# City of Cocoa

# Information Technology & Cybersecurity Policies

Version 2.4
May 22, 2019

Revised By:
Robert Beach
Chief Technology Officer
Information Technology Division, City Manager's Office

Robert Beach
Chief Technology Officer, City of Cocoa

John Titkanich
City Manager, City of Cocoa

**Table of Contents**

# Introduction

**Statement of Purpose**

This document is designed to provide a comprehensive information security framework to manage the electronic resources of the City of Cocoa (City). These practices must be maintained to ensure the highest level of information security possible.

The directives and goals set forth in this policy are owned, implemented, and maintained by the Information Technology Division of the City. It is the responsibility of the City's Chief Technology Officer to periodically review and revise the policy where necessary.

The Information Technology and Cybersecurity Policies is composed of 21 component parts that detail distinct areas of information security as they relate to the City. Each component provides specific directives for the design, implementation, and management of information technology and security at the City. The thirteen components are as follows:

1. Acceptable Use Policy
2. Minimum Access Policy
3. Password Policy
4. Internet Acceptable Use and Filtering Policy
5. Email Policy
6. Cybersecurity Awareness and Training Policy
7. Wireless Communication Policy
8. Public Wireless Communication Policy
9. Remote Access Policy
10. Remote Access Tools Policy
11. Acceptable Encryption Policy
12. Clean Desk Policy
13. Anti-Virus Policy
14. Software Installation Policy
15. Computer Hardware and Peripheral Installation Policy
16. Infrastructure Protection Policy
17. Internet Perimeter Policy
18. Firewall Policy
19. Audit Policy
20. Server and Data Backup Policy
21. Cybersecurity Incident Response (CSIR) Procedure

**Scope**

This policy applies to all electronic resources owned or operated by the City, provided through contracts with applicable third-party vendors, employees, contractors, and other authorized users. This policy does not apply to printed or copied electronic resource materials. These materials are subject to State and Federal law, and City records management disclosure, retention, and destruction policies.

**Policy Objective**

The objectives of the Information Security Policy are comprised of the following:

1. Establish documented policies on privacy, confidentiality, and protection of the City's electronic resources and electronic records.

2. Ensure that the City's electronic resources are used for the purposes appropriate to the City's mission.
3. Publish and make aware the policies regarding the City's electronic resources to City employees, vendors, other agencies affiliated with the City and its citizens.
4. Ensure compliance with state and federal regulatory agencies regarding security of electronic resources.
5. Prevent malicious or inappropriate use of the City's electronic resources.

**Definitions**

1. **Authorized User**: An employee of the City, approved third-party vendor, or other party explicitly approved by the City of Cocoa Chief Technology Officer who has been granted access to the City's electronic resources (including cellular phones), for the purposes of fulfilling his or her job functions or other functions directly related to his or her relationship with the City.
2. **Chief Technology Officer**: The designated party responsible for the development, implementation, and maintenance of the City's Information Technology and Cybersecurity Policy.
3. **Cloud**: A global network of remote servers that operates as a single ecosystem, commonly associated with the Internet.
4. **Compromised systems**: Computer systems that have been subject to unauthorized access to include text messages and chain type emails.
5. **Cybersecurity Incident**: A cybersecurity incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the City's information system.
6. **Denial of Service (DOS)**: An incident in which an end user or organization is deprived of the services of an electronic resource that they would normally expect to be delivered. The deprival is caused by the exhaustion of an electronic resource due to a malicious attack on the resource by compromised systems.
7. **Distributed Denial of Service (DDOS)**: An incident in which an end user or organization is deprived of the services of an electronic resource that they would normally expect to be delivered. The deprival is caused by the exhaustion of an electronic resource due to a magnified malicious attack on the resource by compromised systems.
8. **Electronic resource**: Any telecommunications equipment, cell phone, pager, transmission facility, computer system, data processing and storage system, server system, networking system, program, and application software owned or operated by the City.
9. **Electronic resource access**: Effective control over the location of electronic information and its content. Electronic resource access includes the original information or a copy or modification of the original information. Authorized Information Technology administration is excluded from this definition as it is strictly designated to manage electronic resources (including cellular phones).

10. **Electronic Mail System (email system)**: Any computer or cell phone software application that allows the communication of electronic mail from one computer to another.
11. **Electronic Mail (email)**: Any message, form, image, attachment, program, data, or other content sent, received, stored, or forwarded within an electronic mail system.
12. **Extranet**: An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses.
13. **Firewall**: A logical access control function that acts as a barrier between two or more physical computer network partitions and is used to protect electronic resources from unauthorized access.
14. **Host**: A computer providing computer services for one or more authorized users.
15. **Information Security**: Programmatic measures taken to minimize the risk of unauthorized access achieved by either physical or logical means to the City's electronic resources (including cellular phones).
16. **Internet**: A global system interconnecting computers and computer networks from various independent organizations and end users.
17. **Intranet**: A private system interconnecting computers within an organization's authorized users over the TCP/IP protocol.
18. **Local Area Network (LAN)**: A data communications network connecting computers in a limited geographic area.
19. **Password**: A string of characters which serves to authenticate an authorized user's identity and may grant or deny electronic resource access.
20. **Personally Identifiable Information (PII)**: Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with outer personal or identifying information which is linked or linkable to a specific data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history my include PII. A criminal history record for example inherently contains PII as would a Law Enforcement Notational Data Exchange (NDEx) casefile.
21. **Phishing**: The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information such as passwords and credit card numbers.
22. **Server**: A computer system, which may be hardware and/or software that provides computer services to other computer or telecom systems.
23. **Strong Password**: A string of characters which serves to authenticate an authorized user's identity, and may grant or deny electronic resource access, and meets the following conditions: at least one (1) upper case letter, at least one (1) lower case letter, at least one (1) numeric digit, no more than three (3) consecutive characters of the authorized user's username, no less than eight (8) characters in length, no dictionary-

based word more than 3 characters in length, no match to the authorized user's previous three (3) passwords.

24. **Third-Party vendor**: An organization affiliated with the City for the monetary exchange of goods and services.
25. **Virus**: A computer software program that is attached.
26. **Trojan Horse (Trojan)**: A destructive computer software program that appears as a benign computer software program.
27. **Unauthorized Access**: The unlawful intrusion into any electronic resource for purposes not consistent with the City's mission.
28. **Web page**: A document on the World Wide Web identified by a Unique Resource Locator (URL).
29. **World Wide Web (WWW)**: A global system of computer systems that support documents formatted in Hypertext Markup Language (HTML), readily available to the general public.
30. **Worm**: A self-contained computer virus that can propagate itself through compromised systems.

# Acceptable Use Policy

**Purpose**

The City of Cocoa's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the City's established culture of openness, trust, and integrity. The City is committed to protecting its employees, partners, and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the City of Cocoa. These systems are to be used for business purposes in serving the interests of the City, and of our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every City employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment and electronic resources at the City of Cocoa. These rules are in place to protect the employee and the City. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, and legal issues.

**Scope**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct City of Cocoa business or interact with internal networks and business systems, whether owned or leased by the City, the employee, or a third party. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with City policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, interns, temporary employees, and other workers at the City of Cocoa, including all personnel affiliated with third parties. This policy applies to all equipment that is owned, leased, or operated by the City of Cocoa.

**Policy Statements**

***General Use and Ownership***

1. The City of Cocoa's proprietary information stored on electronic and computing devices whether owned or leased by the City, the employee or a third party, remains the sole property of the City of Cocoa.

2. While the City desires to provide a reasonable level of privacy, users should be aware that the data they create on the City's electronic resources remains the sole property of the City and subject to all federal, state, and local laws.
3. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of City proprietary information.
4. You may access, use or share City proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
5. In general, personal use of City resources should be avoided. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
6. The City subscribes to the principle of Least Privilege when granting network and resource access. Employees will only be granted the least amount of network privileges necessary to complete their job functions.
7. For security and network maintenance purposes, authorized individuals within the City's IT Division may monitor equipment, systems, and network traffic at any time.
8. The City reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

***Security and Proprietary Information***

1. All mobile and computing devices that connect to the City's network must comply with the Minimum Access Policy.
2. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen (Window Key + L) or log off when the device is unattended.
4. Postings by employees from a City of Cocoa email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City of Cocoa, unless posting is in the course of business duties.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

***Unacceptable Use***

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the City of Cocoa authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing city-owned resources.

The lists below are by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use.

***System and Network Activities***

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Cocoa.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting City business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a City computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any City of Cocoa account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the City’s IT Division is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the City's network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

***Email and Communication Activities***

When using City resources to access and use the Internet, users must realize they represent the City of Cocoa. Whenever employees state an affiliation to the City, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the city". Questions may be addressed to the IT Division.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the City's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City or connected via the City's network.
7. Posting the same or similar non-business-related messages to large numbers of groups (newsgroup spam).

***Blogging and Social Media***

1. Blogging by employees, whether using the City's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the City's systems to engage in blogging is acceptable, if it is done in a professional and responsible manner, does not otherwise violate City policy, is not detrimental to the City's best interests, and does not interfere with an employee's regular work duties. Blogging from the City's systems is also subject to monitoring.
2. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the City of Cocoa and/or any of its employees or citizens. Employees are also prohibited from making any discriminatory, disparaging,

defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the City's Non-Discrimination and Anti-Harassment policy.

3. Employees may also not attribute personal statements, opinions or beliefs to the City of Cocoa when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the City. Employees assume all risk associated with blogging.
4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the City's logos and any other City intellectual property may also not be used in connection with any blogging activity

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Minimum Access Policy

**Purpose**

The City of Cocoa's Acceptable Use Policy mandates that all devices connected to City's network comply with the following requirements, referred to collectively as the Minimum Access Requirements (MAR).

Compliance with the MAR helps protect not only the individual device, but also other devices connected through the electronic communications network. The standard is intended to prevent exploitation of network resources by unauthorized individuals, including the use of City resources by unauthorized individuals to attack other systems on the City's network or the Internet.

**Scope**

This Policy applies to all devices connected to the City of Cocoa's network. An exception from the City's Chief Technology Officer is required for any configurations that do not comply with the MAR.

Questions about MAR may be directed to helpdesk@cocoafl.org.

