Policy Subject	**Revision**	1
Information Technology Security Policy		
Effective Date	**Policy Number**	
1/1/2012	ITP 4	

Department
TECHNOLOGY SOLUTIONS

To All City Employees

X Thomas Bonfield
Thomas J. Bonfield, City Manager

I. Purpose

To establish a consistent and consolidated approach to the protection of the City of Durham's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

II. Policy

It is the policy of the City of Durham to guarantee reliable and consolidated security standards for the protection of the City of Durham's Information Technology (IT) data and assets.

III. Definition

Dynamic Host Configuration Protocol (DHCP) – a network configuration protocol for hosts on Internet Protocol (IP) networks.

Domain Name System (DNS) – a hierarchical distributed naming system for computers, services, or any resource connected to the City's network.

Freeware – computer software that is available for use at no cost or for an optional fee, but usually with one or more restricted usage rights.

Information Assets – a definable piece of information, stored in any manner which is recognized as "valuable" to the City.

IT Assets – hardware and software that is owned and operated by the City of Durham.

Shareware – copyrighted software that is available free of charge on a trial basis, usually with the condition that the City pay a fee for continued use and support.

Simple Mail Transfer Protocol (SMTP) – an Internet standard for electronic mail (e-mail) transmission across the City of Durham's Internet Protocol (IP) networks.

IV. Procedure

A. Roles and Responsibilities

1. TS Staff

a. It is the sole responsibility of designated TS staff to assess and monitor the security of the City's internal network and network perimeter. Personnel authorized by the CIO shall make use of any tool or device to probe or monitor the City network segments or computers with specific formal approval from the CIO and/or designee.

b. No other City personnel or entity shall employ any software, tool or device to hamper or restrict the scanning or monitoring capability of tools deployed for this purpose by TS. This serves to eliminate redundant efforts through centralized coordination and preempts potentially harmful negative impacts to network operations.

c. TS must provide the direction and technical expertise to ensure that the City's information assets are properly protected. This includes consideration of the confidentiality, integrity, and availability of both information and the systems that handle it.

d. The CIO and/or designee will act as a liaison on information security matters between all City departments and divisions, as well as external business partners, and must be the focal point for all IT security activities throughout the City.

2. CIO and Audit Services

a. The CIO and Audit Services shall have the responsibility for investigating any suspected security breach, exposure, or weakness in security procedures and make recommendations to the City Manager's Office to reduce or eliminate the exposure.

b. Any suspected compromise or unauthorized use or destruction of the City information assets should be reported immediately to the department head of the department involved, and to the CIO.

3. Department Heads

a. Each City Department Head is responsible for ensuring that IT Security Policy is followed to protect all the City information owned by their department from unauthorized access, use, disclosure, destruction, or modification.

b. Department directors are also responsible for an accurate accounting and enumeration of information assets under their control.

B. Disaster Recovery / Business Continuity

All City departments are responsible for maintaining a Business Continuity/Disaster Recovery plan to address loss of critical information systems and the network connectivity supporting them. This plan must be in compliance with guidelines and documentation standards designated by TS. Those departments seeking assistance in compiling such a plan may contact TS. TS will assist and be responsible for the information and network access.

C. Access Control

1. Authorization to access the City's information assets shall be based on the sensitivity (as established by the department owning the data) of the information and the users need to know, in addition to any federal, state or local regulations.

2. Access to the data or system functions will be authorized by the management of the department which owns and administers the data/system and implemented in accordance with current network operations procedures. In accordance with business functions, ownership will be established and assigned by the department for all information assets.

3. Access to confidential data, write/modify access to public data, or access to restricted system functions will be authorized in writing by the department management before access is given.

4. The City information assets must be used only for authorized business purposes, and usage must comply with all applicable policies and statutes pertaining to the public disclosure of information.

5. Each individual requiring access to City IT resources will access these resources through a unique user name assigned to the City employee or other authorized individual, and will be accountable for all activities performed under that identifier.

6. To prevent unauthorized access, individuals must not leave workstations logged on and unattended for more than 10 minutes without employing a password protected screen saver. There will be exceptions to this on a limited basis (i.e., public access terminals and PCs with appropriate physical security measures, such as those in locked offices).

7. Remote access to the City's internal network will be provided upon request with the department head's approval using TS approved IT tools or applications (see also ITP1– Use of Information Technology Resources).

