Requested by: Information Technology
Prepared by: City Clerk's office

**RESOLUTION NO. 2020-06**

**A RESOLUTION OF THE CITY OF VENICE, FLORIDA ADOPTING A CYBERSECURITY POLICY; AND PROVIDING FOR AN EFFECTIVE DATE**

**WHEREAS**, the City of Venice, Florida ("the City") adopted an Information Technology Usage Policy in 2018 to provide effective guidelines and rules to maintain information technology resources in a consistent, predictable, and reliable manner; and

**WHEREAS**, the City considers the protection and integrity of technology assets owned and leased by the City to be of utmost importance to City staff; and

**WHEREAS**, cybersecurity initiatives are particularly designed and needed to aid in the protection and integrity of technology assets; and

**WHEREAS**, an addition of a Cybersecurity Policy to support the existing Information Technology Usage Policy provides effective guidelines and rules to maintain these resources in a consistent, predictable, and reliable manner to serve the city as business communication tools.

**NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF VENICE, FLORIDA, as follows:**

**SECTION 1.** The above Whereas clauses are ratified and confirmed as true and correct.

**SECTION 2.** The Cybersecurity Policy attached hereto as Exhibit "A", is hereby adopted and incorporated by reference as though fully set out in this resolution.

**SECTION 3.** A copy of the Cybersecurity Policy shall be maintained for public use, inspection and examination in the offices of the city clerk and the information systems department and will be provided to all users.

**SECTION 4.** This Resolution shall take effect immediately upon its approval and adoption as required by law.

**APPROVED AND ADOPTED AT A REGULAR MEETING OF THE VENICE CITY COUNCIL HELD ON THE 10TH DAY OF MARCH 2020.**

_____
Ron Feinsod, Mayor

ATTEST:

_____
Lori Stelzer, MMC, City Clerk

I, Lori Stelzer, MMC, City Clerk of the City of Venice, Florida, a municipal corporation in Sarasota County, Florida, do hereby certify that the foregoing is a full and complete, true and correct copy of a Resolution duly adopted by the City Council of the City of Venice, Florida, at a meeting thereof duly convened and held on the 10th day of March 2020, a quorum being present.

WITNESS my hand and official seal of said City this 10th day of March 2020.

_____
Lori Stelzer, MMC, City Clerk

(S E A L)

Approved as to form:

_____
Kelly Fernandez, City Attorney

# City of Venice

# Cybersecurity Policy

Cybersecurity awareness has been identified by the National Security Agency (NSA) of the United States of America as a threat against entities both public and private. The evolvement of security threats from the infection of a computer virus to the hacking of data for ransom (Ransomware), has required agencies to heighten their efforts to protect users and electronic assets.

Cybersecurity attacks have crippled the ability of public and private agencies from being able to conduct business, provide public services such as responding to 9-1-1 calls, and monitor health and other life safety systems. These attacks can be directed towards the organization and/or the individual (employee) with malicious intentions in their attempts to infiltrate City systems or obtain login information. Those who infect computer systems seek a financial payout, regardless of the harm or damage caused to resources, both human and electronic.

The City considers Information Technology (IT) resources to be City resources. It shall be the policy of the City to maintain these resources in a consistent, predictable, and reliable manner to serve the City as business communication tools. It is imperative to protect City resources from violations of HIPPA, unauthorized release (or theft) of Personal Health Information (PHI), and the protection of Criminal Justice Information (CJI). All users of these IT resources are expected to conduct themselves in a responsible, efficient, professional, and ethical manner and in accordance with city policies, as well as federal, state, and local laws.

## 1. Purpose

The purpose of this policy is to accompany and enhance the current City of Venice IT Usage Policy through additional criteria as they relate to cybersecurity and the protection of network and computer resources. The City authorizes the use of computing and network resources by City employees and authorized contractors in connection with the transaction of official business of the City. All use must be consistent with the intent and requirements of all city policies and must be carried out in an ethical, legal, and responsible manner.

Users of the City IT resources should have no expectation of privacy while using city-owned or city-leased equipment. Information passing through or stored on city equipment can and will be monitored.

This policy also describes the user's responsibilities, informs users (employees, contractors, and other authorized users) of their obligatory requirements for protecting the technology and information assets belonging to the City of Venice, and contains procedures for responding to incidents that threaten the security of the technology and information assets belonging to the City of Venice.

## 2. Definitions

**Externally accessible to public.** Non-employees can access the system via the Internet without a logon ID or password. The system may be accessed via a communication method without providing a logon ID or password. It is possible to access the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.

**Non-Public, Externally accessible.** Users of the system must have a valid authentication credential. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet. A private file transfer protocol (FTP) server used to exchange files with business partners is an example of this type of system.

**Internally accessible only.** Users of the system must have a valid authentication credential. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and is not accessible from the Internet. A private intranet Web Server is an example of this type of system.

**Chief Information Officer (CIO).** The Director of the Department of Information Technology (IT) shall serve as the Chief Information Officer.

**Health Insurance Portability and Accountability Act (HIPPA).** This privacy rule establishes national standards to protect individuals' medical records and other personal health information. It was subsequently modified with the HITECH Act. HITECH incorporated the requirement for technology safeguards in accordance to HIPPA information. Violations of these acts include fines for the organization, to be levied by the Department of Health and Human Services.

**Personal Health Information (PHI).** This is the personal health information of patients that is to be protected through the implementation of HIPPA and the HITECH Act.

**Criminal Justice Information (CJI).** This sensitive information, shared between the FBI, state and local law enforcement agencies, may contain fingerprints, criminal background information, and any other information that may be classified as private. Violations of CJI (authorized access or theft) could result in the Florida Department of Law Enforcement (FDLE) levying fines against the City of Venice or revoking the City's access to the national CJIS (Criminal Justice Information System).