**Policy Statements**

***Software Patch Updates***

City networked devices must only run software for which security patches are made available in a timely fashion. All currently available security patches must be applied either automatically, or on a schedule appropriate to the severity of the risk they mitigate.

***Anti-malware Software***

For Microsoft Windows or Mac OS X devices for which anti-malware software is available, anti-malware software must be running and up-to-date. In addition, the software must run real-time scanning and/or scan the device regularly.

***Host-based Firewall Software***

For Microsoft Windows, Mac OS X, or Linux/Unix devices for which host-based firewall software is available, host-based firewall software must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device. Use of a network-based firewall does not obviate the need for host-based firewalls.

***Use of Authentication***

Network services and local (console) device access must require authentication by means of passphrases or other secure authentication mechanisms unless the explicit purpose of the service/device is to provide unauthenticated access (for example: public web servers or public kiosks) and it can do so without readily allowing it to be used by attackers.

Simple devices like printers, DVR's, media extenders, network attached storage, and router/firewalls that don't support local authentication are exempt from this requirement provided that physical access is restricted. This exemption does not extend to network-facing services running on the device.

***Password/Passphrase Complexity***

When passwords and/or Passphrases are used, they must meet the following complexity specifications:

Passwords and Passphrases MUST:

- Contain at least 8 alphanumeric characters.
- Contain characters from two of the following three character classes:
    - Contain both upper and lower-case letters.
    - Contain at least one number (for example, 0-9).
    - Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/).
- Multi-user systems must be configured to enforce these complexity requirements and require that users change any pre-assigned passphrases immediately upon initial access to the account.
- All default passwords and passphrases for access to network-accessible accounts must be changed at time of network connection.
- Passwords and Passphrases must be changed every 90 days.

***No Unencrypted Authentication***

All network-based authentication must be strongly encrypted. Insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

Traffic for one-time password authentication systems is exempted from this encryption requirement.

Anonymous FTP servers or other services where authentication credentials are requested but not used are exempt from this requirement.

***No Unattended Console Sessions***

Devices must be configured to "lock" or log out and require a user to re-authenticate if left unattended for more than 30 minutes, except in the following cases:

*Devices without auto-locking/logoff capability*

Devices that do not support a configuration that automatically locks or logs off users after a specified period of time (such as network appliances and consumer electronics) may meet this standard through alternate controls, such as physical access restrictions (e.g., appliance stored in a locked office).

*Devices which are physically secured*

Devices kept in a physically secured space not accessible by unauthorized users may be exempted from this standard with the prior approval of the Chief Technology Officer.

*Kiosks and other public-use devices*
Devices configured for public use (research computers) are exempt from this requirement.

***No Unnecessary Services***
If a network service is not necessary for the intended purpose or operation of the device, that service must not be running.

***Privileged Accounts***
Privileged and super-user accounts (Administrator, root, etc.) must not be used for non-administrator activities. A secure mechanism to escalate privileges with a standard account is acceptable to meet this requirement. Network services must run under accounts assigned the minimum necessary privileges.

Devices that do not provide separate facilities for privileged or unprivileged access (e.g., some network appliances and printers with embedded operating systems) are exempt from this requirement.

***Disk Encryption***
Disk encryption is required for company owned workstations and is strongly recommended for agent owned machines. Windows built in (Bitlocker) or Mac built in (FileVault) encryption is sufficient.

**Policy Compliance**
Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Password Policy

**Purpose**

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the City of Cocoa's resources. All users, including contractors and vendors with access to City systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

**Scope**

The scope of this policy includes all personnel (including all personnel affiliated with third parties) who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of Cocoa facility, has access to the City's network, or stores any non-public City information. This policy applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local network equipment logins.

**Policy Statements**

***Password Creation***

All user-level and system-level passwords must conform to the Password Construction Guidelines.

Users must not use the same password for City of Cocoa accounts as for other non-City access (for example, personal ISP account, option trading, benefits, and so on).

Where possible, users must not use the same password for various City access needs.

User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user to access system-level privileges.

Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

All passwords must meet or exceed the following guidelines
Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters.
- Contain characters from two of the following three character classes:
    - Contain both upper and lower-case letters.
    - Contain at least one number (for example, 0-9).

- Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”.

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. (NOTE: Do not use this example as a password!)

***Passphrases***

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

All of the rules that apply to passwords also apply to passphrases.

***Password Change***

All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every 90 days. The authenticating server remembers the last ten passwords used by the users. Therefore, when prompted to change the password, the new password must not be the same as the last ten previously used passwords. This prevents the user from repeatedly using the same password after the 90-day password expiration.

In addition, the password can't be changed for the first 30 days after it has been reset. This prevents users from repeatedly changing passwords until the user is able to reuse their original password.

Password cracking or guessing may be performed on a periodic or random basis by the City of Cocoa IT Division or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to comply with the Password Policy.

***Password Protection***

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential City information.
- Passwords must not be inserted into email messages or any other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers, or family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident to the IT Division immediately and change all passwords.

An account will be locked out after three unsuccessful logon attempts with incorrect passwords. The account will be re-enabled after a period of 30 minutes. If you require immediate assistance, please call the City's IT Helpdesk (321) 433-8590.

***Application Development***

- Application developers must ensure that their programs contain the following security precautions:
- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

## Internet Acceptable Use and Filtering Policy

**Purpose**

The goals of this policy are to outline appropriate and inappropriate use of the City of Cocoa's Internet resources, including the use of browsers, electronic mail and instant messaging, file uploads and downloads, and voice communications. Use of these services is subject to the following conditions.

**Scope**

The City's Internet Acceptable Use and Filtering Policy applies to all employees, contractors, and third-party affiliates of the City of Cocoa regardless of employment status.

**Policy Statements**

Internet access at the City of Cocoa is controlled through individual accounts and passwords. Department directors are responsible for defining appropriate Internet access levels for the people in their department and conveying that information to the City's IT Division.

Each user of the City's system is required to read this Internet policy and agree to the terms of the Internet Acceptable Use and Filtering Policy prior to receiving an Internet access account and password.

***Appropriate Use***

Individuals at the City of Cocoa are encouraged to use the Internet to further the goals and objectives of the City. The types of activities that are encouraged include:

1. Communicating with fellow employees, business partners of the City, and clients within the context of an individual's assigned responsibilities;
2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and

3. Accessing cloud-based applications related to the performance of an individual's assigned responsibilities; and
4. Participating in educational or professional development activities.

The City of Cocoa IT Division will employ active Internet content filtering that will prevent access to sites deemed inappropriate for the workplace. If an authorized user needs access to a website that has been blocked, a request may be submitted to the Chief Technology Officer to be granted access to the blocked site.

***Inappropriate Use***

Individual Internet use will not interfere with others' productive use of Internet resources. Users will not violate the network policies of any network accessed through their account. Internet use at the City of Cocoa will comply with all Federal and State laws, all City policies, and all City contracts. This includes, but is not limited to, the following:

1. The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
2. The Internet may not be used in any way that violates the City's policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of the City of Cocoa, misrepresents the City, or violates any City policy is prohibited.
3. Individuals should limit their personal use of the Internet. The City allows limited personal use for communication with family and friends, independent learning, and public service. The City prohibits use for mass unsolicited mailings, access for non-employees to City resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, competitive commercial activity unless pre-approved by the City's Chief Technology Officer, and the dissemination of chain letters.
4. Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by the Chief Technology Officer.
5. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the City of Cocoa or another individual without authorized permission and in accordance with Florida's Public Records laws.
6. In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business purposes.
7. Individuals will only use City-approved services for voice communication over the Internet.

Examples of websites that may not be accessed through the City's Internet connection include, but are not limited to:

- Alcohol
- Auctions
- Ecommerce/shopping
- Gambling
- Games
- Lingerie/bikini
- Jobs/employment
- Malicious sites
- Nudity
- P2P/File sharing
- Pornography
- Radio
- Social networking
- Television

***Security***

For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the help desk to obtain a password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to Internet services.

***Monitoring and Filtering***

The City of Cocoa monitors all Internet activity occurring on the City's equipment or accounts. The City's IT Division currently employs filtering software to limit access to sites on the Internet. If the IT Division discovers activities which do not comply with applicable law, City, or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

***Disclaimer***

The City of Cocoa assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. The City is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

We encourage you to use your Internet access responsibly. Should you have any questions regarding this Internet Acceptable Use and Filtering Policy, feel free to contact the City's IT Helpdesk at helpdesk@cocoafl.org or (321) 433-8590.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or

3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Email Policy

**Purpose**

Electronic mail is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy, and security risks, thus it's important for users to understand the appropriate use of electronic communications.

The purpose of this email policy is to ensure the proper use of the City's email system and make users aware of what the City deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the City of Cocoa's Network.

**Scope**

This policy covers appropriate use of any email sent from a City of Cocoa email address (@cocoafl.org or @cocoapolice.com) and applies to all employees, vendors, and agents operating on behalf of the City of Cocoa.

**Policy Statements**

All use of email must be consistent with the City's policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper business practices.

The City's email account should be used primarily for City of Cocoa business-related purposes; personal communication is permitted on a limited basis, but non-City related commercial uses are prohibited.

Email should be retained as required by Florida's Public Records laws. In many cases, an email is considered a public record if it contains communications regarding official City of Cocoa business. The recipient of an email message is the Custodian of Record for that message and is responsible for providing the record upon request. Neither the IT Division nor the backup systems they employ are designated the custodian of record for email messages.

The City utilizes tools and appliances to backup email records for disaster recovery purposes only. Backups of the email system will be retained for a period of five years and utilized for disaster recovery purposes only and not public records retention or retrieval. It is solely the responsibility of the Custodian of Record to retain and provide public records according to the requirements of Florida's Public Records laws.

The City's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national

origin. Employees who receive any emails with this content from any City employee should report the matter to their supervisor immediately.

Users are strictly prohibited from transmitting any Criminal Justice Information (CJI) utilizing the City's email platform.

Users are prohibited from automatically forwarding City email to a third-party email system. Individual messages which are forwarded by the user must not contain confidential or above information.

Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct City of Cocoa business, to create or memorialize any binding transactions, or to store or retain email on behalf of the City. Such communications and transactions should be conducted through proper channels using City-approved documentation.

