Policy Subject Use of Information Technology Resources

Revision 1

Effective Date 1/1/2012

Policy Number ITP 1

Department TECHNOLOGY SOLUTIONS

To All City Employees

X Thomas Bonfield

Thomas J. Bonfield, City Manager

I. Purpose

To provide uniform guidelines for the proper management and protection of Information Technology (IT) resources.

II. Policy

It is the policy of the City of Durham to ensure a consistent and consolidated approch to the purchase, implementation, monitoring and protection of the City of Durham's IT resources.

III. Definition

Information Technology Resources – includes hardware (desktops, laptops, iPads, servers, storage devices, tablets, printers, copiers, scanners, faxes, etc.), software, voice/data systems, cell phones and smartphones, networks, user accounts, and associated processes/services).

Electronic Messaging – includes, but is not limited to email, instant messages, text messages, video messages, blog posts, forum posts, wiki posts, social site posts, images, and audio or video recordings.

Shared City of Durham Systems – IT resources that are shared throughout the enterprise such as network, storage area network (SAN), switches, etc.

IV. Procedure

A. Purchase

The purchase of any IT assets, such as computer related hardware (desktops, laptops, netbooks, Smartphones, tables, iPads, printers, etc.) and software (office productivity tools, business software, SaaS, tablets, cloud, web and mobile based applications, etc.) ***must be approved by the CIO/designee***.

B. Personal Use

While the City of Durham's IT resources are intended for business use only, it is recognized that, on occasion, personal use may be necessary. To that end, any personal use must not:

- violate applicable laws, regulations, contractual agreements, intellectual property rights or City Policies
- incur security risks to the City
- incur any additional cost to the City
- not interfere with work duties
- be used for personal gain or for solicitation

C. Use of Personal IT hardware and Software for City business

The use of personal IT hardware and software for any City business **must be approved by CIO/designee.**

D. Privacy

Personnel within the scope of this policy are advised that they have no privacy rights and that there is no reasonable expectation of privacy when using City IT resources.

1. The City's users should be aware that the data they created on City IT or communications systems remains the property of the City of Durham and is not private (unless the data is protected by privacy or confidentiality laws).

2. City information that is stored on or transmitted to or from City or personal systems, including all endpoints such as tablets and cell phones, is subject to disclosure pursuant to the North Carolina Public Records Law (G.S. 132).

E. Monitoring, Auditing and Inspection Activities

1. The City of Durham has the right to monitor, audit, and/or inspect any and all aspects of the City's IT resources without advance notice to any users. Failure to monitor in any specific situation does not constitute a waiver of the City's right to monitor.

2. At the written request of a Department Director for one of their respective employees, or upon authorization by the City Manager, Human Resources Director, or Audit Services Director, the Chief Information Officer (CIO) or designee has the authority to monitor and/or inspect any City IT system without notice to users.

3. For security and network maintenance purposes, authorized individuals within the City of Durham Technology Solutions Department may monitor equipment, IT systems, data, and network traffic at any time.

F. Security

1. The City of Durham's system security must be maintained at all times. Users must take all reasonable precautions, including but not limited to: safeguarding passwords, maintaining reasonable physical security around City of Durham equipment, and locking or logging off unattended workstations.

2. A user who is actively logged on to a City of Durham system is responsible for any activity that occurs whether or not they are present.

3. Passwords and User System Access

   a. The City of Durham Technology Solutions Department and/or its designees are responsible for the creation, assignment, and deletion of all user accounts for the City's systems.

   b. PASSWORD AND ACCOUNT DO'S

      I. Users are responsible for protecting their passwords and access to assigned accounts (network, systems, applications, etc.) at all times.
      II. Passwords must be changed at least every 90 days.
      III. Create strong passwords (greater than eight characters, mixed case, mixed letters, numbers, and symbols; use long phrases when possible).
      IV. Log off unused systems, and/or utilize a password protected screen saver.
      V. Compromised passwords/accounts must be reported to the Information Technology Department.
      VI. Refer anyone who asks for your password to this policy.

   c. PASSWORD AND ACCOUNT DON'TS

      I. Do not use weak passwords (simple words, names, personal dates, all alpha, all same case, predictable patterns, e.g.,12345, zyxw, asdf, etc.).
      II. Do not give your password to anyone verbally, or electronically, for any reason. Your password belongs to you and only you.
      III. Do not use personal, non-City system passwords (e.g., home email, home Internet, eBay, etc.) as passwords for City systems.
      IV. When possible, do not reuse the same password for multiple systems.
      V. Do not store written passwords in any area accessible by others.
      VI. Do not store passwords electronically unless they are encrypted and inaccessible to others.

   d. The level of access to the network, servers, applications, and personal computers will be administered by the Technology Solutions Department based upon the job tasks for the individual user.

