City of Dover Acceptable Use Policy

A Message to all System Users

This document formalizes the City policy for all employees as well as contractors and other "users" of our City's communications and computer systems. Each department may also choose to develop and enforce its own acceptable use policies to further regulate use within its local environment.

This Acceptable Use Policy is your resource to help you make sound decisions in using communications and computer systems to do your job.

Our goal is to put controls in place that will help protect the City from sabotage and espionage. The threat is real, as each day, IT intercepts hundreds of viruses and suspicious messages containing executable files trying to bypass our security systems. These controls also help minimize the potential risks of misuse. This misuse includes unnecessary Internet usage causing network and server congestion. This Acceptable Use Policy is your (the user's) guide for helping us achieve this goal by conducting City of Dover business with integrity, respect, and prudent judgment.

Each department is responsible for the activity of its users and for ensuring that its users follow this Acceptable Use Policy. Violations not promptly remedied by the user may result in termination of these services.

Introduction

Users are accountable for familiarizing themselves with this policy and using it as a guidepost for your daily decisions and actions when using these services.

Read the policy and give careful attention to those subjects that most pertain to your job duties.

Understand the purpose of this policy and your overall responsibilities for standards of business conduct.

Consult with your supervisor or the IT Department for additional clarification of this policy.

Note the Following:

Applicability

City of Dover's expectations for responsible use are applicable to all parties who use the City communications and computer systems on behalf of the City, including, but not limited to, its employees, consultants, in-house contractors, and other "users."

Limitations

This acceptable use policy does not address every possible scenario or condition regarding acceptable use. If it is not specifically addressed within this document, consult with IT.

Acceptable Use of Communications and Computer Systems

City of Dover communications and computer systems are vital to our business and critical to overall

communications. Our success is directly related to safeguarding and properly using these systems.

What are City communications and computer systems?

City of Dover communications and computer systems are any equipment, hardware, software, or networks (including wireless networks) owned, provided or used by or on behalf of the City of Dover that store or transmit voice or non-voice data. This includes telephones, cellular/wireless telephones, voice mail, computers, e-mail, facsimiles, pagers, and City Intranet or Internet access (including when accessed through personally owned computers).

Note: When personal computers or other electronic devices are not owned by the City but are used for City business, the City retains the right to access any City records or materials developed for City use. Also, we must ensure that any City materials are appropriately safeguarded according to applicable standards in this section, including, but not limited to, virus protection of, protected access to, and backup of these materials.

Access, Maintenance and Protection

Users must safeguard the confidentiality and integrity of City systems, including strong password logons (see https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb) access codes, network access information, log-on IDs from improper access, alteration, destruction, and disclosure. Users shall only access or use these systems when authorized. Users must abide by City standards contained in this section and any other City policies regarding protecting data and information stored on these systems.

Cybersecurity Awareness Training

All employee who access the City of Dover's IT assets are required to take Cybersecurity training within 15 days of being granted access. This training will consist of a series of short videos on the most prevalent issues in IT security, and will take approximately 30 minutes. All employees will renew this training yearly during the month of October.

Employees who click on more than 2 Phishing tests in a 12-month period will be asked to retake the training.

Unlawful and Inappropriate Use

Users are obligated to never use City systems (such as the Intranet or Internet) to engage in activities that are unlawful, violate City policies, or in ways that would:

- Be disruptive, causing unnecessary offense to others.
- Be considered harassing, discriminatory, or creating a hostile work environment.
- Result in the City of Dover's liability, embarrassment, or loss of reputation.

External groups or organizations are not permitted to access the City's computer network, except as permitted by IT.

Protection and Integrity of Data

Users must maintain the integrity of City information and data stored on City systems by:

- Introducing data into our systems that serve a legitimate business purpose.
- Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
- Protecting data and information stored on or communicated across our systems and not accessing this data or information (customer data, employee records, etc.) unless authorized.

- Protecting data and information communicated over internal or public networks (the internet) to avoid compromising or disclosing nonpublic City communications
- Not attempting to bypass IT Security measures.

Personal Use

While City systems are intended for primarily business/instructional purposes, limited (incidental and occasional) personal use may be permissible when authorized by your manager and it does not:

- Interfere with your work responsibilities.
- Involve interests in personal outside business and/or other non-authorized organizations and activities (including, but not limited to selling personal property/items or soliciting for or promoting commercial ventures, charitable, religious, or political activities).
- Violate any of the standards contained in this code or other City policies.
- Downloading or streaming of music and video files is *prohibited, unless approved by your supervisor.*

Virus Protection

If users suspect a virus, they must not use the applicable computer systems and equipment until the virus is removed and they will report the matter immediately to the IT Department. The City of Dover has purchased anti-virus software for all city computers.