Using a reasonable amount of City resources for personal messages is acceptable, but nonwork-related email shall be saved in a separate folder from work related email. Employees are strongly encouraged to exercise good judgement when using City email for personal matters. Sending chain letters or joke emails from a City of Cocoa email account is prohibited.

City employees shall have no expectation of privacy in anything they store, send, or receive on the City's email system.

The City's IT Division may monitor messages without prior notice and reserves the right to do so at any time.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Cybersecurity Awareness and Training Policy

**Purpose**

The purpose of the Cybersecurity Awareness and Training Policy is to implement a cybersecurity awareness and training program for all City of Cocoa employees and elected officials. The City understands that "people", not necessarily technology, are often the largest threat to the security of sensitive information and our network infrastructure.

When addressing cybersecurity threats, human error is a factor that is often overlooked. It is estimated that nearly one-third of all attacks are initiated by "inadvertent actors" (employees) who accidently allow access to an attacker through phishing or other attack vectors. Although human error can never be completely eliminated, by establishing a clear cybersecurity awareness and training program, the risks posed by these attacks can be reduced.

A strong cybersecurity awareness program requires that City personnel be trained on security policies, procedures, and technical controls. All staff must have the necessary skills to carry out their assigned duties in a secure manner that protects the City from unnecessary risk.

**Scope**

This policy covers all users with a City of Cocoa email address (@cocoafl.org or @cocoapolice.com) and applies to all employees, vendors, and agents operating on behalf of the City of Cocoa.

**Policy Statements**

Technical IT security controls (firewalls, filters, intrusion detection systems, etc.) are a vital part of our cybersecurity framework but are not alone sufficient to secure all our information assets. Effective information security also requires the awareness and proactive support of all workers, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and frauds, for example, which directly target vulnerable humans rather than IT and network systems.

Lacking adequate information security awareness, workers are less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information in danger through ignorance and carelessness.

Whereas "awareness" implies a basic level of understanding about a broad range of information security matters, "training" implies more narrowly-focused and detailed attention to one or more specific topics. Training tends to be delivered through classroom or online courses, while awareness tends to be delivered by multiple communications methods such as seminars, case studies, written briefings and reference materials (for self-motivated study), posters, and conversations. Awareness provides the foundation level of knowledge and

understanding for training to build upon. In other words, cybersecurity awareness and training are complementary approaches.

In order to protect the City's valuable information, all employees must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

***Policy Details***

The City's Cybersecurity Awareness and Training Program will ensure that all workers achieve and maintain at least a basic level of understanding of cybersecurity matters, such as general obligations under various cybersecurity policies, standards, procedures, guidelines, laws, regulations, contractual terms plus generally held standards of ethics and acceptable behavior.

Cybersecurity awareness and training activities shall commence as soon as practicable after workers join the organization; initially through Cocoa Atlas and ongoing training through the City's partnership with KnowBe4. The awareness activities will continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness of current issues and challenges in this area.

Where necessary and practical, security awareness and training materials should suit their intended audiences in terms of their styles, formats, complexity, technical content etc. Everyone must understand why information security is so important.

A range of compliance measures will be undertaken to achieve widespread compliance with various cybersecurity obligations. While the details vary according to the specific nature of those obligations including the risks associated with non-compliance, the IT Division anticipates a mixture of routine, periodic and ad hoc compliance activities such as simulated phishing messages, reviews and audits, which may include checking compliance with mandatory cybersecurity awareness and training classes, awareness test results, and other metrics.

Mandatory City-wide cybersecurity awareness training classes will be conducted semi-annually and must be completed by all employees, elected officials, vendors, and agents associated with the City of Cocoa. Non-compliance with assigned training or failing a simulated phishing test four (4) or more times within a rolling 12-month period will result in suspension of the individual's email account and network access, or other disciplinary action as outlined in the Policy Compliance section below. Email account and network access will be restored upon successful completion of the assigned semi-annual or remedial training assigned.

***Responsibilities***

- The City's Chief Technology Officer is accountable for running an effective cybersecurity awareness and training program that informs and motivates workers to help protect the City's information assets, and third-party information (including personal data) in our care.

- The City's Chief Technology Officer is responsible for developing and maintaining a comprehensive suite of cybersecurity policies (including this one), standards, procedures and guidelines.
- The City's IT Helpdesk is responsible for helping workers on basic information risk, security, privacy and related matters.
- Department Directors and Division Managers are responsible for ensuring that their staff and other workers within their remit participate in the cybersecurity awareness, training, and educational activities where appropriate or mandated.
- City employees are personally accountable for complying with applicable policies, laws and regulations at all times.
- The City's IT Division is authorized to assess compliance with this and other corporate policies at any time.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 5/22/2019 | IT Division | New Policy |
| | | |

# Wireless Communication Policy

**Purpose**

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

The purpose of this policy is to secure and protect the information assets owned and/or operated by the City of Cocoa. The City provides computer devices, networks, and other electronic information systems to meet its missions, goals, and initiatives. The City grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the City of Cocoa's private wireless network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the City's Chief Technology Officer are approved for connectivity to a City of Cocoa network.

**Scope**

All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the City must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a City network or reside on a City site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, tablets, and other wireless enabled devices. This includes any form of wireless communication device capable of transmitting packet data.

**Policy Statements**

***General Requirements***

All wireless infrastructure devices that reside at a City site and connect to a City network, or provide access to City data must:

- Abide by the standards specified in the Wireless Communication Policy.
- Be installed, supported, and maintained by the City IT Division or an approved support team.
- Use City approved authentication protocols and infrastructure.
- Use City approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.
- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible

Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

***Lab and Isolated Wireless Device Requirements***

All lab wireless infrastructure devices that provide access to information classified as Confidential or above, must adhere to section above. Lab and isolated wireless devices that do not provide general network connectivity to the City of Cocoa network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity).
- Not interfere with wireless access deployments maintained by other support organizations.
- Lab device Service Set Identifier (SSID) must be different from <Company Name> production device SSID.
- Broadcast of lab device SSID must be disabled.

***Home Wireless Device Requirements***

Wireless infrastructure devices that provide direct access to the City of Cocoa network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Policy.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the City's network. Access to the City's network through this device must use standard remote access authentication.

All home wireless infrastructure devices that provide direct access to a City of Cocoa network must adhere to the following:

- Enable Wi-Fi Protected Access Pre-Shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS.
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point.
- Disable broadcast of SSID.
- Change the default SSID name.
- Change the default login and password.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including

all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Public Wireless Communication Policy

**Purpose**

The goals of this policy are to outline appropriate and inappropriate use of the City of Cocoa's public wireless Internet resources, including the use of browsers, email and instant messaging, file uploads and downloads, and media streaming (voice and video). Use of these services is subject to the following conditions.

**Scope**

This network is the property of the City of Cocoa and may be accessed only by authorized guests.

Guest wireless Internet access at the City of Cocoa is controlled through access via a captive portal. Each user of the City's public wireless system is required to read the Public Wireless Communication Policy and agree to an acceptable use agreement prior to receiving a guest wireless Internet access.

**Policy Statements**

The data you send and receive over this network is not encrypted and may be viewed or intercepted by others. Use this network at your own risk. Privacy and security safeguards are the user's responsibility; this network does not provide any. The City of Cocoa offers this service as a "best effort" offering and does not warrant or represent that this service will be uninterrupted, error-free, or secure. Users should be aware that there are security, privacy, and confidentiality risks inherent in wireless communications and technology.

The City of Cocoa may monitor any activity or retrieve any information transmitted through this network, to ensure compliance with City policy, and with federal, state, and local law. By accessing and using this network, you are consenting to such monitoring and information retrieval by the City of Cocoa. Users should have no general expectation of privacy or confidentiality when using this network.

The City of Cocoa guest wireless Internet facilities may not be used for any of the following at any time:

1. Any activities which violate local, state, or federal statutes are prohibited.
2. "Cracking/Hacking" Example: Attempting to circumvent user authentication or security of any host, network, or account on the City's systems or The Internet at large is strictly forbidden.
3. "Denial of service" attacks of any kind are forbidden. Use of the City's systems or networks (willfully or negligently) in a manner that encumbers disk space, processors, bandwidth, or other system resources so as to interfere with others' normal use of services on the City's network, or any other systems or networks is prohibited.

Attempting to knock a server off-line, slow down our connection, or knock any other user offline is prohibited.

4. Use of TCP or UDP port scanners to scan remote networks without the express written consent of that networks' administrator is prohibited.
5. Dissemination of spam and/or viruses, whether knowingly or as the result of a worm or virus on your computer, is prohibited. Attempting to send any virus or malicious material including any type of "Out of Band" packet to any other Internet user is prohibited.
6. Spamming is prohibited. Example: Sending unsolicited mass mailings of any nature, including those with an "opt-out option" for continuation. The opt-out option is inviting those who do not wish to receive more email to reply to you.
7. Mail-bombing is prohibited. Example: Sending a large number of email messages, or singularly large email messages, to a single address in order to flood someone's mailbox.
8. Forging any email header to obscure the originator of the message.
9. Creating or participating in pyramid schemes or chain letters.
10. Sending any type of harassing email, either by language, size, or frequency. This includes sending email or instant messages to any person who has asked explicitly that you do not.
11. The posting of pornographic or otherwise indecent or offending materials. The City of Cocoa is the sole arbiter of what constitutes "indecent" or "offending."
12. Unauthorized use of copyrighted or trademarked logos, phrases, or names.
13. Distribution of any software or materials in violation of any copyrights or distribution licenses. (MP3s/Warez/etc.).
14. The posting of slanderous or defamatory materials or articles.
15. Distribution of any material which violates local, state, or federal statutes.

By accessing the City of Cocoa’s public wireless network, I agree to be bound by the terms of this policy and acknowledge that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or City policy.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City’s policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Remote Access Policy

**Purpose**

Remote access to our City's network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our City's network. While these remote networks are beyond the control of the City of Cocoa's policies, we must mitigate these external risks the best of our ability.