4. Physical Security

   a. Shared City of Durham IT resources (network, servers, systems, etc.) will be physically secured by the Technology Solutions Department.

   b. Access to the data center, disaster recovery site, phone switches and other key infrastructure is limited by lock with access granted to authorized personnel only.

   c. Media, such as daily and monthly backups, will be stored in a secure area with access granted to authorized TS personnel only.

   d. Users are responsible for the physical security of assigned IT resources.

   e. To the degree possible, IT resources should be protected from theft and/or vandalism, fire and other natural environmental hazards.

   f. Laptops, cell phones, etc., in vehicles must be stored in the trunk or otherwise out of sight. They may never be left in non-City vehicles overnight.

   g. Employees should exercise precautions to ensure that their computer hardware is not exposed to dangers related to their specific use, i.e., accidental beverage spills, improper ventilation of air intakes, etc.

5. Application Security Standards

All software applications which manage sensitive or confidential data, whether acquired from a third party or developed internally must adhere to the following security requirements:

   a. Must support authentication of individual users
   b. Must not store or transmit user credentials in a clear text or easily reversible form
   c. Must support application scope restriction based on user levels
   d. Must support user tracking for critical transaction activity

G. Third-Party Access to City of Durham IT Resources

Third parties include vendors, contractors, or other guests that require access to City of Durham IT resources is only permitted for City business purposes. No third party may be allowed access to City systems without written approval from the CIO/Director of Technology Solutions Department or designee.

H. Remote Access

1. Remote access to the City's IT resources (access to the City's systems from external systems, e.g., via the Internet) consumes technology resources above and beyond those required for local access. The Technology Solutions Department will review requests and grant remote access based upon business cases and resources available.

2. Remote access users are subject to all policies herein.

3. Additional security requirements may be established for remote access systems by the Technology Solutions Department.

I. Prohibited Use

The following is a list of examples of prohibited uses. This is not intended to be a comprehensive and complete list. Other uses not listed here may be deemed as prohibited:

1. Any use that violates Federal, State, or Local laws or regulations is expressly prohibited.
2. Knowingly or recklessly interfering with the normal operation of computers, networks, or other related equipment is prohibited.
3. Connecting unauthorized equipment to the network for any purpose is prohibited.
4. Running or installing unauthorized software on the City's computers is prohibited.
5. Copying of any software from the City's computers, for other than archiving purposes, is prohibited.
6. Using the City's network to gain unauthorized access to any computer system is prohibited.
7. The use of the City's systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, libelous, or other offensive or abusive material (including messages, images, video, or sound) is prohibited.

J. Reporting Violations

1. Every department should follow IT procedures to monitor compliance with the IT use policies within this document, and to report violations (both by "insiders" such as employees and contractors and "outsiders" such as unauthorized visitors, trespassers and hackers).

2. It is the responsibility of each IT user to remain diligent in the identification and reporting of IT policy violations. Staff is required to report any suspicious, abnormal or unnatural behavior or events to his or her supervisor and the CIO/Director of the Technology Solutions Department by email, in person, or in writing via interoffice mail.

K. Hardware/Software Standards, Procurement, and Installation

1. The City's Technology Solutions Department has the sole responsibility for establishing IT standards. The City of Durham's Technology Solutions Department and/or its designees are responsible for procuring, maintaining inventory, and installing technology required for City operations. The Technology Solutions Department is also responsible for engaging and managing relationships with technology vendors.

2. All software installation media must be stored by the Technology Solutions Department.

L. Technology Support

The City of Durham's Technology Solutions Department has primary responsibility for IT technical support. Unless Technology Solutions has specified otherwise for a particular system, users should always contact Technology Solutions for all technology-related needs.

M. Desk and Cell Phones

1. Desk Phones

a. The City of Durham provides its staff with telephones for conducting official City business. City phone use should be restricted to official city business purposes, except for emergency and important telephone communications, such as child care needs, medical appointments, and other critical communications. Reasonable, infrequent personal use of the City's telephone system by employees is permitted, but should not interfere or conflict with official City business use.

b. Personal calls should be made for the well-being of the individual or his/her immediate family or for personal business that requires immediate attention. Any personal long distance telephone calls made by staff must be reimbursed to the City.

