

Goal #5 – Protect City Information and Data

Obj. 1 - Implement citywide Information Security Program

Obj. 2 - Ensure information systems that host customers' applications and data are secure

Obj. 3 - Provide security systems and services



The City must adhere to federal and state privacy and data security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI). Executive Order 1-48, policy on IT Security, mandates that the City develop and maintain a citywide information security program. This is being accomplished by utilizing the National Institute of Standards and Technology (NIST) Cyber Security Framework as a guide in establishing and implementing information security policies, procedures and handbooks to facilitate appropriate protection and accountability of information.

The Chief Information Security Officer (CISO) has developed an *Enterprise IT Security Roadmap* that, when fully implemented, will provide the needed protection of the City's business and privacy information. A number of key security initiatives were started in Fiscal Year 2015 and are planned for completion in Fiscal Year 2016. This roadmap includes an automated threat removal platform that will be implemented citywide and will significantly reduce the inherent security risk (from the use of IT resources) to City businesses.

The threat removal platform provides capabilities that will enable the automated implementation of critical security controls that are essential to securing information systems that host customer applications and data.

Key security initiatives that have commenced in Fiscal Year 2015 and will continue through Fiscal Year 2016 include:

1. Malware Defenses
2. Automate Threat Removal
3. Continuous Vulnerability Assessment and Remediation
4. Security Risk Intelligence
5. Data Loss Prevention
6. Mobile Device Management (MDM)
7. Cyber Security Awareness Training
8. Cyber Security and Disaster Recovery Planning