The purpose of this policy is to define rules and requirements for connecting to the City of Cocoa's network from any host. These rules and requirements are designed to minimize the potential exposure to City from damages which may result from unauthorized use of City resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

**Scope**

This policy applies to all City of Cocoa employees, contractors, vendors, and agents with a City-owned or personally-owned computer or workstation used to connect to the City's network. This policy applies to remote access connections used to do work on behalf of the City of Cocoa, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to any City of Cocoa network.

**Policy Statements**

It is the responsibility of the City's employees, contractors, vendors and agents with remote access privileges to the City's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City of Cocoa.

General access to the City's network is strictly limited to City employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the City's network from a personal computer, Authorized Users are responsible for preventing access to any City computer resources or data by non-Authorized Users. Performance of illegal activities through the City's network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use the City's networks to access the Internet for outside business interests.

Remote access connections are granted under the terms of *Acceptable Use Policy* and *Acceptable Encryption Policy*. Remote access to the City's network will be granted by the City's Chief Technology Officer to approved City employees. Remote access is only permitted if

necessary by job function and operational need. Any remote access connection to the City must apply encryption to communications between the employee and the City and will use an encryption method contained in the *Acceptable Encryption Policy*. Each remote access connection granted will be authenticated by the following attributes:

1. Unique Active Directory Username
2. Active Directory Password
3. Unique VPN Group Name

Once authenticated, remote access employees will be permitted to access resources based on job function. The IT Division will grant access based on the employee's need. Internet access over any remote access connection for recreational use by employees is strictly prohibited and will be explicitly denied by Information Technology Internet monitoring and filtering system per the terms of the *Internet Acceptable Use and Filtering Policy*. Employees will be outfitted with the proper software necessary to create a remote access connection to the City's network. This software will be distributed to employees by the IT Division as necessary.

Personally owned devices (BYOD or Bring Your Own Device) are not allowed on the City network. All personally owned devices must connect remotely and must conform to all standards contained in the Remote Access Policy.

***Third-Party Requirements***

Remote access connections are granted under the terms of *Acceptable Use Policy* and *Acceptable Encryption Policy*. Remote access to the City's network will be granted by the City's Chief Technology Officer to approved third-parties at his/her sole discretion. Communications between a vendor or third-party and the City must always be encrypted according to the standards set forth in the *Acceptable Encryption Policy*. Third-parties will meet these encryption standards when accessing any of the City's electronic resources over the Internet or an insecure network. Prior to being granted access to the City's network, third-parties must complete the Third-Party Connection Agreement (Appendix A). In this Agreement, third parties must list the following:

1. Justification for Connectivity
2. List of electronic resources (including cellular phones), for which access is needed, including communications port names and numbers
3. Proof that third-party systems meet the encryption standards set forth in City's Acceptable Encryption Policy

Third parties who meet these requirements may be granted access to the City's electronic resources specified in the completed Third Party Connection Agreement at the Chief Technology Officer's sole discretion. Only access to required resources will be permitted; access to all other resources will be implicitly denied. Access to the permitted resources will be logged by the network management system, both at the entrance point to the City's network (firewall), and on the resources themselves.

Once a third party does not have further need for access, its connection to the City's electronic resources shall be removed. Access logs from these resources shall be maintained on the network management system to keep a full audit trail on all communications between the third-party and the associated resource.

For additional information regarding the City of Cocoa's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., please contact the IT Helpdesk at helpdesk@cocoafl.org or (321) 433-8590.

***Requirements***

1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs), https) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.
2. Authorized Users shall protect their login and password, even from family members.
3. While using a City-owned computer to remotely connect to the City's network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
4. Use of external resources to conduct City business must be approved in advance by the City's Chief Technology Officer and the appropriate Department Director.
5. All hosts that are connected to the City's internal networks via remote access technologies must use the most up-to-date anti-virus software and must be approved by the City's IT Division, this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.
6. Personal equipment used to remotely access the City's networks must meet the requirements of City-owned equipment for remote access.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or

3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Remote Access Tools Policy

**Purpose**

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems when away from the office, and vice versa. Examples of such software include TeamViewer, GotoMeeting, LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the City's network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on the City of Cocoa's computer systems.

This policy defines the requirements for remote access tools used at the City of Cocoa

**Scope**

This policy applies to all remote access where either end of the communication terminates at a City of Cocoa computer asset.

**Policy Statements**

All remote access tools used to communicate between City of Cocoa assets and other systems must comply with the following policy requirements.

***Remote Access Tools***

The City of Cocoa provides mechanisms to collaborate between internal users, with external partners, and from non-City systems. The approved software list can be obtained from the IT Helpdesk at helpdesk@cocoafl.org. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

1. All remote access tools or systems that allow communication to City resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
2. The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
3. Remote access tools must support the City's application layer proxy rather than direct connections through the perimeter firewall(s).

4. Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the City of Cocoa's Acceptable Encryption Policy.
5. All City of Cocoa antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard City of Cocoa procurement process, and the City's Chief Technology Officer must approve the purchase.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Acceptable Encryption Policy

**Purpose**

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States. This policy is designed to provide compliance with FDLE for encryption over insecure networks as well.

**Scope**

This policy applies to any City communications that are transmitted or received over insecure networks. This includes Internet communications that occur between electronic resources (including cellular phones), within Cocoa's network and other parties across the Internet, except for the following communications protocols:

- Simple Mail Transfer Protocol (SMTP)
- Hypertext Markup language (HTTP)
- Hypertext Markup language over TLS/SSL (HTTPS)
- Domain Name System (DNS)
- Internet Security Association and Key Management Protocol (ISAKMP)

This policy also includes City communications that occur between the Police Department and other sites, whereby these other sites are connected to the Police Department by way of an intermediate service provider which owns and operates the intermediary equipment. This does not apply to Internet communications originating from users at the Police Department accessing internet-based public resources.

**Policy Statements**

Any electronic communications that fall within the scope of this policy are to be encrypted using the following:

***Encryption Algorithms***

1. U.S Advanced Encryption Standard (AES) in accordance with U.S. FIPS PUB197 (256·bit keys supported).

***Digital Signature Algorithms***

1. RSA in accordance with Public Key Cryptographic Standards (PKCS) specification PKCS#1 Version 2.0, ANSI X9.31, IEEE 1363, ISO/IEC 14888-3 and U.S. FIPS PUB186-2 (1024-bit, 2048-bit, 4096-bit and 6144-bit supported).
2. DSA in accordance with the Digital Signature Standard, U.S. FIPS PUB 186-2, ANSI X9.30 Part 1, IEEE P1363 and ISO/IEC 14888-3 (1024-bit supported).

***Hash Algorithms***

1. SHA-1, SHA-2S6, SHA-384 and SHA-S12 in accordance to U.S. FIPS PUB 180-2 and ANSI X9.30 Part 2.
2. MDS Message-Digest algorithm in accordance with RFC 1321.

***Key Exchange Algorithms***

1. RSA key transfer in accordance with RFC 1421 and RFC 1423 (PEM), PKCS#1 Version 2.0, IEEE P1363.
2. Diffie-Hellman key agreement in accordance with PKCS#3.
3. SSL v3 and TLS v1.2 in accordance with RFC 2246.

***Integrity Checks***

1. HMAC in accordance with RFC 2104

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Clean Desk Policy

**Purpose**

A clean desk policy is an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase an employee's awareness about protecting sensitive information.

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers, and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

**Scope**

This policy applies to all City of Cocoa employees and affiliates.

**Policy Statements**

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down or locked at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat removable mass storage devices such as BluRay, CDROM, DVD, hard drives, or USB drives as sensitive and secure them in a locked drawer.
- All printers and fax machines should be cleared of papers as soon as they are printed.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Anti-Virus Policy

**Purpose**

The purpose of this policy is to establish standards to be met by any systems connected to the City's network to ensure effective virus prevention and detection. These standards are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of the City's resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, and damage to critical City internal systems.

**Scope**

This policy applies to all City of Cocoa employees, contractors, vendors, and agents with a City-owned or personally-owned computer or workstation used to connect to the City's network. This policy applies to remote access connections used to do work on behalf of the City of Cocoa, including reading or sending email and viewing intranet web resources.

**Policy Statements**

All computer systems defined in this policy's scope must have adequate anti-virus software installed and scheduled to run periodically. This software must also be scheduled to periodically update its virus definition files from a trusted source. Any City-owned or operated computer systems must have the City's standard anti-virus software platform installed and managed from the City's anti-virus management server. The software will receive its virus definition files from the City's management server periodically in order to keep the most current virus definitions. Any computer system defined in the scope that does not meet these standards will be denied access to the City's network. It is the responsibility of Information Technology Division to verify the anti-virus requirements of any computer system that will be connected to the City's network prior to making this connection.

All USB port connections on city assets will be disabled by Group Policy. Introduction of Virus content is very common through the use of removable storage media via the USB ports. While they are a convenient tool and increasingly so, they are also a major threat even to the most secure of networks.

Systems that are found to be infected with viruses will be immediately disconnected from the City's network and quarantined. Upon quarantine, the system will be investigated by the Information Technology Division to diagnose which virus has infected the system. Once the virus has been identified and removed from the system, it may be re-connected to the City network

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring,

remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Software Installation Policy

**Purpose**

Allowing employees to install software on City computing devices opens the organization up to unnecessary exposure. Conflicting file versions or applications can prevent programs from running properly, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on City-owned or operated equipment.

The purpose of this policy is to outline the requirements around installation software on the City's computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within City's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

**Scope**

This policy applies to all City of Cocoa employees, contractors, vendors and agents with a City-owned device. This policy covers all computers, servers, smartphones, tablets and other computing devices owned or operated by or for the City of Cocoa.

**Policy Statements**

Employees may not install software on the City's computing devices operated on the City's network.

Software requests must first be approved by the requester's manager and then be made to the Information Technology Division via the Help Desk in writing or via email.

Software must be approved and maintained by the Information Technology Division.

Only Information Technology Division employees will be granted administrative rights to install and maintain software applications. No one outside of the IT Division is permitted to install, maintain, or administer locally installed software applications.

All software purchases must be approved by the City's Chief Technology Officer and a Computer Service Request (CSR) must be completed by the requesting department and approved prior to purchase.