Properly Licensed Software

Users will use only approved and properly licensed software and will use it according to the applicable software owner's license agreements. **Installing any software, including freeware (screensavers, browsers, etc) is prohibited unless approved by IT**.

Treatment of Third-Party Data or Software

Users must ensure that any nonpublic City information or software of a third party that is stored, copied, or otherwise used on City systems is treated according to City of Dover's standards regarding nonpublic City information and applicable agreements and intellectual property restrictions.

City of Dover Monitoring

City communications and computer systems, including, but not limited to, computer networks, data files, e-mail and voice mail, are subject to monitoring by the IT Staff and your management to ensure the integrity of the technology, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes. Employees should have no expectation of privacy in regard to use of these services.

Use of E-Mail and the Internet

Inappropriate use of e-mail includes, but is not limited to, sending or forwarding:

- Messages, including jokes or any language that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive, or otherwise inappropriate (this includes but is not limited to messages about age, race, gender, disability, national origin, any other legally defined discriminatory classifications or similar matters.)
- Pornographic or sexually explicit materials.
- Chain letters.
- Information related to religious materials, activities, or causes – including inspirational messages.

- Solicitations unless sanctioned by the City of Dover.
- Auction-related information or materials unless sanctioned by the City of Dover.
- Games or other software copyrighted materials without a legitimate business or instructional purpose (and then only according to the rights and licenses granted by the owner of the games, software, or copyrighted material.)
- Messages that disparage companies or products.
- Materials related to personal commercial ventures or solicitations for personal gain (including, but not limited to messages that could be considered pyramid schemes).
- Information related to political materials, activities, or causes unless sanctioned or permitted by the City of Dover.
- Unauthorized or inappropriate mass distribution of communication.
- Any other materials that would be improper under this policy or other City of Dover policies.

Inappropriate use of the Internet includes, but is not limited to, accessing, sending or forwarding information about, or downloading (from):

- Sexually explicit, harassing, or pornographic sites.
- "Hate sites" or sites that can be considered offensive or insensitive.
- Auction sites for personal use.
- Gambling sites.
- Non City of Dover business-related chat sites.
- Underground or other security sites which contain malicious software and/or instructions for compromising City of Dover security.
- Games, software, audio, video, or other materials that are not properly licensed to use or transmit, or that are inappropriate.
- Offensive or insensitive materials, such as sexually or racially oriented topics.
- Intentional importation of viruses.

Remedial Action

When IT learns of a possible inappropriate use, IT will immediately notify the employee or supervisor who must take immediate remedial action and inform IT of its action. Repeated violations will be addressed with the Department Director. In instances where criminal activity is suspected, IT will work directly with the proper authorities, and follow their guidance in determining appropriate action.

Inappropriate use of City communications and computer systems may be grounds for discipline up to and including dismissal.

In an emergency, in order to prevent further possible unauthorized activity, IT may temporarily disconnect that employee or building from the network. If this is deemed necessary, every effort will be made to inform the employee or building personnel prior to disconnecting, and every effort will be made to reestablish the connection as soon as it is safe to do so.

Unauthorized activity or non-acceptable usage determined at the department level may be subject to remedial action being taken in accordance with the acceptable use policy of that department (if applicable) as well as those actions outlined above. The remedial action outlined in departmental policies may differ from the remedial action as outlined in this policy. Should there be any conflict, Human Resources will make a determination as to applicability.

QUESTIONS OR COMMENTS ON THIS POLICY

Please address any questions or comments to the IT Director.

The City of Dover Password Policy

A. Overview

All employees and personnel that have access to City of Dover computer systems must adhere to the password policy defined below in order to protect the security of the network, protect data integrity, and protect computer systems. Adopting a good password policy is the most important barrier to unauthorized access.

B. Purpose

This policy is designed to protect the City of Dover resources on the network by requiring strong passwords. It also establishes password protection requirements along with standards for acceptable passwords.

C. Scope

This policy applies to any and all personnel who have any form of computer account requiring a password on the City of Dover network including but not limited to a domain account and e-mail account.