**Security Administrator.** An employee of IT shall be designated by the CIO as the Security Administrator for the City of Venice.

**System.** A device or collection of devices utilized to perform a set of tasks such as transmitting data/information from one point to another point. A system may be a 9-1-1 call system, a utility billing system, an e-mail system, permitting system, or another electronic communications system.

## 3. What Are We Protecting

It is the obligation of all users to protect the technology and information assets belonging to the City. This information must be protected from ransom, destruction, unauthorized access, and theft. Technology and information assets include computer hardware, software, and the data generated through or on those devices. Systems may be classified to a security level based on the type of information they store or are used to convey.

## 4. Classifications of Systems

| Security Level | Description | Example |
|---|---|---|
| RED | This system contains confidential information – information that cannot be revealed to personnel outside the City. Even within the City, access to this information is provided on a "need to know" basis.<br><br>The system provides mission-critical services vital to the operation of the City. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the City. | Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information. |
| GREEN | This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network. | User department PCs used to access Server and application(s). Management workstations used by systems and network administrators. |
| WHITE | This system is not externally accessible. It is on an isolated network segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services. | A test system used by system designers and programmers to develop new computer systems. |

| | | |
|---|---|---|
| BLACK | This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information. | A public Web server with non-sensitive information. |

## 5. Threats To Security

One of the biggest security threats is interactive computer use and breaches associated with interactive computer use. For the purposes of this policy, interactive computer use is defined as use of a computing device by a City employee, contractor, guest, or other authorized user. Steps to be taken to minimize threats to security are outlined below, however this is not a comprehensive list.

a. Employ least privilege security—a user will have the network and computer security privileges needed to perform their daily tasks.
b. Network and computer login account access will not be shared.
c. Remove access to systems when employees are separated from employment.
d. Physically secure computer assets so that only staff with appropriate need can access.

## 6. Hackers and Vandals

a) Amateurs are the most common type on the Internet and represent a high probability of attack. These people take advantage of crimes of opportunity and routinely scan networks and the Internet for vulnerabilities to exploit.
b) Criminal hackers and saboteurs represent a low probability of attack as they are trained.
c) Nation-State are individual hackers or teams of hackers, often from a military or other government institution, with vast resources, that can target governments, businesses, and financial institutions.

## 7. User Classification

| **User Category** | **Privileges & Responsibilities** |
|---|---|
| Department Users (Employees) | Access to application and databases as required for job function. (RED and/or GREEN and/or WHITE and/or BLACK cleared) |
| System Administrators | Access to computer systems, routers, hubs, and other infrastructure technology required |

| | |
|---|---|
| | for job function. Access to confidential information on a "need to know" basis only. |
| Security Administrator | Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function. |
| Systems Analyst/Programmer | Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices. |
| Contractors/Consultants | Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by the CIO. |
| Other Agencies and Business Partners | Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws. |
| General Public | Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information. |

**8. Monitoring Use of Computer Systems**

The City has the right and capability to monitor electronic information created and/or communicated by persons using City computer systems and networks, including e-mail messages and usage of the Internet. It is not the policy or intent to continuously monitor all computer usage by employees or other users of the computer systems and network. However, users of the systems should be aware that the City may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, online length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with the City of Venice IT Usage Policy.

**9. User Security Testing**

At random intervals, users of the network may be tested through various means, including e-mail, social engineering, and phone calls, to remind users of potential network security threats. Security threats harm the network and its resources and can cause the City's information to be held hostage for ransom.

**10. Use of the City's Network and/or its Electronic Assets**

Users of the City's network and/or its electronic assets shall avoid opening attachments or clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")

Users of the City's network and/or its electronic assets shall be suspicious of clickbait titles (e.g. offering prizes, advice) from external sources to the City of Venice.

Users of the City's network and/or its electronic assets shall check e-mail and names of people they receive a message from to ensure that the e-mail is legitimate (read the sender's e-mail address…does it say a City employee's name with a Gmail account, for example).

Users of the City's network and/or its electronic assets shall look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, and excessive number of exclamation marks.)

Users of the City's network and/or its electronic assets shall avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary.

Users of the City's network and/or its electronic assets shall ensure that the recipients of the transferred data are properly authorized people or organizations.

Users of the City's network and/or its electronic assets shall avoid accessing suspicious websites.

**11. Access Control**

A fundamental component of this policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. Access control exists at multiple layers and may be implemented through one or more means that may include the use of a logon ID, password, passphrase, security token, and/or biometric device.

**12. Connecting Devices to the Network**

Only authorized devices may be connected to the City's network(s). Authorized devices include PCs and workstations owned by the City that comply with the configuration guidelines of the City. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach non-company computers that are not authorized, owned and/or controlled by the City to the network.

**13. Security Incident Handling Procedures**

The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the City of Venice's computer network. Some examples of security incidents are:

- Illegal access to the City's computer system. For example, a hacker logs onto a production server and copies or destroys data. The hacker may also implement software to encrypt the data and thus hold the information hostage, demanding payment for unencrypting of the data.
- Damage to a City computer system or network caused by illegal access. Releasing a virus or worm would be an example of damage.
- Denial of service attack against a City server. For example, a hacker initiates a flood of packets against a City server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computers outside of the City's network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees who believe their technology device or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the CIO or Security Administrator immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem. An affected or infected device may be permanently removed.

**14. Policy Violations**

Violations of this policy will be handled in accordance with the Policy Violations section of the city of Venice IT Usage Policy.