The Information Technology Division will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees,

contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Computer Hardware and Peripheral Installation Policy

**Purpose**

Allowing employees to install hardware on the City's network infrastructure opens the organization up to unnecessary exposure. Improper installation of computer hardware or peripherals can prevent systems from running properly, introduce the potential for hardware failure, and expose the City's network to potential security risks.

The purpose of this policy is to outline the requirements around installation of computing hardware and peripherals on the City's network infrastructure. To minimize the risk of loss of network functionality, the exposure of sensitive information contained within City's computing network, the risk of introducing malware, and the legal exposure of operating inappropriate hardware.

**Scope**

This policy applies to all City of Cocoa employees, contractors, vendors and agents with a City-owned or operated device. This policy covers all computers, servers, smartphones, tablets and other computing devices owned or operated by or for the City of Cocoa.

**Policy Statements**

Individuals covered under the scope of this policy may not install any electronic devices on the City's network.

All computing hardware or peripheral requests must first be approved by the requester's manager and then be made to the Information Technology Division via the Help Desk in writing or via email.

All computing hardware and peripherals must be approved and maintained by the Information Technology Division.

Only Information Technology Division employees are permitted to install and maintain computing hardware attached to the City's network infrastructure. No one outside of the City's IT Division is permitted to install, maintain, or administer any computing hardware or peripheral.

All computing hardware or peripheral purchases must be approved by the City's Chief Technology Officer and a Computer Service Request (CSR) must be completed and approved prior to purchase.

The Information Technology Division will obtain and install all computing hardware and peripherals.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Infrastructure Protection Policy

**Purpose**

This policy defines information security standards to be met by all electronic resources owned or operated by the City. These standards are constructed to minimize exposure to potential unauthorized access resulting in the disruption to critical electronic resource operation.

**Scope**

This policy applies to any electronic resources to which logical or physical access can be obtained. This includes digital and optical distribution frames, transmission facilities, switches, routers, firewalls, servers, backup devices, and any other electronic resource equipment not included in this list.

**Policy Statements**

Appropriate controls must be implemented to protect physical access to all electronic resources where these controls can be implemented reasonably and with an acceptable level of risk. Any electronic resource should be restricted within facilities to lockable rooms, or at the minimum, housed within lockable cabinets within common facilities. Wall-mounted cabinets may be provisioned where minimal equipment is needed. At primary facilities, those defined by hubs or data centers for City operation, separate designated rooms are required, with lockable doors and restricted access. The Chief Technology Officer may authorize exceptions to structural requirements of this policy where it is either not practical or too costly for a facility to strictly comply.

Access to equipment consoles must be restricted by password protection on router, switch, and firewall console ports and server consoles. The specifics of the password implementation are covered in detail in the Password Policy. Console adapter cables should be removed from facilities containing equipment with external console ports. This equipment includes routers, switches, and firewalls. Server consoles will be restricted by password protected screen savers. After 15 minutes of inactivity, the password protected screen saver will be started automatically by the server. Similarly, after 15 minutes of inactivity on router, switch, and firewall equipment, an auto-logout feature will be activated.

Logical access to electronic resources will be restricted in order to prevent unauthorized access from remote terminal sessions. This portion of the policy applies to router, switch, and firewall equipment. Every piece of equipment must meet the following configuration standards:

1. Local user accounts are disabled on the equipment. Routers must use RADIUS/TACACS+ for user authentication to the equipment. A single backup user account will be maintained in case of RADIUS/TACACS+ failure for backdoor authentication. This account is subject to the requirements defined in the Password Policy.
2. Any terminal lines must be password protected, according to the requirements defined in the Password Policy.

3. The enable secret password on the equipment must be kept in a secure encrypted form. The enable password will be disabled, being less secure than the enable secret password.
4. Any connection attempts to equipment will be logged to the City's network management system.
5. Computer systems connecting to the City of Cocoa network will have the following statement posted in clear view upon login:

   "I hereby acknowledge that I have read and understand the City of Cocoa's Information Technology and Cybersecurity Policies. By proceeding with the login process, I agree to abide by these policies and ensure that persons working under my supervision abide by these policies. I understand that usage of the City's systems and network are monitored, recorded, and subject to audit for administrative and security purposes. By accessing this system or network, I expressly consent to such monitoring and recording. I understand that if I violate the City's Information Technology and Cybersecurity Policies, I may face legal or disciplinary action according to applicable law or City policy.

   I hereby agree to indemnify and hold the City of Cocoa and its elected officials, officers, trustees, employees, and agents harmless for any loss, damage, expense or liability resulting from any claim, action or demand arising out of or related to the user's use of the City-owned computer resources and the network, including reasonable attorney fees. Such claims shall include, without limitation, those based on trademark or service mark infringement, trade name infringement, copyright infringement, unfair competition, defamation, unlawful discrimination or harassment, and invasion of privacy.

   All information or data stored in City of Cocoa systems or network is the property of the city and is protected and governed by the applicable laws.

   By clicking the "OK" button below, I acknowledge this system use notification statement and agree to be bound by its terms."

Access Control Mechanisms shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operation for all IT systems to:

1. Prevent multiple concurrent active sessions for a single user account.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

The Information Technology Division will identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. Appropriate service pack, patch, or hot

fixes shall promptly be installed upon identification of flaw. The following policies shall be followed regarding patch management:

1. All patches shall be tested prior to Install.
2. It must be possible to roll back a patch, update, etc.
3. Updates shall be automatic without individual user intervention.
4. Patches shall be centrally managed.
5. Patch requirements discovered during security assessments, continuous monitoring, or incident response activities shall be addressed expeditiously.

In addition to the logical access restrictions mentioned in this policy, the IT Division will also disallow:

- IP directed broadcasts
- IP traffic from all foreign states except the United States and Canada
- TCP and UDP small services
- Source routing

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Internet Perimeter Policy

**Purpose**

This policy defines information security standards to be met by all electronic resource equipment owned or operated by the City that has a connection to the public Internet. These standards are constructed to minimize exposure to Internet-based threats that may cause disruption to critical electronic resource operation, loss of sensitive information, or malicious use of the City's electronic resources.

**Scope**

This policy applies to any electronic resources owned or operated by the City that are connected to the public Internet. This encompasses switches, routers, firewalls, servers, smartphones, tablets, and computers that have connectivity to the public Internet or are connected to a De-Militarized Zone (DMZ) through which a logical connection to the public Internet is made. This policy applies to proxied connections using network address translation (NAT) and port address translation (PAT) as well.

**Policy Statements**

Appropriate controls must be implemented to protect the City's electronic resources from the threats inherent in the public Internet. Physical connectivity to the public Internet is an operational necessity for the City in its communication with citizens and among City departments. Therefore, this inherent risk must be minimized through cybersecurity policy measures, implemented on Internet-facing equipment owned or operated by the City. This equipment must be effectively secured and maintained using a combination of firewalling, filtering, intrusion detection and mitigation, and prevention.

The default Internet Perimeter policy that underlies all specific standards within this policy is to deny all inbound Internet connections to the City's electronic resources unless explicitly necessary and justifiable by an authoritative party or a business-critical communication. This position denies all access to the City's resources reachable by the public Internet. Only business-critical communications are allowed by default. Business-critical communications are defined as those that support the operation of the City, its vendors, and its affiliates in fulfillment of the City's mission. The following protocols are defined as business-critical to the City:

- Simple Mail Transfer Protocol (SMTP)
- Hypertext Markup language (HTTP)
- Hypertext Markup language over TLS/SSL (HTTPS)
- Domain Name System (DNS)
- Internet Security Association and Key Management Protocol (ISAKMP)

Protocols other than those listed above shall be denied unless proper approval is granted by the City’s Chief Technology Officer. These protocols shall be permitted for inbound access to

specific electronic resources behind the City's Internet perimeter. Protocols shall be permitted from any source host on the public Internet to one destination host only. Protocols shall be configured individually for access to the City's resources, always at the Transport Layer (Layer 4), using TCP/UDP ports, and never at Network Layer (Layer 3) IP addresses. This will provide access to only the respective applications, and never full IP access to the City's resources. The access rules that allow these business-critical communications will log matches to provide audit trail information.

In cases where communication ports other than those listed above need to be accessed, proper justification will need to be presented to the Chief Technology Officer for review. *Appendix B: Request for Access Template* provides the form that will be used to request access to a nonstandard communication port. If the Chief Technology Officer's review of the form provides justifiable cause with an acceptable level of risk, the Chief Technology Officer may grant access at his/her sole discretion. If the Chief Technology Officer's review does not provide justifiable cause, or the risk level Is unacceptable, the Chief Technology Officer will deny the request for access. The Chief Technology Officer also has the right to suggest other options for access that comply with the standards established in the *Encryption Policy*.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Firewall Policy

**Purpose**

In order to maintain a secure operating environment for computer and network resources, the City of Cocoa operates firewalls between network areas with different security postures. This policy supports effective and secure firewall management as an essential element of a layered approach to network security.

**Scope**

All employees and contractors of the City of Cocoa involved in the planning, maintenance, and operation of the City's networks are required to abide by this policy. This policy applies to all firewalls managed by the organization, including:

- Data center and DMZ firewalls
- City Hall firewalls
- Branch office firewalls
- Servers with micro-segmentation capabilities

This policy includes all hardware or software acting as a firewall, as defined in this policy, whether or not the hardware or software is generally referred to as a firewall (example: some routers and hypervisors can enable firewall capabilities).

**Policy Statements**

The City of Cocoa IT Division will manage and configure firewalls to control network traffic in a manner consistent with the security postures of the interfacing networks. Networks will be assigned a security posture based on the most sensitive asset within that network. Firewall rulesets and equipment will be standardized within the following firewall archetypes, differentiated on the basis of the requirements and security posture of the networks they separate:

- Data center and DMZ firewalls: Data center firewalls separate the data center network from a "demilitarized zone" (DMZ). DMZ firewalls separate the DMZ and data center networks from all other networks.
- Micro-segmentation firewalls: Granular, software-defined traffic controllers at the application level.
- City Hall firewalls: City Hall firewalls separate the City Hall local area network (LAN) from other internal and external networks.
- Branch office firewalls: Branch office firewalls separate branch office LANs from other internal and external networks. Branch office requirements are assumed to be homogeneous. A request for change (RFC) to a branch office firewall ruleset must demonstrate that other methods of achieving the intended business objective of the change are not feasible.