D. System Development and Maintenance

1. Production applications must be hosted on hardware with appropriate capacity and fault-tolerance requirements, and with physical and logical access controls, change controls, and contingency/disaster recovery plans adequately accounted for.

2. As a goal, system development activities should take place in an environment separate from production information systems.

3. Systems hosting production applications must not be used for software development or testing, and wherever possible development and test environments must be implemented on network segments separate from production systems.

4. Before a new system is developed or purchased, management of the user department(s) must have clearly specified the relevant security requirements. All software development and acquisition requirements shall include security requirements which are consistent with the City's security and network usage policies. All new IT system implementations shall be reviewed and approved for IT security policy compliance by TS. All production information systems must employ a formal change control procedure to ensure that only authorized changes are made. To prevent changes in hardware and software from contributing to or creating security vulnerabilities, prior to installation, every non-emergency change to production systems must be compliant with the IT security architecture and approved by management as part of the formal change control process.

5. Prior to moving software which has been developed in-house to production status, programmers and other technical staff must remove all special access paths so that access may only be obtained via normal secured channels. All trap doors and other shortcuts that could be used to compromise security must be removed. All system access privileges needed for development efforts, but not required for production operation and support, must be removed.

E. Security

1. Network Security

To ensure network stability and security, primary responsibility for defining and maintaining the enterprise network topology and all enterprise network services will belong to the IT Infrastructure Division within TS. No City employee or contracted third party shall attach any device to the City's internal network that provides any network service (i.e., DNS, DHCP, SMTP, etc.) without the prior approval of the CIO and/or designee. No City employee or contracted third party shall assign a static IP address to any network attached device without coordinating with the IT Infrastructure Division. It is the sole responsibility of the IT Infrastructure Division to assign network addresses, add or delete subnets, and configure and maintain all network infrastructure equipment that routes (operates at network layer of TCP/IP stack) traffic on the City enterprise network. All usage of the City's network resources is subject to acceptable use guidelines as defined. All connectivity to networks external to the City must be reviewed and approved by the CIO and/or designee.

2. Physical and Environmental Security

All City-owned information systems and supporting network infrastructure will be secured by an appropriate level of physical security. Servers containing production information systems shall be housed in restricted access areas requiring badge and/or bio-metric access. Wiring closets containing infrastructure devices must also be locked at all times. TS personnel designated by the CIO must have access to all wiring closets. It is the responsibility of departmental management to provide appropriate physical security measures for all department owned information resources.

3. Security Awareness

Responsibility for IT security on a day-to-day basis is every City employee's duty. All City employees are expected to acquire and maintain an awareness of the requirements and provisions established in this policy, and to conduct all activities in compliance with the policies and procedures referenced herein.

F. Cloud Data Security

The CIO is required to ensure that selected departmental/enterprise cloud based applications comply with the following data security requirements before contracting with vendors for that service. Cloud Applications that do not comply with the security requirements will not be approved. The data security requirements are as follows:

- Vendor must offer data assurances such as protection against data breaches, unauthorized access and provide disclosure of data storage locations. The vendor must also provide assurances in the contract regarding data ownership, data segregation and access to data. In addition, the contract must state how legal data holds, public record request, e-discovery and request regarding how disposition of data will be handled.

- Vendor must provide the City the right to inspect and audit the City's data.

- Vendor must provide disaster recovery and business continuity.

- Vendor must sanitize the storage when service is terminated.

- Vendor must provide the City the ability to encrypt.

- Vendor must supply all the City's data within one week in open standards formats.

- Vendor may need to comply federal, state and local data regulatory requirements.

V. Other

A. This policy applies to all the information assets of the City, no matter where they reside, or what form or technology is used to store, process, or transport data.

B. Technology Solutions (TS) is responsible for establishing and maintaining the City-wide Standard Operating Procedures (SOPs) for IT security. IT security SOPs are subject to approval by the Chief Information Officer (CIO).

C. Compliance with this policy is mandatory and considered a condition of continued employment. Any violation(s) of this policy may result in disciplinary action to include termination. Contractors, business partners, and other non-City personnel must comply with the provisions of this policy (unless another more restrictive policy has been approved relating to a specific concern/control) when accessing the City's information assets. Failure to do so may result in the termination of the relationship with the City, and the City may pursue legal action for damages that arise as the result of any breach of this policy.

VI. Attachment

None.