**RESOLUTION 21-194**

**A RESOLUTION OF THE CITY OF PANAMA CITY BEACH, FLORIDA, ADOPTING INFORMATION TECHNOLOGY (IT) SECURITY POLICIES.**

**BE IT RESOLVED** by the City Council of the City of Panama City Beach that the IT Security Policies attached and incorporated herein as Exhibit A to this Resolution are hereby adopted and approved.

**THIS RESOLUTION** shall be effective immediately upon passage.

**PASSED** in regular session this 22nd day of July, 2021.

**CITY OF PANAMA CITY BEACH**

By: _____
Mark Sheldon, Mayor

**ATTEST**:

_____
Lynne Fasone, City Clerk

# *Information Security Policy*

City of Panama City Beach, FL

(Date)

## TABLE OF CONTENTS

## Introduction

This Information Security Policy ("Policy") of the City of Panama City Beach (the "City") encompasses aspects of Information Technology, information security, and must be distributed to all City employees. In this Policy, "You" refers to City employees, as well as certain vendors or independent contractors of the City when appropriate. This Policy includes sections that may directly apply to You and your work, and You are required and expected to comply with this Policy. Other provisions of this Policy may apply to the IT Department. This Policy may contain references to other City policies that should be consulted directly for further details.

This Policy provides information security guidance that You must follow in addition to any obligations described in other City policies, employee handbook, or applicable law. You are expected to read, understand, and follow this Policy and to sign the Acknowledgment Form in Appendix A. Everyone is responsible for ensuring the City systems and information are protected from unauthorized access and improper use. If you are unclear about any aspects of this Policy, You should seek advice and guidance from Your direct supervisor.

The City reserves the right to monitor, access, review, audit, copy, store, or delete when permitted by law any electronic communications, equipment, systems and network traffic for any purpose to ensure the safeguard of information, protection of systems, and confirm compliance with this Policy as well as applicable laws.

## 1. Safeguarding Confidential Information.

The City handles sensitive and confidential information on a daily basis. This sensitive and confidential information may include personally identifying information of City employees, customers from the public, confidential financial information, and other information protected by local, state, and federal privacy and consumer protection laws. The City is committed to respecting the privacy of its employees and customers and to protect Confidential Information in accordance with this Policy and applicable law.

All information maintained by the City is generally classified as either (1) Public Information or (2) Confidential Information.

You must apply appropriate security controls for information that You store, transmit, or otherwise use on behalf of the City. You should designate "Confidential Information" by marking it "Confidential" where feasible.

**1.1 Public Information.** Public Information is information that is available to the general public or is generally and readily available in public records, media, or publication.

a. Public Information Examples. Some Public Information examples include, but are not limited to:

i. press releases;
ii. public records, minutes, agendas, resolutions, ordinances;

iii. documents or records subject to public records laws;
iv. job announcements; and
v. any information that is already publicly available via another source.

Do not assume that information You obtain from the City's internal network is publicly available. For example, drafts of certain records, contracts, and documents may be considered Confidential Information until published and released. Consider all information with sensitive financial, health, or personal information to be Confidential Information and not available for public disclosure without authorization unless You verify that the information can be treated as Public Information.

1.2 **Confidential Information.**. Confidential Information is information that may cause harm to the City, its employees, individual customers, or the general public if improperly disclosed or released. The potential harm from unauthorized access to Confidential Information can relate to an individual's privacy, lead to fraudulent financial transactions, as well as incur legal or regulatory liabilities, embarrassment and other harm to the City or the public.

Mark Confidential Information to denote its status when technically feasible. Applications or databases that contain Confidential Information may be marked with an initial banner shown upon system access.

You must have authorization to disclose Confidential Information to an external party. Seek guidance from your supervisor or have clear authorization prior to disclosing Confidential Information.

a. Confidential Information Examples. Some Confidential Information examples include, but are not limited to:

i. Employee records, health records, and intellectual property;
ii. Customer-provided data including personal information, financial information, or other sensitive information;
iii. Attorney-client privileged or work product information;
iv. Certain infrastructure, utility, or security plans, standards, designs, or other information that may be harmful to the public if disclosed;
v. Internal Communications, emails, policies, and directives from City management, regardless of such being addressed to You individually, a limited group, or City wide;
vi. Any information designated as "confidential" or some other protected information classification by an external party, subject to a current non-disclosure or other similar agreement;
vii. Information protected from disclosure by local, state, and/or federal law; and
viii. Passwords to access any financial account information or gain access to other Confidential Information.

b. Safeguards. You must protect Confidential Information with specific administrative, physical, and technical safeguards implemented according to risks, including (but not necessarily limited to):

i. Authentication. Electronically stored Confidential Information must only be accessible to an individual after logging in to the City's network.

ii. Copying/Printing/Faxing/Scanning. Only scan, make copies, and distribute Confidential Information to the extent necessary or permissible under any applicable non-disclosure agreement, Court Order or Florida law. Take reasonable steps to ensure that others who do not have a legitimate need to know do not view the information.