All firewalls will be configured to allow service traffic by exception (whitelisting). Specific firewall rulesets will be maintained by the Network Administrator in the City's IT Division. New firewalls will be built using standard images.

Data center firewalls will allow connections into the data center on predetermined ports and deny all other connections. All other firewalls will allow the following connections by default:

- More secure network to less secure network: Allow all connections on standard ports defined in the *Internet Perimeter Policy* and deny otherwise.
- Less secure network to more secure network: Allow connections on preapproved ports for that firewall archetype and deny otherwise.

End-user VPN connections will terminate at City Hall, branch office, or DMZ firewall.

All firewalls will be integrated to facilitate logging, correlation and alerting, auditing and compliance, and forensic analysis activities. Firewall logs will be stored and reviewed by the IT Division periodically for abnormal activity, in accordance with the *Audit Policy*. A monthly report of trends will be reviewed by the City's Chief Technology Officer. Firewall logs will be backed up and retained for a period of one year.

Firewalls will be tested and audited every two years, including capacity and penetration testing. Testing activities must be scheduled outside of normal business hours.

Exceptions to firewall rules will be assessed and approved or rejected based on a review of requirements and the security posture of networks separated by the firewall. All requests for a firewall rule change or exception must state the business objective for the change. All requests for a firewall rule change must be made through the City's Chief Technology Officer. The Chief Technology Officer will then review the requested change with the City's Senior Network Administrator for approval or denial. Their approval or denial of the requested rule change is final. Exceptions to standard rules will be clearly documented, including the business reason for the change. Firewall rule changes will be implemented by the City's Senior Network Administrator.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Audit Policy

**Purpose**

The purpose of this policy is to set forth standards by which the electronic resources of the City may be audited to ensure compliance with the City's *Information Technology and Cybersecurity Policies*. Audits will be periodically and non-periodically performed for the following reasons:

1. To ensure the integrity, confidentiality, and availability of City information and resources.
2. To investigate possible security risks and incidents to the City's electronic resources.
3. To monitor the use of the City's resources to ensure they are being appropriately used, consistent with the terms of all applicable policies contained within the *Information Technology and Cybersecurity Policies*.

**Scope**

This policy covers all electronic resources owned or operated by the City, including electronic systems, data, and communications. Parties covered by this policy include City employees, vendors, and other agencies affiliated with the City.

**Policy Statements**

The City's electronic resources are subject to audit by the City's IT Division at the discretion of the City's Chief Technology Officer. The Chief Technology Officer will develop a routine schedule whereby certain electronic resources will be audited for the purposes documented in this policy. The Chief Technology Officer will also perform non-routine, unscheduled audits of certain electronic resources to ensure compliance.

The following are the types of audits that will be performed:

***Compliance Audits***

These audits are performed to ensure the continual compliance to information security standards, dictated by the City's *Information Technology and Cybersecurity Policies*, federal, state, and local agencies. The prime objectives of these audits are to review supporting procedures and standards as they comply with approved policies, assess the efficiency and effectiveness of the City's *Information Technology and Cybersecurity Policies*, and ensure the upkeep of the City's policies to current organizational and technical changes within the City.

Compliance audits will be performed for the following policies:

- Acceptable Use Policy
- Email Policy
- Password Policy
- Anti-Virus Policy
- Clean Desk Policy

***Infrastructure Audits***

These audits are performed on the City's hardware, software, applications, databases, and other electronic resources to ensure that approved policies, procedures, and standards dictated by the City's *Information Technology and Cybersecurity Policies* are being applied in practice to the City's operations.

Infrastructure audits will be performed for the following policies:

- Infrastructure Protection Policy
- Internet Perimeter Policy
- Acceptable Encryption Policy
- Remote Access Policy
- Software Installation Policy
- Computer Hardware and Peripherals Installation Policy

***High Exposure Audits***

These audits are performed on specific areas of high exposure at a high frequency to ensure that the approved policies, procedures, and standards dictated by the City's *Information Technology and Cybersecurity Policies* remain current to federal, state, and local agency best practices for information security. High Exposure audits will be performed for the following policies:

- Internet Perimeter Policy
- Remote Access Policy

All audits will be scheduled at the discretion of the Chief Technology Officer. The schedule may be adjusted in cases where unscheduled audits need to occur within a given period. Audit work shall be documented by the IT Division as the audits are carried out. This documentation shall include the following:

- Source of information obtained
- Methodology and steps to carry out audit
- Description of findings
- Conclusions

This information shall be provided to the Chief Technology Officer for a final review after each audit has been completed. Human Resources and the appropriate department director will be notified by the Chief Technology Officer if a violation occurs.

**Policy Compliance**

The City of Cocoa IT Division reserves the right to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, remote access, business tool reports, and internal and external audits. All employees, contractors, consultants, interns, temporary, and other workers at the City of Cocoa, including all personnel affiliated with third parties that connect to a City of Cocoa network agree to be bound by the terms of this policy.

Any exception to this policy must be approved by the City's Chief Technology Officer.

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Server and Data Backup Policy

**Purpose**

Data is one of the City of Cocoa's most important assets. Data backup mechanisms help safeguard the information assets of the City of Cocoa, prevent the loss of data in case of accidental deletion or corruption of data, system failure, or disaster, and permit timely restoration of information and business processes, should such events occur.

Backup copies of the City's server and data infrastructure are for disaster recovery purposes only and not to meet Florida Public Records law records retention requirements.

**Scope**

This policy applies to all critical data in the City of Cocoa, including data outside of the City's network stored in a cloud service. "Critical data," in this context, includes email, personal and shared files, specific databases and web contents, and operating systems. The definition of critical data, and scope of this backup policy, will be reviewed periodically.

This policy applies to staff who may be creators and/or users of such data. The policy also applies to third-parties who access and use City systems and IT equipment or who create, process, or store data owned by the City of Cocoa.

This policy does not refer to backing up of data that resides on individual desktop or laptop computers, tablets, smartphones, or any other end-user device. Responsibility for backing up data on local systems rest solely with the individual user. It is strongly encouraged that end users save their data to the appropriate network server in order for their data to be backed up regularly in accordance with this policy.

**Policy Statements**

Unless otherwise noted, system data will be backed up according to the following default schedule.

***Hyperconverged Environment***

- Hourly Snapshots retained for a period of 72 hours.
- Daily snapshots retained for a period of 90 days.
- Weekly snapshots retained for a period of 1 year.

***Converged Environment***

- Hourly Snapshots retained for a period of 72 hours.
- Daily snapshots retained for a period of 90 days.
- Weekly snapshots retained for a period of 1 year.

***All Other Environments***

- Daily backups (full and/or incremental) retained for a period of 90 days.
- Weekly full backups retained for a period of 3 years.

Weekly full backups of all servers will be created locally and uploaded to an offsite cloud location for a retention period of 3 years.

Backups will be periodically verified as follows:

- Snapshot logs will be reviewed for errors on a daily basis.
- Corrective actions will be taken when errors are identified.
- Random test restorations will be performed once a week to verify backup integrity.

Restoration of accidentally deleted or corrupted information must be made through the Chief Technology Officer.

Any exceptions to this policy are at the sole discretion of the City's Chief Technology Officer.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Cybersecurity Incident Response (CSIR) Procedure

**Purpose**

This procedure introduces the City of Cocoa Cybersecurity Incident Response Team (CSIRT) and defines its roles and responsibilities in complying with the Information Security Policy for reporting of computer security violations, compromises, or incidents.

The CSIRT provides services and support to the City for preventing, handling and responding to computer security incidents and providing reactive and pro-active approaches to security incident management.

This procedure is pursuant to and in accordance with the following Federal, State, and law enforcement agency regulations and guidelines for responding to and reporting computer incidents related to City's computer security:

1. Chapter 282.318, Florida Statutes - Security of Data and Information Technology Infrastructure Act.
2. Government Information Security Reform Act, Public Law 106-398, Appendix 114 Stat. 1654A-269.
3. Health Insurance Portability and Accountability Act (HIPAA), Public Law 104- 191, Section 1171(6).
4. Health Insurance Reform: Security Standards; Final Rule. Chapter 164.308(a)(6)(ii).
5. Florida Department of Law Enforcement (FDLE) - The Florida Computer Crime Center (FC3).

**Scope**

This policy covers all electronic resources owned or operated by the City, including electronic systems, data, and communications. Parties covered by this policy include City employees, vendors, and other agencies affiliated with the City.

**Procedure**

The CSIRT works to prevent the occurrence of security incidents, is the initial respondent to any incidents that occur, analyzes incidents, establishes resolution and procedures to prevent future occurrences, and make reports to local and state agencies, as required.

***Team Members***

The core team is comprised of the Chief Technology Officer, Senior Network Administrator, the System Administrator, and the Technical Services Supervisor. In addition to the core members who provide leadership and direction, support members in the following areas will be included as the incident warrants: law enforcement, administration, human resources, and information technology functional specialists.

***Team Leadership and Duties***

The Team Leader for the City is the Chief Technology Officer. The Team Leader has management responsibility for activities of the CSIRT, except the authority to convene an investigation. The Team Leader will perform the following duties:

- Ensure that the IR staff Is trained in proper CSIR procedures.
- Convene the CSIRT at regular intervals.
- Contact the City Manager's Office.
- Conduct meetings of the CSIRT.
- Report periodically status of incidents to the City Manager's Office.
- Manage Class 1 incidents.
- Manage Class 2 incidents.
- Ensure necessary information regarding Class 2 and Class 3 incidents is reported to the City Manager's Office.
- Coordinate non-investigative team activities.
- Conduct a debriefing of lessons learned and report to the City Manager's Office.

***CSIRT Roles, Responsibilities and Duties***

*Role of the CSIRT*

The CSIRT is a first responder to security incidents which affect the City. The team performs vital functions in regards to mitigating and investigating an apparent information security incident to minimize damage to the City's computer systems, network and data. The role of the CSIRT is to respond rapidly to any suspected security incident by identifying and controlling the suspected incident, notifying users of the proper procedures to preserve evidence, and reporting ail findings to management.