2. Cell Phones

a. It is the policy of the City of Durham to provide cell phones to employees for business use, when use of cell phones will increase the level of service provided to the City's customers, increase the level of safety for applicable City employees, reduce the cost of providing services, and/or satisfy legal requirements.

b. Personal calls should be made for the well-being of the individual or his/her immediate family or for personal business that requires immediate attention.

c. Employees will reimburse the City for personal calls at an applicable rate if it increases the cost to the City. It is the responsibility of Department Directors or their designees to review individual invoices to ensure reimbursement for personal calls. It should be noted that cellular bills with call details are public record and available upon request.

d. Technology Solutions Responsibilities

1. Technology Solutions will notify each department head/designee of cell phone usage in a written monthly report provided by the City's current cell phone provider.
2. Technology Solutions will perform an analysis of usage to assist the department in identifying low usage. If a cell phone has no usage, then the department head or designee must submit in writing justification for keeping the cell phone. If the department has good justification for keeping a cell phone, then Technology Solutions will look into prepaid options for cellular service.
3. Technology Solutions will send a quarterly report of those employees receiving a stipend and those employees having city issued cell phone to each department direct/designee and requests a written response form the department as to the validity of te repots. In addition, Technology Solutions will review the findings from each department. If Technology Solutions finds exceptions, the department will notify the other departments and take corrective action immediately.

e. Designee/Department Director Responsibilities

1. Review the invoice for any extra cost (i.e., text messaging, fi there is not a text plan)
2. Review for unauthorized downloads of ring tones, games, etc.
3. Review for Cell Phone Assignment – The designated employee is to review the invoice for accuracy in the cell phone assignment
4. Review for Phone Usage – To ensure that employees are reconciling the invoice, highlighting personal calls for reimbursement, and no usage. If the cellular users have made personal call, then they are to remove the City for those personal calls. If a cell phone has no usage, then the department head or designee must submit in writing justification for keeping the cell phone. I the department has good justification for keeping a cell phone, then Technology Solutions will look into prepaid options for cellular service.

f. Procurement/Activation

Only the CIO or his/her designee in the Technology Solutions Department is authorized to contact the City's current cell phone provider to procure/activate new or replacement cell phones. Other employees are prohibited from entering into cell phone agreements with cell phone providers for City cell phones.

g. Operation of Cell Phones

Employees who are required to be available by a City-provided cell phone as part of their job duties must maintain their cell phone in a useable and active status.

h. Personal Cell Phones Used for City Business

If an employee uses their personal cell phone to conduct City business, they may receive a cell phone allowance which must be approved and certified by the employee's Department Director.

i. Cell Phone Allowance

If a Department Director determines that an employee needs to be contacted for City business by cell phone, then the employees can opt to receive a city cell phone or use their personal cell phone. If the employee opts to use their personal cell phone, they will be allotted an allowance to be determined annually. This cell phone allowance will be included in the first payroll check of each month and the allowance is taxable. Cell phone allowance is not intended to cover the entire cost of an employee's cellular service. Employees cannot receive both a monthly cell phone allowance and a City-owned cell phone at the same time. Employees are responsible for reporting to their immediate supervisor if the above occurs. Employees are responsible for giving their cell phone numbers to their Department Director or designee so that it can be published in the City's cellular directory for emergencies and other City use.

N. Storage Media Recycling and Disposal

1. The purpose of this section is to ensure that all digital media is properly recycled or disposed of for reasons pertinent to data security, software license protection, and in compliance with environmental regulations.

2. If a hard disk, tape, CD, DVD, ZIP disk, diskette, or other storage device can be re-used, users should erase the existing data from the device and continue to use it, or make it available for someone else to use.

3. If the digital media is unusable or is no longer needed, it should be sent to the Technology Solutions Department's Support Division for destruction.

4. Un-recycled or unusable media must be completely erased using a disk sanitizer utility. If that is not possible, the media should be physically damaged in a manner to render it unreadable by any device.

V. Other

A. For security reasons, administrator-level network, server, and PC access, is limited to Technology Solutions support staff and/or their designees.

B. The scope of this policy includes all personnel who have access to the City of Durham's IT resources (employed by the City or not).

C. IT resources containing City of Durham data that are hosted by third parties outside of the City's network and the personnel with access to those IT resources are also subject to this policy.

D. All IT resources defined in this policy, along with all information transmitted by, received from, and stored upon, said IT resources are considered to be possessed by, and are the property of the City of Durham.

E. The City of Durham's IT resources use is subject to various Federal, State, and Local laws (i.e., Sarbanes-Oxley, HIPAA, Red Flag, PCI DSS, etc.).

F. Compliance with this policy is mandatory and considered a condition of continued employment. Any violation(s) of this policy may result in disciplinary action including 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 IT resources. 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.