HAMPTON VA

No. IT– 021	Policy Name: IT Security Policy
Effective Date: 7-1-2011 Last Revised Date: 7-4-2014	Citywide Policy _ IT Policy X IT Procedure _
Approved By: IT Director	

IT Security Policy

1. INFORMATION TECHNOLOGY (IT) SECURITY POLICY STATEMENT

1.1 Background

The City of Hampton (COH) relies heavily on the application of information technology (IT) for the effective delivery of government services. Rapid and continuing technical advances have increased the dependence of COH departments on IT. COH data, software, hardware, and tele-communications are recognized by departments as important resources and must be protected through an IT security program.

The IT security program shall be built on the concept of public trust. The City's IT security pro-gram provides a sustainable and consistent approach to IT security that can be replicated across networks, applications, and transactions.

1.2 Guiding Principles

The following principles guide the development and implementation of the COH IT Security Pro-gram.

COH Data is:

A critical asset that shall be protected;

Restricted to authorized personnel for official use.

IT Security must be:

A cornerstone of maintaining public trust;

Managed to address both business and technology requirements;

Risk based and cost effective;

Aligned with COH priorities, industry-prudent practices, and government requirements;

The responsibility of all users of COH IT systems and data

The Security Triad – The City's IT Security Policy follows the concepts of the IT security triad. The classic security triad is based on three tenants: confidentiality, integrity, and availability. Each of these tenants offer some level of protection, but the combination of these tenants allows the city to keep data private where appropriate, insure data has not been corrupted, and keep the systems up and running.

Confidentiality – The concept of protecting confidentiality relies on defining and enforcing appropriate access levels of information.

Integrity – This is the concept of protecting data from modification or deletion by unauthorized individuals and ensuring that authorized individuals have safeguards in place to reduce

Statement of Policy

It remains the policy of the COH that the IT Department and each department head is responsible for the security of the department's data and for taking appropriate steps to secure IT systems and data through the implementation and enforcement of IT policies and procedures.

Departments that have access to or handle data that is subject to legislations, regulations and/or industry standards such as Health Insurance Portability and Accountability Act of 1996 (HIPPA), Internal Revenue Service (IRS) 1075, the Privacy Act of 1974, the Payment Card Industry (PCI) standard, the Rehabilitation Act of 1973, the Federal National Security Standards, Commonwealth of Virginia security policies etc., shall inform the IT department if appropriate and shall include the respective requirements within the department's policies and procedures. IT will establish procedures as appropriate for systems requiring specific legal or regulation requirements as needed by departments.

The function of this policy is to protect COH IT systems and data from credible threats, whether internal or external, deliberate or accidental. It is the policy of COH to use all reasonable IT security control measures to:

Protect COH data against unauthorized access and use;

Maintain the integrity of the data

Ensure COH data residing on any IT system is available when needed

Comply with appropriate local, federal, state and other legislative, regulatory and industry requirements

The remainder of this policy document is divided to subcategories for ease of use.

Section 2. addresses key IT Security Roles and Responsibilities

Section 3. addresses the IT Security Program and Standards

Section 4. addresses IT Security Compliance

Section 5. address the IT Audit Process

KEY IT SECURITY ROLES & RESPONSIBILITIES

This section defines the key IT security roles and responsibilities included in Hampton's IT Security Program. It is important that everyone in the organization participate and promote IT security in order to have a successful program and protect IT assets and data.

IT Governance Board

- Approves IT Security Policies
- Directs the IT Department to develop appropriate policies and standards where necessary
- Recommends IT Security Audits and Risk Assessments for the IT Department and other City Departments responsible for IT infrastructure and applications
- Reviews Risk Assessments, disaster recovery plans and tests, and IT Security Audit reports and approving corrective action plans.
- Assists the IT Director in the promulgation and enforcement of IT Security Policies

IT Director & Staff

- Develops policies, procedures and standards for assessing the security risks, determining the appropriate security measures and performing security audits of City IT assets.
- Administers and maintains the COH IT Security Program
- Provides solutions, guidance and expertise on IT security
- Maintains awareness of the security status of sensitive systems
- Prepares, disseminates and maintains IT security policies, standards, guidelines and procedures as appropriate
- Collects data relative to the state of IT security in the COH and communicating as needed
- Provides consultation on balancing an effective IT security program with business needs
- Develops and tests a disaster recovery plan for IT managed resources
- Reviews and approves the COH IT portion of the Emergency Operations Plan and Continuity of Operations Plan, to include the IT Disaster Recovery Plans for all City Departments operating IT infrastructure
- Develops and maintains an IT security awareness program for COH employees
- Coordinates and provides IT security information to the departments

