Office 365, when following all applicable City of Portland BTS, Bureau of Human Resources and Auditor’s Office Administrative Rules.
2. Personal devices are not allowed to connect directly to the City network. Devices not secured and maintained by the City to BTS security standards present unpredictable risks.

Supporting Practices

With assistance from the Bureau of Technology Services, bureau and office managers must ensure that Authorized Users are provided with information on safe practices for malware protection and that these safe practices are always observed.

As per BHR Administrative Rule, 4.08, Information Technologies, City Authorized Users are reminded of the expectation to observe safe practices regarding the use of devices to minimize malware risks.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

1) BTS Technology Definitions – https://www.portlandoregon.gov/citycode/article/114449
2) (BTS) Technology Standards Directory (and Acronyms) -- https://www.portlandoregon.gov/bts/article/44978
3) City of Portland Information Security Standards

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.
This rule was reviewed and revised as part of a periodic review. September 2, 2019.
This rule was reviewed and revised as part of a periodic review. June 30, 2020.
This rule was reviewed as part of a periodic review. September 1, 2021.