*Responsibilities of the CSIRT*

- Report Incidents to the City Manager.
- Convene as required upon notification of a reported computer security incident.
- Respond to activities that might interrupt the network services to any part of the City.
- Assist with recovery efforts, document incidents, and provide regular reports to the City Manager's Office.
- Classify City security incidents.
- Maintain awareness of and Implement procedures for effective response to computer security incidents.
- Stay current on functional and security operations for the technologies within their area of responsibility.
- Select additional support members as necessary for the reported incidents.

*Duties of the CSIRT*

The CSIRT does not make policy decisions or take action following an investigation. It receives its direction from and is accountable directly to the City Manager's Office. All investigations activities will be performed by local law enforcement.

Duties include:

- Conduct a preliminary assessment to determine the root cause, source, nature, extent of damage and recommended response to a computer security incident.
- Manage the release of information to the City Manager's Office for eventual media consumption.
- Prepare a report of findings, root causes, lessons learned, and recommended actions for management review.
- Carry out directions of management communicated through the City Manager's Office.
- Formalize the CSIRT process in accordance with City's guidelines.

***Computer Security Incident Classifications***

1. *Identifying Computer Security Incidents - General*
   A computer security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the City's information system.
2. *Identifying Computer Security Incidents - HIPPA Related*
   If in the course of duty, a member of the Information Technology team or another person using the City's computer systems, e.g., Finance, Human Resources, is accidentally exposed to any individual's health information in accordance with HIPPA, then that incident is classified a Class 1. If the exposure is intentional, whether successful or attempted, then that Incident is classified a Class 2.
3. *Notification of Security Incidents - CJIS Related*
   Any security Incidents involving CJIS information or the CPD network are automatically classified as Class 2 and the FDLE CJIS ISO, FDLE Customer Support Center, or the FDLE Network Administrator shall be notified.
4. *Notification of Security Incidents*
   Successful incident handling requires that employees be able to report incidents in a convenient, straight forward fashion. At the City all incidents are to be reported to the Helpdesk for subsequent reporting to the Chief Technology Officer/CSIRT Leader.
5. *Classification of Security Incidents*
   It is the responsibility of the CSIRT to classify security incidents into three classes based on the severity of the incident: Class 1, Class 2 and Class 3.
   a. Class 1 incidents: are localized to one computer, minor, and may not require full CSIRT involvement or completion of a CSIR form. This type of incident will be reviewed by the appropriate staff as determined by the Chief Technology Officer.

The Chief Technology Officer/CSIRT Leader may escalate a Class 1 incident to a Class 2 incident if deemed appropriate.

Examples of Class 1 incidents are:

- Localized virus attacks not detected and removed by security systems.
- Accidental exposure to HIPPA information.
- Internet abuse, excluding criminal behavior.
- Incidents traceable to end user error or system failure.
- Minor attempts at intrusion, scanning or pinging.
- Missing IT devices or equipment.
- Theft of IT devices.
- Proactive detection of possible email abuse, fraud, phishing or covert information gathering.

b. Class 2 incidents: are localized to two or more computers in the City's network, high Impact, and require full CSIRT involvement, completion of a CSIR form, reporting to the CDCIR, for determination of escalation, assistance, and the need to report the incident to other agencies.

Examples of Class 2 incidents are:

- Coordinated, distributed attacks.
- Intentionally, successful, or attempted access to HIPPA information.
- Any attacks which cause Denial of Service (DOS).
- Financial fraud involving computers.
- Unauthorized activity involving any sensitive systems (Superion, Tyler, Kronos, etc.).
- Internet abuses which violate Local, Federal or State law.
- Web Defacement.
- Customer data compromised.

c. Class 3 incidents: are Class 1 or Class 2 Incidents reported to the CDCIR and classified as having an enterprise wide Impact and extends to entities outside of the City's network.

6. *Escalation Process- Classification of Security Incidents*

An incident may be escalated from a Class 1 to a Class 2 in any of the following ways:

- Decision of the CSIR Team Leader or designee.
- Determination of Chief Technology Officer.
- Additional related events, i.e., emergence of a distributed, coordinated attack.
- Request by the City Manager.

The escalation and the reason for the escalation must be documented as part of the process.

***Investigative Process***

Upon receipt of a Class2 or Class 3 incident for investigation from the CSIRT, the Chief Technology Officer, or the City Manager, the Cocoa Police Department (CPD), General Crime Unit shall be notified. The CPD will conduct and coordinate investigative activities. If the incident warrants, the CPD will notify FDLE (Florida Department of Law Enforcement) or other appropriate law enforcement agencies. In cases where the incident has been referred to law enforcement, the CSIRT will continue to assist and coordinate where necessary and advisable, but not to compromise or impede the criminal investigation. Additionally, when an incident has been referred, the CSIRT will receive its direction from law enforcement and assume primarily a support role.

Once CSIRT has referred an incident for investigation to law enforcement, a formal investigative process will be used. The process will be appropriate to the incident, consistent with law enforcement investigative procedures, and conducted in accordance with industry standards. All investigators or those providing technical expertise and assistance to law enforcement investigators will contemporaneously and thoroughly document their actions and findings and retain said documentation for future use, i.e., as a witness in either administrative litigation or criminal proceeding and submit a copy to the law enforcement agency lead investigator for retention in the case file and for use in preparing the final report. Additionally, in conducting the investigation, the law enforcement agency will collect, maintain, and preserve all evidence in accordance with State records retention schedules.

***Report Process***

A Cybersecurity Incident Reporting Form (Appendix C) must be completed by the CSIRT for all Class 2 and Class 3 incidents. All Class 2 and 3 incidents must be reported to the City Manager's Office by the Chief Technology Officer. All completed forms must be maintained and filed by the CSIRT leader for three (3) years or until legal action (if warranted) is complete.

The CSIRT is responsible for reporting their findings to the City Manager's Office at the conclusion of an incident. This report should include the following:

1. *Executive summary* - include a description of the incident, methods of investigation and general conclusion.
2. *Detailed conclusions* - include one section for each conclusion drawn by the CSIRT. These sections describe how the CSIRT arrived at the conclusion, list exculpatory evidence that may prove contradictory, provide evidence that support the conclusion, and log entries that can show a chain of events that support the CSIRT's conclusion.
3. *Recommendations* - the report should conclude with the CSIRT's recommendation for avoidance of future or repeat incidents.

***Emergency/Disaster Management (EDM) Plan***

Incident handling by the City's CSIRT is closely related to EDM planning as well as support and operations. The CSIRT may be viewed as a component of contingency planning because it provides the ability to react quickly and efficiently to disruptions in normal processing.

**Policy Compliance**

Violations of this policy will be treated like other allegations of wrongdoing at the City of Cocoa. Allegations of misconduct will be handled according to established City procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable the City's policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements;
4. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.

**Revision History**

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 10/1/2018 | IT Division | New Policy |
| | | |

# Appendix A: Third-Party Connection Agreement

## CITY OF COCOA

## THIRD-PARTY CONNECTION AGREEMENT

This Third-Party Connection Agreement by and between the City of Cocoa, a Florida corporation, with principal offices at 65 Stone Street, Cocoa, FL 32922, ("City") and _____ _____, a business partner with principal offices at _____ _____ ("Company") is entered into as of the date last written below ("the Effective Date").

This Agreement consists of this signature page and the following attachments that are incorporated in this Agreement by this reference:

1. Attachment 1: Terms and Conditions
2. Attachment 2: Third Party Connection Request
3. Attachment 3: City of Cocoa Connection Methods

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by the laws of the State of Florida without regard to choice of law provisions.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

| | *City of Cocoa* |
|---|---|
| Partner | City |
| Partner Authorized Signature | Chief Technology Officer Signature |
| Name | Name |
| Date | Date |

**Attachment 1**
**THIRD-PARTY CONNECTION AGREEMENT**
**TERMS AND CONDITIONS**

**Statement of Purpose**: To ensure that a secure method of connectivity is provided between City and Business Partner and to provide guidelines for the use of network and computing resources associated with the Connection as defined below.

**Definitions**: "Connection" means one of the City connectivity options listed in the Third-Party Connection Methods.

1. *Right to Use Connection*. Business Partner may only use the Connection for business purposes as outlined by Attachment 3: Third Party Connection Request.
2. *Network Security*. Business Partners will allow only employees approved in advance by City ("Authorized Company Employees") to access the Connection. Business Partners shall be solely responsible for ensuring that Authorized Employees are not security risks, and upon City's request, Partner will provide City with any information reasonably necessary for City to evaluate security issues relating to any Authorized Partner Employee.

   Partner will promptly notify City whenever any Authorized Employee leaves Partner's employ or no longer requires access to the Connection.

   Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the Connection is secure and is used only for authorized purposes, and (b) such party's business records and data are protected against improper access, use, loss alteration or destruction.
3. *Notifications*. Partner shall notify City in writing promptly upon a change in the user base for the work performed over the Connection or whenever in Partner's opinion a change in the connection and/or functional requirements of the Connection is necessary.
4. *Payment of Costs*. Each party will be responsible for all costs incurred by that party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Connection.
5. *Disclaimer of Warranties*. Neither Party makes any warranties, expressed or implied, concerning any subject matter of this Agreement, including, but not limited to, any implied warranties of merchantability and fitness for a particular purpose.
6. *Limitation of Liability*. Except with respect to a party's confidentiality obligations under this Agreement, in no event will either party be liable to the other party for any special, indirect, incidental, punitive or consequential damages (including loss of use, data, business or profits) arising out of or in connection with this Agreement, including without limitation, any damages resulting from any delay, omission or error in the

electronic transmission or receipt of data pursuant to this Agreement, whether such liability arising from any claim based upon contract, warranty, Tort (including negligence), product liability or otherwise, and whether or not a party has been advised of the possibility of such loss or damage.