Department Heads and Department Managers

- Promotes IT security safeguards and assists in the enforcement of this policy and the Acceptable Use Policy
- Supports and facilitates the communications process between the IT department and departmental users
- Promotes IT security awareness programs and enables employees to carry out their responsibilities for securing IT systems and data
- Escalates problems, requirements, and matters related to IT security to the highest level necessary for resolution
- For departments that maintain their own IT infrastructure these additional duties apply

Prepares, disseminates and maintains IT security policies, standards, guidelines and procedures for their departmental systems

Develops and tests annually an IT Disaster Recovery plan for critical systems under their control

Follows all IT security policies and standards in this document as they pertain to systems under their control

Manages risk and develops any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.

Designates a system administrator for the system

Adheres to other portions of this policy that addresses departments owning and maintaining their own systems and infrastructure

Data Owner – The Data Owner is the department manager responsible for policy and practice decisions regarding data. This is generally the department that has responsibility for the business process supported by an IT system. The data owner is responsible for the following:

Evaluates and classifies sensitivity of the data

Defines protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements and business needs

Communicates data protection requirements to IT or the system administrator

Defines requirements for access to the data

System Administrator – The System Administrator is an analyst, engineer, consultant or technical staff member who implements, managers and/or operates a system or systems at the direction of the IT department, system owner or data owner. The system administrator assists departmental management in the day to day administration of IT systems and implements security controls on IT systems for which the system administrator has been assigned responsibility.

IT System Users – All users of COH IT systems including employees, elected officials, volunteers and contractors are responsible for the following:

Read and comply with IT security requirements and policies

Report breaches of IT security, actual or suspected, to the IT department.

Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

Follow the IT Acceptable Use Policy and other appropriate IT policies and procedures

Participate in IT Security Awareness activities

7 **Departments Owning and Managing IT Infrastructure and Critical Systems** – The City of Hampton has several departments that own, manage and operate IT infrastructure or IT services for use by their department or other associated departments with limited or no support from the City's IT department. These department staff must develop and implement appropriate security policies and procedures that meet or exceed those described in this policy.

IT SECURITY PROGRAM COMPONENTS AND STANDARDS

The policy of the COH is to secure its IT systems using methods based on the sensitivity of the data processed and the risks to which the systems and data are subject, including the dependence of critical department business processes on the data and systems.

3.1 **Risk Management** – The IT department will conduct an IT Risk Assessment every three years. Departments that manage critical infrastructure will also conduct IT Risk Assessments every three years. The City's standard for Risk Assessments will include the following components:

a. Inventory IT Assets and Critical Systems

b. Assess Data Center Vulnerabilities

c. Confirm Disaster Recovery Plan (DRP) within the business context

d. Assign Priorities of Assets

e. Document, Track and Manage Risks

Risk Assessment reports will be presented to the IT Governance Board with recommendations from the IT Director. The IT Governance Board will provide guidance, direction and approve recommendations to reduce risks. The IT Governance Board will also assist the IT Department in identifying funding sources and obtaining funding for approved major projects to reduce IT risks.

Contingency and Disaster Recovery Planning – IT contingency planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and data that support essential business functions if an event occurs that renders the IT systems and data unavailable. IT continuity of operations includes continuity of operations planning (COOP), disaster recovery planning, and IT system back up and back up restoration. The Virginia Department of Emergency Management provides COH guidance on COOP planning. The City Emergency Operations Center manages the city's COOP plan. Disaster Recovery Planning supports Continuity of Operations Planning by defining specific policies and procedures for restoring IT systems and data that support essential business functions, on a schedule that supports City mission requirements. IT system back up and restoration

defines plans and restoration schedules that meet department mission requirements for the back up and restoration of data. The city's standards for DRP, back up and restoration are as follows:

a. Critical data is incrementally backed up and a copy is stored in an alternative Hampton site

b. A full back up of critical data is completed weekly and a back up copy is stored outside of Hampton's flood zone

c. A disaster recovery plan for all critical systems should be in place

d. The DRP will rely on and support the COOP plan as produced by the City's Emergency Operations Center.