When faxing Confidential Information, use a cover sheet that informs the recipient that the information is the City's Confidential Information. Set fax machines to print a confirmation page after sending a fax. Locate copiers, fax machines, scanners, and other office equipment in physically secured areas and configure them to avoid storing Confidential Information.

iii. Encryption. Confidential Information should be encrypted, when possible, especially when it is stored on a laptop, smartphone, or mobile storage devices, if permissible, You should seek assistance from the IT Department related to encryption if necessary.

iv. Physical Security. Only store Confidential Information on systems or in paper form in physically secured areas.

**2. Acceptable Use.**

The purpose of an Acceptable Use policy is not to impose restrictions that are contrary to established culture of openness, trust and integrity but to ensure safeguards of Confidential Information and comply with best practices and City standards. The City is committed to protecting its employees, the public, and the City itself from illegal or dangerous computer activity. The IT Department will maintain an approved list of technologies and devices and personnel with access to such device.

a. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of computer systems. Individual departments should create guidelines for personal use of City computer systems consistent with the job duties of employees in that department. In the absence of such guidelines, employees should consult their supervisor or manager regarding personal use of City computer systems.
b. Employees should take all necessary steps to prevent unauthorized access to Confidential data.
c. Keep passwords secure and do not share access to accounts. Authorized users are responsible for the security of their passwords and accounts.

d. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
e. All POS and PIN entry devices should be appropriately protected and secured so they cannot be altered or tampered with.
f. A list of devices will be maintained by the IT Department and regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any tampering of devices.
g. Information contained on portable computers is especially vulnerable, and special care should be exercised to secure information on portable or remote devices.
h. Postings by employees from a City email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City, unless posting is in the course of employee's business duties and is authorized.
i. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

## 3. Unacceptable Use.

Under no circumstances is an employee of the City authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing technology, resources, or computer systems of the City. The following activities are generally prohibited, although certain employees may be exempt 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).

The lists below are not exhaustive but provide a general framework for activities which fall into the category of unacceptable use.

### 3.1 System and Network Activities.

The following activities are strictly prohibited:

a. Violation 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.
b. 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 does not have an active license.
c. Accessing data, a server, or an account for any purpose other than conducting legitimate City business, even if you have access to such data.
d. Exporting software, technical information, encryption software, or technology in violation of applicable laws.

e. Hacking, spoofing, or the introduction of malicious programs into the network, computer system, or server (e.g., viruses, worms, Trojan horses, e-mail bombs, key stroke monitoring, etc.).
f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is performed remotely.
g. Using City computer systems or resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
h. Making fraudulent offers of products, items, or services originating from any City account.
i. 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 is within the scope of regular duties of the employee.
j. Port scanning or security scanning unless previously approved by IT Department or supervisor.
k. Executing any form of network monitoring which will intercept data not intended for the employee unless this activity is a part of the employee's normal job description and duties.
l. Circumventing user authentication or security of any host, network or account.
m. Introducing honeypots, honeynets, or similar technology on the City networks.
n. Spying, stalking, harassing, or attempting to install spyware or other unauthorized monitoring or surveillance tools.
o. Committing criminal acts such as terrorism, fraud, extortion, or identity theft or downloading, accessing, or distributing pornography or other obscene materials.
p. Interfering with or denying service to any user (for example, denial of service attack).
q. Crypto mining or the mining of data or cryptocurrency using City resources.
r. 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.

### 3.2 Email and Communication Activities.

When using City resources to access and use the Internet, You must remember that You represent the City. If You state an affiliation with the City, You 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 Department.

The following activities are strictly prohibited:

a. Sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
c. Unauthorized use, or forging, of email header information.
d. 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.
e. Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
f. Use of unsolicited email originating from within City networks to advertise or solicit for any organization or business unrelated to the City.

### 3.3 Blogging and Social Media.

a. Blogging by employees, whether using City property and systems or personal computer systems, is also subject to the terms and restrictions of this Policy. Limited and occasional use of City systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate this Policy, is not detrimental to the best interests of the City, and does not interfere with Your regular work duties. Blogging from City systems is subject to monitoring by the City.
b. Employees are prohibited from revealing any City Confidential Information, proprietary information, trade secrets or any other sensitive information while blogging.
c. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the City and/or any of its employees. Employees are 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.
d. Employees may not attribute personal statements, opinions or beliefs to the City when engaged in blogging. If You express Your beliefs and/or opinions in blogs, You may not, expressly or implicitly, represent Yourself as an employee or representative of the City. Employees assume any and all risk associated with blogging.
e. City trademarks, logos and any other City intellectual property may not be used in connection with any blogging activity.