D. Password Protection

1. Never write passwords down.
2. Never send a password through e-mail.
3. Never include a password in a non-encrypted stored document.
4. Never tell anyone your password.
5. Never reveal your password over the phone.
6. The credentials (username/password) you use to logon to the City network should **NEVER** be used for any other computer or website.
7. Never hint at the format of your password.
8. Never reveal or hint at your password on a form on the internet.
9. Never use the “Remember Password” feature of application programs such as Chrome, your e-mail program, or any other program.
10. Never use your City of Dover password on an account over the internet which does not have a secure login - the web browser address should start with https:// rather than http://
11. Report to the IT Department any suspicion of your password being compromised.
12. If anyone asks for your password, refer them to the IT Department.
13. Be careful about letting someone see you type your password.

E. Password / Passphrase Requirements

1. Password must be at least 15 characters (including spaces).
2. Password must be changed, at least, every 365 days.
3. You will not be able to reuse the same password for four change cycles.
4. You will be locked out of your account after five (5) failed attempts.

F. Recommendation

A password that uses a passphrase is much more difficult to guess or crack than a password consisting of just “password” or any other single dictionary word. With each complexity requirement (upper case, lower case, number, special character, etc) to make a password stronger, the likelihood of writing it down increases exponentially, and that defeats the purpose. A passphrase is easier to remember and eliminates the need to write it down. You should also make it something that is easy to type.

It is recommended to use a mixture of lower case, upper case, numbers, and/or special characters – any mixture is sufficient.

G. Examples

As an example, you could use, **the rain in spain** (17 characters). That would be sufficient; however, you could make it better. For instance, **The rain @ Spain** (16 characters) is much stronger. Adding capitalization, numbers, and/or special characters greatly increase its security without necessarily increasing its complexity. Something as simple as **I l0ve mom & dad** (16 characters) is another great passphrase example.

My truck is blue
The hou$e is green
I dr1ve to work

You can check your password’s strength at this site:
http://www.microsoft.com/protect/yourself/password/checker.mspx

If you want to see how long it would take to crack your password from a standard computer, visit http://howsecureismypassword.net/ Use this site to check your password format. **Don’t use your actual password**, but rather a password formatted similarly.

You can change your password at any time. Press ***Ctrl-Alt-Del*** and select ***Change Password***

For additional information or guidance, contact the IT Department.

ACKNOWLEDGMENT STATEMENT

City of Dover - Acceptable Use Policy

City Employee

This is to certify that I have read and agree to abide by the guidelines set forth within the City of Dover Acceptable Use Policy. As an employee of the City of Dover, I fully intend to comply with this policy realizing that I am personally liable for intentional misuse or abuse of the City's communications and computer systems. If I have any questions about the policy, I understand that I need to ask my supervisor or IT for clarification.

If I refuse to sign this acknowledgement form, my supervisor will be asked to sign this form indicating that I have been given time to read and have questions answered about this policy. The supervisor will read this statement to me prior to signing the document and advise me that by not signing this document my rights to use the City's Communications and Computer Systems may be denied and may affect my ability to meet my job requirements.

Printed Name: _____

Signature: _____

Department: _____

Date: _____

Supervisor Signature (*as required)

_____

Comments:

_____

ACKNOWLEDGMENT STATEMENT

City of Dover - Acceptable Use Policy

Non-City Employee

This is to certify that I have read and agree to abide by the guidelines set forth within the City of Dover Acceptable Use Policy that apply to my use. (Some users may use a combination of communications and computing resources.) As an authorized user of the City of Dover's communications and computing resources, I fully intend to comply with this policy realizing that I am personally responsible for intentional misuse or abuse of the City's communications and computer systems. I understand that the City of Dover has no authority over non-city employees. However, all users must agree to abide by all policies, standards promulgated by the IT Department as a condition of access and continued use of these resources. If IT learns of possible inappropriate use, IT will immediately notify the affiliate responsible, which must take immediate remedial action and inform IT of its action. In instances where affiliates do not respond in a timely or reasonably appropriate manner, are "repeat offenders", or if criminal activity is suspected, IT will work directly with the proper authorities, and follow their guidance in determining appropriate action. In an emergency, in order to prevent further possible unauthorized activity, IT may temporarily disconnect the user or affiliate. If I have any questions about the policy, I understand that I need to ask IT for clarification.

If I refuse to sign this acknowledgement form, my rights to use the City's Communications and Computer Systems may be denied and may affect my ability to meet my job requirements.

Printed Name: _____

Signature: _____

Company: _____

Date: _____

Witness:_____

Witness name (printed)_____