7. *Confidentiality*. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the others technology and products that is confidential and of substantial value to that party, which value would be impaired if such information were disclosed to third parties ("Confidential Information"). Should such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure. Each party agrees that it will not use in any way for its own account, except as provided herein, nor disclose to any third party, any such Confidential Information revealed to it by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information. Upon request by the receiving party, the disclosing party shall advise whether it considers any information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly, each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information. The receiving party's obligation of confidentiality shall not apply to information that: (a) is already known to the receiving party or is publicly available at the time of disclosure; (b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or (c) becomes publicly available after disclosure through no fault of the receiving party.
8. *Term, Termination, and Survival*. This Agreement will remain in effect until terminated by either party. Either party may terminate this agreement for convenience by providing written notice in email or paper correspondence, which notice will specify the effective date of termination. Either party may also terminate this Agreement immediately upon the other party's breach of this Agreement. Sections 5, 6, 7, and 8 shall survive any termination of this Agreement.
9. *Miscellaneous*.
    - Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.
    - Waiver. The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

- Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.
- Force Majeure. Neither party will be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

**Attachment 2**
**THIRD-PARTY CONNECTION AGREEMENT**
**THIRD-PARTY CONNECTION REQUEST**

In accordance with the Third-Party Connection Policy, all requests for third-party connections must be accompanied by this completed Third Party Connection Request. This document should be completed by the third-party requesting a connection and the Information Technology staff members working with the third-party requesting the Connection.

| | |
|---|---|
| **Third-Party Company Name** | |
| **Contact Name** | |
| **Contact Phone Number** | |
| **Contact Email Address** | |
| **Public Source IP Address or Subnet** | |
| **Existing Connections with Cocoa** | |
| **Executed Non-Disclosure in Place** | |
| **Anti-virus Installed on Client Device** | |
| **Date of Last Update of Anti-virus** | |
| **Personal firewall Activated on Client** | |
| **Drive Encryption Activated on Client** | |
| **Affiliation to Cocoa** | |
| **Names or Count of Third-Party Employees Using Connection** | |
| **Purpose of Connection and Business Need** | |
| **City Resources to be Accessed** | |

| | |
|---|---|
| **Length of Time Connection will be Active and Expiration Date of Connection** | |

**Attachment 3**
**THIRD-PARTY CONNECTION AGREEMENT**
**THIRD-PARTY CONNECTION METHODS**

In accordance with the Third-Party Connection Policy and the Acceptable Encryption Policy, any third-party connection made by a third-party to the City shall use the following standards. For remote access Connections, in which a single computer system is accessing the City's network, the following standards shall be used:

***Encryption Algorithms***

1. U.S Advanced Encryption Standard (AES) in accordance with U.S. FIPS PUB197 (256·bit keys supported).

***Hash Algorithms***

1. SHA-1, SHA-2S6, SHA-384 and SHA-S12 in accordance to U.S. FIPS PUB 180-2 and ANSI X9.30 Part 2.
2. MDS Message-Digest algorithm in accordance with RFC 1321.

***Key Exchange Algorithms***

1. RSA key transfer in accordance with RFC 1421 and RFC 1423 (PEM), PKCS#1 Version 2.0, IEEE P1363.
2. Diffie-Hellman key agreement in accordance with PKCS#3.
3. SSL v3 and TLS v1.2 in accordance with RFC 2246.

***Key Composition***

1. Strong Password/Passphrase Required

For site-to-site Connections, in which a dedicated IPSec termination device is maintained by Company and a dedicated IPSec termination device is owned or operated by City, the following standards shall be used:

***Encryption Algorithms***

1. U.S Advanced Encryption Standard (AES) in accordance with U.S. FIPS PUB197 (256·bit keys supported).

***Hash Algorithms***

1. SHA-1, SHA-2S6, SHA-384 and SHA-S12 in accordance to U.S. FIPS PUB 180-2 and ANSI X9.30 Part 2.
2. MDS Message-Digest algorithm in accordance with RFC 1321.

***Key Exchange Algorithms***

1. RSA key transfer in accordance with RFC 1421 and RFC 1423 (PEM), PKCS#1 Version 2.0, IEEE P1363.

2. Diffie-Hellman key agreement in accordance with PKCS#3.
3. SSL v3 and TLS v1.2 in accordance with RFC 2246.

***Key Composition***

1. Strong Password/Passphrase Required

## Appendix B: Request for Access Template

This template is used as an accompaniment to the Third-Party Connection Agreement for any access required by third-parties that cannot comply with the City's Third-Party Connection Policy, Acceptable Encryption Policy, and Internet Perimeter Policy. This Appendix is used in cases where third-parties, for technical reasons, cannot comply with these policy requirements, but require access for a business need. This template will be completed with the accompanying Third-Party Connection Agreement for review by the City's Chief Technology Officer. The Chief Technology Officer will review the Third-Party Connection Agreement with the completed Request for Access Template and determine if the business need justifies the risk associated with fulfilling the third-party's Connection. It is at the sole and exclusive discretion of the Chief Technology Officer to accept or reject the Request for Access. This template is to be completed by the third-party and the Information Technology staff working directly with the third-party.

| | |
|---|---|
| **City Department Working with Third-Party** | |
| **Reasons the Third-Party Cannot Comply with City's Policies** | |
| **Connection Options Supported by Third-Party** | |
| **Can the City Accommodate the Third-Party Connection Options** | |
| **Technical Steps Needed for City to Accommodate Third-Party Connection Option and Grant Access** | |
| **Business Justification** | |

# Appendix C: Cybersecurity Incident Report Form

**CYBER SECURITY INCIDENT REPORT FORM**

| **TIME/DURATION** | |
|---|---|
| Incident/Issue Number: | |
| Type: (see definitions) | |
| Level: (see definitions) | |
| Class: (see definitions) | |
| Date/Time Incident Occurred: | |
| Date/Time Incident Discovered: | |
| Date/Time Incident Reported: | |
| **SECTION 1 – REPORTING PARTY/INDIVIDUAL INFORMATION** | |
| Organization: | |
| Contact Name: | |
| Department/Division: | |
| Telephone Number: | |
| E-mail Address: | |
| **SECTION 2 – TARGET ORGANIZATION** | |
| Organization: | |
| Resource: | |
| Contact Name: | |
| Department/Division: | |
| Telephone Number: | |
| E-mail Address: | |
| **SECTION 3 – TARGET SYSTEM** | |
| Target(s) Owner's Name: | |
| Target(s) Owner's Position/Title: | |
| Target(s) Supervisor Phone: | |
| Target(s) Supervisor Division: | |
| Target(s) IP Address: | |
| Target(s) DNS Name: | |
| Target(s) NetBIOS Name: | |
| Target(s) Level of Information Compromised: | |
| Target(s) Operating System: | |
| Target(s) Storage Device or Backup: | |
| Target(s) Evidence Preservation Step: | |

| | |
|---|---|
| Target(s) Actively Compromised: | |
| Target(s) on DHCP: | |
| Target(s) System Classification (server, web application, end-user host, database, etc.): | |
| Target(s) application system name: | |
| Target(s) internet accessibility: | |
| Target(s) impact on City business: | |
| Target(s) criticality: | |
| Target(s) contains confidential data: | |
| **SECTION 4 – SOURCE** | |
| Source(s) IP: | |
| Source(s) DNS name: | |
| Source(s) NetBIOS name: | |
| Source(s) name and address: | |
| Source(s) Internet service provider: | |
| Source(s) location: | |
| Source(s) Agency, Company, or ISP notified: | |
| **SECTION 5 – INCIDENT/INTRUSION SUMMARY** | |
| Type of incident or attack: | |
| Method of detection: | |
| Description of incident or attack: | |
| **SECTION 6 – INCIDENT/INTRUSION DETAILS** | |
| Was system compromised: | |
| Impact on operation: | |
| Is active attack currently on-going: | |
| Exploited vulnerability description (MS or CVE Number): | |
| Suspicion of Root-Kit or Key-Logger compromise: | |
| Any domain credentials or other passwords potentially | |

| | |
|---|---|
| discovered from compromised system: | |
| Has comprised system used as a staging point for deeper attacks: | |
| Length of time system may have been compromised: | |
| Origin of attacks, Inside/Outside: | |
| **SECTION 7 – LAW ENFORCEMENT INVOLVEMENT** | |
| Chain of custody issues: | |
| Preservation of evidence: | |
| Machine powered off at time of or after compromise discovery: | |
| Management authorization for passing investigation and evidence to law enforcement agents or investigation: | |
| Decision to perform live or offline forensics: | |
| Can this system be taken offline for evidence without impacting business operation: | |
| Failover/Backup for continuous operation during offline during investigation or evidence storage: | |
| Investigation log or journal chronological detailing procedure and steps of investigation and evidence collection: | |
| Screen shots of investigation or system tools results or outputs: | |
| Cryptographic Hash made of gathered logs, documents containing screenshots, text outputs (e.g., netstat, directory listing, and task list), etc.: | |

| SECTION 8 – NOTIFICATION: INTERNAL | |
|---|---|
| City Manager: | |
| Chief Technology Officer: | |
| Police Department: | |
| Finance Department: | |
| Human Resources Division: | |
| **SECTION 9 – NOTIFICATIONS: EXTERNAL** | |
| City Attorney's Office: | |
| FDLE: | |
| FBI: | |
| DHS: | |
| MS-ISAC and/or Water-ISAC: | |
| Other: | |

| INCIDENT TYPE | | | |
|---|---|---|---|
| **CAT** | **DEFINITION** | **CAT** | **DEFINITION** |
| 1 | Theft or loss of data device | 6 | Unauthorized Probe/Information Gathering |
| 2 | Unauthorized Root or User access | 7 | Virus/Trojan/Worm/Malicious Code/Malware |
| 3 | Confidentiality of Information | 8 | System Misuse |
| 4 | Denial of Service | 9 | Rogue Access Point (Wireless) |
| 5 | Web Defacement | 10 | Miscellaneous |

| INCIDENT CLASS | | |
|---|---|---|
| **CLASS** | **SCOPE** | **IMPACT** |
| 1 | Local Agency | Low |
| 2 | Local Agency | High |
| 3 | Interagency | Critical |

| INCIDENT LEVEL | | |
|---|---|---|
| **LEVEL** | **GENERIC** | **SPECIFIC** |
| 1 | Public | |
| 2 | Confidential | |
| 3 | Confidential | HIPPA (Patient Health Info) |
| 4 | Confidential | FDLE (Florida Department of Law Enforcement) |
| 5 | Confidential | PCI (Payment Card Industry) |