Ee. Testing of the disaster recovery plan will be on a component basis and will oc- cur annually or as necessary.

f. Tests of back up restorations will take place where it is feasible and does not put production systems at risk. The tests will occur annually unless there are major infrastructure or configuration changes that warrant additional testing.

3.3 **IT System Security** – The purpose of IT systems security is to define the standards necessary to provide adequate and effective protection for City systems in the area of system hardening, system interoperability security, malicious code protection, logical access controls, data protection and network threats. All system security is managed solely by the Department of Information Technology and by designated department administrators. Departments managing their own IT systems are subject to the IT system security standards. The Acceptable Use policy identifies additional standards for end users.

IT system security standards are as follows:

a. All servers and desktops shall have the currently supported standard Antivirus software installed.

b. All servers will be patched on a regular basis

c. Support contracts for critical assets should be maintained and provide for the level of service necessary to support the business criticality of the system

d. UPS and redundant power should be installed on all systems that are deemed to support critical systems

e. Password procedures shall be implemented and the password strength policy should be based on the sensitivity of the data being protected. Strong passwords and forced password changes on at least a 90 day basis should be used for systems with sensitive data. Default passwords shall never be used. Passwords shall not to be shared for any reason.

f. User accounts shall be unique to the individual. Shared accounts should only be used on an exception basis as approved by the Information Technology Director.

. Users will not have administrative rights on PCs. Users needing this capability must contact the Department of Information Technology with a justification and must be adequately trained to ensure proper security controls.

h. Users dialing in with PC software are to notify the Department of Information Technology and register their connection to prevent unauthorized access.

i. The City has an established process to identify and evaluate threats and assign appropriate action based on risks.

j. Firewalls must be implemented where appropriate and have security logging turned on.

k. The City will deploy a multi-layered protection at the Internet gateway, the network server and desktop levels to prevent the introduction of malicious code into the system.

l. System and/or data access must be explicitly granted to personnel by the system or data owner. Departments will put procedures in place to explicitly grant access. A periodic review of access to systems by individual users of the data will be conducted by IT and the Department Data Owner. Default access will not be allowed.

m. Only approved members of the IT Engineering staff or other department staff approved by the IT Director will maintain full administrative rights on City servers regardless of location or purpose. Other individuals within IT may have admin rights to specific servers on an as needed basis. Departments that manage their own servers will limit server admin rights to only specific individuals with a high level of technical and security knowledge. The IT Director will provide guidance and recommendations to departments on the skills and knowledge needed by server administrators. The list of server administrative staff in other departments will be maintained by the IT department engineering staff.

3.4 **Facilities Security** – Physical security safeguards provide a first line of defense for information resources against physical damage, physical theft, unauthorized disclosure of information, loss of control over system integrity and interruption to computer services. Standards for facilities are as follows:

a. Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

b. Access to critical computing hardware must be controlled by rules of least privilege.

c. System configurations (Hardware, wiring, displays, and networks) or critical systems must be documented. Installations and changes to those physical configurations must be governed by a formal change management process.

33.5 **Personnel Security** – Personnel security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf of the City. Security standards below apply to personnel:

a. Separation of duties and least privilege principles shall apply to all critical systems and to other systems where appropriate. In cases where there are not the personnel or processes available to support this, additional monitoring and logging will be applied by IT, the system administrator and/or the data owner. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. Least privilege refers to granting a user only those accesses that they need to perform their official duties.

B

b. Background screening for all employees will take place as per the Human Resources policy. The City IT department will assume that personnel screened by Human Resources and approved for employment in positions requiring system access will not require additional screenings in IT. Departments may perform their own additional screenings as desired. An additional procedure for approving IT contractors will be in place.

c. System and/or data access must be explicitly granted to personnel by the system or data owner and not allowed by default. IT and department data owners will have procedures and controls in place to track system access.

m. Access must be terminated concurrent with when the requirement for access no longer exists, i.e., termination, transfer, promotion, retirement, or change of duties. Departments shall notify the IT department as soon as these changes take place to ensure compliance. IT and departmental data owners will have procedures in place to ensure the timely and accurate termination of access.

