CITY OF DENTON

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE

SECTION:	GENERAL POLICIES/PROCEDURES/DIRECTIVES	REFERENCE NUMBER: 506.02
SUBJECT:	TECHNOLOGY SERVICES	INITIAL EFFECTIVE DATE: 10/1/17
TITLE:	USER AUTHORIZATION, IDENTIFICATION, AND ACCOUNTABILITY	LAST REVISION DATE:

ADMINISTRATIVE DIRECTIVE

The purpose of this directive is to outline the accountability guidelines for use of computer equipment and technology systems at the City of Denton (City). Lack of accountability can introduce unacceptable risks to the employee and to the City. Therefore, this directive is enacted to protect the employee and the City's interests. This does not include computers that are designated for public use.

I. ROLES AND RESPONSIBILITIES

A. Managers/Supervisors- City managers/supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties and notifying Technology Services of changes in access status.

B. System Administrators – Technology Services system administrators have the responsibility of periodically reviewing user access privileges and notifying management of any access concerns.

II. ACCESS AUTHORIZATION AND ACCOUNT MANAGEMENT PROCESS

A. Prior to being granted access to City computer resources, the needs of every employee, contractor, vendor, guest, or individual should be given ample consideration and authorization granted to allow access to only the City resources that is needed to perform his/her duties. *This should be a formal process, whereby authorization is approved and a record of what is needed to perform required duties. The resource the individual is allowed to access is kept on file as listed below.*

B. Access Authorization will need to be established or reviewed under the following conditions:
   1. An individual begins work;
   2. The individual transfers to another area resulting in job function changes;
   3. Employment terminates; or

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE:	*USER AUTHORIZATION, IDENTIFICATION AND ACCOUNTABILITY*	*REFERENCE NUMBER:* *506.02*

4. The individual requires additional functions or access to fulfill a specific duty, or the worker no longer requires access.

C. Access Modification- Request for modifying individual access. (i.e., to grant or disallow additional permissions) should be accomplished by submitting a new request via electronic or hard copy.

D. Emergency Access- Requests for temporary emergency access must also be documented.

III. USER IDENTIFICATION AND PASSWORD PROTECTION

A. Unique Identification
Authorized users should be assigned unique user identifications for access to City network and information systems.

B. Use of Unique Identification
User identifications must be used only by the assigned user.
1. Authorized individuals are responsible for activities using their assigned user identification and password.
2. City assigned user identifications should not be used as personal user identifications outside of City (e.g., non-City of Denton websites, Internet, Yahoo, AOL, etc.).

C. Passwords
Strong passwords must meet all the following criteria.
1. Network and information systems should require passwords to be changed every 90 days, where possible.
2. All passwords must be a minimum of eight (8) characters in length, where possible.
3. Contain both alphabetic and numeric characters. All passwords should contain at least one alphabetic (a – z), one numeric character (0 – 9), and one capital letter as the system allows.
4. It is recommended that that passwords not be constructed by using personal information or words found in a dictionary. Examples of personal information include a spouse's name, children's names, automobile license plate, social security number, birthday, etc.
5. The password must be different than the last four passwords.
6. A password may not be changed for a minimum of seven (7) days after a password is set, without the approval of Technology Services.

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE:	*USER AUTHORIZATION, IDENTIFICATION AND ACCOUNTABILITY*	*REFERENCE NUMBER:* *506.02*

Below are some other examples of password variations that purposely avoid using complete English word patterns. By injecting numbers and special characters instead of letters, these passwords will take exponentially longer for a dictionary program to guess.

- Dog.lov3r
- dOG.lov3r
- i7ovemydog!!
- d0gsaremybestfr13nds
- sn00pdoggyd0G
- Karm@beatsDogm@
- C@ts-and-Dogs-Living-together

D. Recording Passwords
Passwords should not be written or otherwise recorded where they are accessible or recognizable by anyone else, such as taped to computer screens, stored under keyboards, or visible in a work area.

E. User Account Inactivity
If a user account has not been accessed for a period of 90 days, the account will be disabled. After the account has been disabled for 30 days, it will be removed from the system.

F. Sharing Passwords
Passwords should not be shared or used by others. This includes a co-worker, manager, supervisor, friend, vendor, partner, information technology staff, administrative assistant, or others.

G. "Remember Password" Feature
Features that allow applications or systems to "remember" passwords should not be used.

H. Automated Logon Prohibited
Macros, quick keys, shortcuts, or like technology to automate entry of User ID's and/or passwords should not be constructed or used.

I. Compromised Password
A password should be changed immediately when it has been compromised or when there is suspicion that it has been compromised.

IV. PASSWORD CONTROL

These changes require the submission and approval of a change request form or proposal to the Chief Technology Officer or his/her designee. The Change Request should:

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE:	*USER AUTHORIZATION, IDENTIFICATION AND ACCOUNTABILITY*	*REFERENCE NUMBER:* *506.02*

A. Password Changes
When a user is unable to change their own password and needs Technology Service to change their password, A Change Request form should be filled out and signed by their immediate supervisor and then submitted via electronic or hardcopy to User Support. Once Technology Services has processed the request, the user and their supervisor, will be notified of the change. Alternatively, users that have enabled the self-service password reset feature are able to change and/or reset their own password without submitting a change request. For assistance with setting up the self-service password reset feature, please contact User Support at extension 8300.

B. Initial Or Reset Passwords
Passwords issued by Technology Services will be valid only for the first log-on. Users should create unique passwords at the first log-on or session.

C. Unsuccessful Attempts
Five (5) consecutive, unsuccessful attempts to access a City network or information system will automatically suspend or disable the user's ability to successfully log-on. The account will be locked for a minimum of 30 minutes, or until an administrator enables the user account.

D. Vendor Default Passwords
Should be changed before any computer or communications system is released for production and used for City business. In addition, Vendor accounts for remote or on-site maintenance are only enabled during the time period needed by the vendor and monitored by City employees during use.

E. Idle User Sessions
If a user's workstation has been idle for more than 30 minutes the workstation will be locked with their network password the user will be required to enter their password to gain access to the workstations.

F. Automated Systems
To the extent possible, information technology should be designed, configured, and implemented to adhere to these provisions.

V. ENFORCEMENT

In order to safeguard City resources, violators of this directive may be subject to disciplinary action and penalties under applicable law. The City may temporarily suspend, block or restrict access to computing resources and accounts, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, confidentiality, or

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE:	*USER AUTHORIZATION, IDENTIFICATION AND ACCOUNTABILITY*	*REFERENCE NUMBER:* *506.02*

availability of City computing and network resources, or to protect the City from liability. If violations of this directive are discovered, which are illegal activities, the City may notify appropriate authorities. The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as a result of violations of this directive.

VI. EXCEPTIONS

Any exceptions to this directive will require written authorization. Exceptions granted will be issued a directive waiver for a defined period of time. Requests for exceptions to this directive should be addressed to the Chief Technology Officer or designee.