IT 17.08: Operational Security Procedures

Policy Authority

BTS Administrative Rule 2.01- Security Administrative Rule
BTS Administrative Rule 2.16- Firewall Security and Management
BTS Administrative Rule 2.07- Virus Prevention and Recovery
BTS Administrative Rule 2.08- Incident Reporting and Response
BTS Administrative Rule 2.17- Payment Card Security Standards

Purpose

In order to maintain an effective information security program and compliance with various security regulations such as Payment Card Industry- Data Security Standard (PCI-DSS), the Bureau of Technology Services (BTS) should maintain a set of operational security procedures that provide guidance to BTS staff on security duties that are to be performed on a periodic basis. These procedures ensure that basic maintenance is specified and measured which in turn creates transparency and accountability into BTS' information security measures used to protect the City against internal and external threats to its information assets.

Procedure

In order to accomplish the aforementioned BTS Administrative Rules, certain periodic security procedures must be established. The implementation details of these procedures are defined below. These procedures provide for the following:

- Objective- desired outcome
- Means- specific tasks that are used to accomplish the objective
- Responsible party- the BTS division responsible for accomplishing the task
- Time Interval- the regularity with which the task is repeated

Objective- Limit unauthorized wireless access

Means	Responsible Party	Time Interval
Check for the presence of unauthorized wireless access points	Information Security	Daily
Categorize newly discovered wireless access points	Information Security	Weekly

Objective- Retain an evidentiary trail of physical security

Means	Responsible Party	Time Interval
Check video surveillance digital video recorder (DVR) for operational status and video storage.	Production Services	Weekly
Check data center logs for usage and accuracy	Production Services	Weekly
Check BTS lobby logs for usage and accuracy	Administrative Team	Weekly

Objective- Minimize the presence of unpatched workstations and servers in the city's environment

Means	Responsible Party	Time Interval
Deploy and verify security patches are applied to servers as specified by patching schedule.	Server Support	Monthly
Deploy and verify Microsoft security patches are applied to workstations.	Support Systems	Monthly
Deploy and verify Acrobat Reader, Flash, and Java security patches are applied to workstations	Support Systems	Semiannually

Objective- Minimize the presence of malware in the City's information assets.

Means	Responsible Party	Time Interval
Check for the presence of up to date DATs (signature files) within repositories.	Information Security	Daily
Check for repository replication	Information Security	Daily
Check for agent to server communication on servers.	Information Security	Weekly
Remediate agent to server communication failures (on servers)	Information Security Server Support	Daily
Check and report uncleaned malware detections on servers and workstations	Information Security	Weekly
Remediate uncleaned malware detections on servers.	Server Support	Weekly
Remediate out-of-date anti-malware (scanner or engine) software on workstations.	Desktop Support	Quarterly
Remediate out-of-date anti-malware software (scanner or engine) on servers.	Information Security	Weekly

Objective- Limit password attacks

Means	Responsible Party	Time Interval
Change all non-PCI scope administrative passwords	Server Support	Semiannually
Change all PCI scope administrative and service account passwords	Server Support	Every 90 Days

Objective- Discovery and log significant security threats and events

Means	Responsible Party	Time Interval
Confirm PCI-DSS scope devices are actively logging to security incident log platform	Information Security	Monthly
Perform internal and external network vulnerability scans.	Information Security	Quarterly
Resolve annual network vulnerability scan issues	Network Engineering	Quarterly
Perform internal and external penetration testing on PCI scope systems	Information Security	Quarterly
Resolve penetration testing issues on PCI scope systems	Web Services	Quarterly

Objective- Maintain up to date security software

Means	Responsible Party	Time Interval
Check for new versions of software/firmware on firewalls, firewall management console, SSL VPN, two-factor authentication platform, and secure web gateway	Information Security	Monthly
Check for new versions of log collection tools such as SNARE and epilog	Information Security	Monthly
Check for new versions of anti-malware software for clients and servers	Information Security	Daily
Install new versions of anti-malware software	Information Security	As Needed
Check for the presence of up to date Digital Vaccines for wireline Intrusion Prevention Devices (IPS)	Information Security	Weekly

Revision History				
Version	**Effective Date**	**Authored By (Name, Dept)**	**Approved By (Name, Dept)**	**Date**
1.0	6/21/10	Logan Kleier, Information Security	Bureau Leadership Team	6/15/10