3.6 **Incident Management –** Incident handling refers to those practices, technologies and/or services used to respond to suspected or known breaches of security safeguards. Information technology security incidents refer to deliberate, malicious acts which may be technical (e.g. creation of viruses, system hacking) or non-technical (e.g. theft, property abuse, service disruption). The standards below apply to City security incident management.

- The city will have in place an incident process which identifies the responsibilities and actions to be taken in response to incidents.
- Information on how and when users report incidents will be periodically sent to users to reinforce use of the process.

IT Asset Management – IT asset management concerns protection of the components that comprise COH IT systems by managing them in a planned, organized and secure fashion. Standards for asset management apply to the City's IT department as well as departments

that own and/or manage infrastructure, software and services supporting City functions. The IT standards for the City Asset management are as follows:

- Change control processes will be in place and documented
- Software licenses will be managed and be in compliance with contractual and legal obligations and terms. Illegal and unlicensed (unless in the public domain) software will not be allowed in the City's IT environment. Departments downloading software from the Internet will be responsible to ensure that legal terms are met and adhered to. Departments will notify IT of new software downloads and purchases.
- IT will maintain an inventory of software purchased through the IT department for end user and enterprise systems.
- Physical IT assets will be tracked and a record of the asset will be maintained
- IT and departments managing infrastructure will maintain up to date configurations of servers, software, networks and other critical system components.

The IT Department will approve all servers, software, configurations and network access of systems that access and/or utilize COH network resources.

Application Security - Encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, access threats, development, deployment, upgrade, or maintenance of the application. The IT standards for the City application security are as follows:

- IT or the department maintaining the application will maintain copies of software applications contracts, maintenance agreements, software changes, upgrades, configurations, source code, up to date vendor contacts and escalations, and other critical information to the maintenance and operation of the application.
- A list of major departmental applications will be maintained by IT with appropriate contact information.
- Application system administrators will be identified and properly trained on the operation of the system and the processes for changes and updates. IT will maintain a list of application system administrators
- Departments will develop secure processes for granting application access to only appropriate users.

COMPLIANCE – Compliance activities are performed and managed to ensure that security measures continue to remain in place and are adhered to by all individuals.

Monitoring Activities – Monitoring is used to improve IT security, to assess appropriate use of COH IT resources and to protect resources from attack. Use of COH IT resources constitutes permission to monitor that use. There is no expectation of privacy when utilizing IT COH resources. The City of Hampton reserves the right to:

- Review the data contained in or traversing COH IT resources
- Review the activities on COH IT resources
- Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the IT Director.
- For investigative purposes the IT Director has the responsibility to authorize monitoring or scanning activities for network traffic, application and data access, user commands; email and Internet usage, and message data content for the COH IT systems and data.
- The use of keystroke logging is prohibited, except when required for security investigations, law enforcement investigations and approved in writing by the department head.
- The COH will monitor infrastructure in order to maintain a security environment. The standards for infrastructure monitoring are as follows:
    - IT will monitor systems for secure baselines and policy compliance.
    - Infrastructure monitoring may include penetration testing, user audit trails, logging, change management approvals, intrusion detection, user behavior anomalies, repeated failed log-in attempts, etc.
- IT may at anytime install new tools to better monitor COH services.

- Installing or using unauthorized monitoring devices is prohibited. Departments managing their own servers or infrastructure shall notify IT of the monitoring tools being utilized.

Internet Privacy – The Code of Virginia requires every public body in the Commonwealth that has an Internet website to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the requirements of the code. The COH shall have an Internet policy posted on the website where it is easily accessed by citizens.

AUDITING

Security audits are periodically conducted to check the effectiveness of all the components of the IT security program. These audits can be for just IT or as part of a specific departmental audit. The IT Department will participate in and be the point of contact for all City audits relating to IT security. In addition, the IT Governance Board can direct Security audits to be performed on any and all IT systems in the COH. IT Security audit findings will be reported to the IT Governance Board and any other appropriate departments. A corrective action plan will be developed by the IT department and submitted to the IT Governance Board and any appropriate department heads and managers.

Attachment A

IT Security Responsibilities for Departments Owning and Managing IT Infrastructure and Critical Systems

The City of Hampton has several business areas that own and manage major and critical IT systems and services that support citizens and the City's business processes. These departments include but are not limited to:

1. Hampton Police
2. Library
3. Public Works
4. Conventions and Visitor's Bureau
5. Social Services
6. Coliseum
7. Economic Development
8. Parks & Recreation
9. Health Department

Others as appropriate

Departments with their own systems and services must develop and implement appropriate security policies and procedures in keeping with the City's security policy and in line with their business risk.

Department IT Manager & Staff Responsibilities

Develops policies, procedures and standards for assessing the security risks, determining the appropriate security measures and performing security audits of departmental IT assets in consultation with the City's IT Department.

Administers and maintains the department's IT Security Program

Provides solutions, guidance and expertise on IT security to departmental management and directors

Maintains awareness of the security status of sensitive systems

Prepares, disseminates and maintains IT security policies, standards, guidelines and procedures as appropriate within their department. Provides copies and updates of security policies, standards and guidelines with the City's IT Depart-

ent.

Collects data relative to the state of IT security in the department and communicating risks to departmental management and the City's IT Department.

Coordinates and provides IT security information to the department users

Develops and tests annually an IT Disaster Recovery plan for critical systems under their control and reports findings to the City's IT Director.

Follows all IT security policies and standards in this document as they pertain to systems under their control.

Manages risk and develops any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.

Designates a system administrator for the system(s)

Promotes IT security safeguards and assists in the enforcement of this policy and the Acceptable Use Policy

Supports and facilitates the communications process between the IT department and departmental users

Promotes IT security awareness programs and enables employees to carry out their responsibilities for securing IT systems and data

Data Owner – The data owner is responsible for the same tasks as specified in Section 2.4 of this policy.

System Administrator – The system administrator is responsible for the same task as specified in Section 2.5 of this policy

IT System Users – the system users have the same level of responsibility as specified in Section 2.6 of this policy.

IT SECURITY PROGRAM COMPONENTS AND STANDARDS

Departments managing their own IT systems and infrastructure will put in place a security pro-gram with the following components and standards. The program will be developed and implemented in consultation with the City's IT Department.

Risk Management – The department will conduct an IT Risk Assessment every three years. Standard for Risk Assessments will include the following components:

a. Inventory IT Assets and Critical Systems

b. Assess Data Center Vulnerabilities

c. Confirm Disaster Recovery Plan (DRP) within the business context

d. Assign Priorities of Assets

e. Document, Track and Manage Risks

Risk Assessment reports will be presented to the City's IT Director who in turn will review the findings with the IT Governance Board with recommendations from the IT Director. The IT Governance Board will provide guidance, direction and approve recommendations to reduce risks.

Contingency and Disaster Recovery Planning –Departments managing their own systems will adhere to the city's standards for DRP, back up and restoration as follows:

a. Critical data is incrementally backed up daily and a copy is stored in off site in a secure location accessible by the Department's management and the City's IT staff.

b. A full back up of critical data is completed weekly and a back up copy is stored outside of Hampton's flood zone in a secure location accessible by the Department's management and the City's IT staff.

c. A disaster recovery plan for all critical systems should be in place

e. Testing of the disaster recovery plan will be on a component basis and will occur annually or as necessary.

f. Tests of back up restorations will take place where it is feasible and does not put production systems at risk.

IT System Security – All system security is managed by the department's designated department IT managers and administrators in consultation with the City's IT Department. Departments will inform IT of all designated department administrators and their contact information. Departments managing their own IT systems are subject to the following IT system security standards and the City's Acceptable Use policy.

IT system security standards are as follows:

a. All servers and desktops shall have the currently supported standard Antivirus software installed.

b. All servers will be patched on a regular basis

c. Support contracts for critical assets should be maintained and provide for the level of service necessary to support the business criticality of the system

d. UPS and redundant power should be installed on all systems that are deemed to support critical systems

e. Password procedures shall be implemented and the password strength policy should be based on the sensitivity of the data being protected. Strong pass-words and forced password changes on at least a 90 day basis should be used for systems with sensitive data. Default passwords shall never be used. Pass-words shall not to be shared for any reason.

f. User accounts shall be unique to the individual. Shared accounts should only

e used on an exception basis as approved by the City's Information Technology Director.

g. Users will not have administrative rights on PCs. Users needing this capability must contact the Department's IT Manager with a justification and must be adequately trained to ensure proper security controls. Department managers will also notify the City's IT department of users with administrative rights on PCs.

h. Users dialing in with PC software are to notify their Department's IT Manager and the City's Department of Information Technology and register their connection to prevent unauthorized access.

i. The department has an established process to identify and evaluate threats and assign appropriate action based on risks.

j. Firewalls must be implemented where appropriate and have security logging turned on.

k. Departments will deploy a multi-layered protection at the Internet gateway, the network server and desktop levels to prevent the introduction of malicious code into the system.

l. System and/or data access must be explicitly granted to personnel by the sys-tem or data owner. Departments will put procedures in place to explicitly grant access. A periodic review of access to systems by individual users of the data will be conducted by IT, the Department's IT Manager and the Department Data Owner. Default access will not be allowed.

m. Departments that manage their own servers will limit server admin rights to only specific individuals with a high level of technical and security knowledge. The IT Director will provide guidance and recommendations to departments on the skills and knowledge needed by server administrators. The list of server administrative staff in other departments will be maintained by the IT department engineering staff.

Facilities Security –Standards for facilities are as follows:

a. Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

b. Access to critical computing hardware must be controlled by rules of least privilege.

c. System configurations (Hardware, wiring, displays, and networks) or critical systems must be documented. Installations and changes to those physical con-figurations must be governed by a formal change management process.

Personnel Security – Security standards below apply to personnel:

Separation of duties and least privilege principles shall apply to all critical systems and

o other systems where appropriate. In cases where there are not the personnel or processes available to support this, additional monitoring and logging will be ap-plied. Separation of duties refers to dividing roles and responsibilities so that a sin-gle individual cannot subvert a critical process. Least privilege refers to granting a user only those accesses that they need to perform their official duties.

Background screening for all employees will take place as per the Human Resources policy. Departments may perform their own additional screenings as desired. An additional procedure for approving IT contractors will be in place.

System and/or data access must be explicitly granted to personnel by the system or data owner and not allowed by de-fault. Department data owners will have procedures and controls in place to track system access.

Access must be terminated concurrent with when the requirement for access no longer exists, i.e., termination, transfer, promotion, retirement, or change of duties. Departments will have procedures in place to ensure the timely and accurate termination of access.

Incident Management – The standards below apply to security incident management.

The department will have in place an incident process which identifies the responsibilities and actions to be taken in response to incidents. Security incidents that have the potential to disrupt City services will also be communicated to the City's IT department.

Information on how and when users report incidents will be periodically sent to users to reinforce use of the process.

IT Asset Management The IT standards for the asset management are as follows:

Change control processes will be in place and documented

Software licenses will be managed and be in compliance with contractual and legal obligations and terms. Illegal and unlicensed (unless in the public domain) software will not be allowed.

Departments downloading software from the Internet will be responsible to ensure that legal terms are met and adhered to. Department IT Managers will maintain a list of new software downloads and purchases.

Physical IT assets will be tracked and a record of the asset will be maintained

Departments managing infrastructure will maintain up to date configurations of servers, software, networks and other critical system components.

The IT Department will approve all servers, software, configurations and network access of systems that access and/or utilize COH network resources.

Application Security - The IT standards for the City application security are as follows:

Departments will maintain copies of software applications contracts, maintenance

greements, software changes, upgrades, configurations, source code, up to date vendor contacts and escalations, and other critical information to the maintenance and operation of the application.

A list of all departmental applications will be maintained by the department's IT Manager with appropriate contact information. This list will be shared with the City's IT department on a periodic basis.

Application system administrators will be identified and properly trained on the operation of the system and the processes for changes and updates. The department's IT manager will maintain a list of application system administrators that will be shared with the City's IT department on a periodic basis.

Departments will develop secure processes for granting application access to only appropriate users.

Monitoring –The standards for infrastructure monitoring are as follows:

Departments will monitor systems for secure baselines and policy compliance.

Infrastructure monitoring includes penetration testing, user audit trails, logging, change management approvals, intrusion detection, user behavior anomalies, repeated failed log-in attempts, etc.

Departments managing their own servers or infrastructure shall notify IT of the monitoring tools being utilized.

AUDITING

Departments will participate in and be the point of contact for all audits relating to IT security of their departments. In addition, the IT Governance Board and/or the City's IT Director can direct Security audits to be performed on any and all departmental IT systems in the COH. IT Security audit findings will be reported to the IT Governance Board and any other appropriate departments. A corrective action plan will be developed by the department and submitted to the IT Director and the IT Governance Board and any appropriate department heads and managers