## 4. Physical Security.

Access to Confidential Information must be physically restricted to prevent unauthorized individuals from obtaining, accessing, or transmitting Confidential Information.

a. Visitors must always be escorted by a City employee in areas that maintain Confidential Information and/or access to buildings with network storage equipment.

b. City employees should be trained to report suspicious behavior and indications of tampering of devices to the IT Department or supervisors. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
c. Strict control must be maintained over the storage and accessibility of Confidential Information.
d. All computers must have a password protected screensaver enabled to prevent unauthorized use.

## 5. Security Awareness and Procedures.

The protection of Confidential Information demands regular training of all employees and contractors. The City shall:

a. Review procedures for handling Confidential Information and hold periodic security awareness meetings to incorporate these procedures into day-to-day City practice.
b. Distribute this Policy to all employees and contractors to read. It is required that all employees and contractors confirm that they understand the content of this Policy by signing an Acknowledgement Form (see Appendix A).
c. All employees that handle Confidential Information will undergo background checks (such as criminal and credit record checks, as permissible by law) before commencement of employment with the City.
d. All third parties with access to credit card account numbers must comply with card association security standards (PCI/DSS).

## 6. Network Security Incident Response Plan.

The purpose of the Incident Response Plan is to achieve a coordinated and deliberate response to a network security incident by the Incident Response Team. The Incident Response Team shall investigate all reported or detected incidents, and be responsible for coordination, implementation, mitigation, remediation, and other steps necessary in response to an incident.

**6.1 Incident Reporting. Immediately notify the IT Department via phone call, in person, or by support ticket if you discover a security incident or suspect a breach in the City's information security controls.** From that point, the Incident Response Team will assess the situation and implement the appropriate response. The City maintains various forms of monitoring and surveillance tools to detect security incidents, but You may be the first to become aware of a problem. Early detection and response can mitigate damages and minimize further risk to the City, so You should contact the IT Department immediately if You encounter any suspicious or questionable occurrence with the City information resources or devices.

Treat any information regarding security incidents as Confidential Information and do not share it, internally or externally, without specific authorization.

a. Security Incident Examples. Security incidents vary widely and include physical and technical issues. Some examples of security incidents that You should report include, but are not limited to:

i. loss or suspected compromise of user credentials or physical access devices (including passwords, tokens, keys, badges, smart cards, or other means of identification and authentication);
ii. suspected malware infections, including viruses, Trojans, spyware, worms, or any anomalous reports or messages from anti-virus software or firewalls;
iii. loss or theft of any device that contains Confidential Information, including computers, laptops, tablet computers, smartphones, USB drives, disks, or other storage media;
iv. suspected entry (hacking) into the City's network or systems by unauthorized persons;
v. any breach or suspected breach of Confidential Information;
vi. any attempt by any person to obtain passwords, financial account information, or other Confidential Information in person or by phone, email, or other means (sometimes called social engineering, or in the case of email, phishing); and
vii. any other situation that appears to violate this Policy or otherwise create undue risks to the City's information assets.

b. Compromised Devices. If you become aware of a compromised computer or other device:

i. immediately deactivate (unplug) any network connections, but do not power down the equipment because valuable information regarding the incident may be lost if the device is turned off; and
ii. immediately notify the IT Department.

**6.2 Incident Response Team.**. The Incident Response Team is comprised of the following individuals:

Jason Pickle – IT Manager
Travis Gordon – IT System Administrator
Jose Salcido – IT/PD Network Engineer
Lori Philput – HR and Risk Management
Holly White – Assistant City Manager
Drew Whitman – City Manager
Amy Myers – City Attorney

**6.3 Event Management.** Report all suspected incidents, as described in this Policy, and then defer to the incident response process. Do not impede the incident response process or conduct your own investigation unless specifically authorized to do so. As part of the incident response process, depending on the circumstances, the Incident Response Team may perform some or all of the following steps:

a. Upon notification of a possible security incident, the Incident Response Team will investigate the incident, contain any harmful programs, and assist any compromised employee or department in limiting the exposure and in mitigating the risks associated with the incident.
b. Ensure compromised computer system(s) is isolated from the network.
c. Gather, review and analyze the logs and related information from various central and local safeguards and security controls.
d. In consultation with the City Attorney, notify appropriate insurance representatives and/or engage a breach response team.
e. In coordination with a breach response team, conduct appropriate forensic analysis of compromised system.
f. Determine if additional policies and procedures are needed to avoid a similar incident in the future.
g. Determine whether additional technical or physical safeguards are required in the environment where the incident occurred.
h. In consultation with the City Attorney and/or breach response team, contact internal and external departments, individuals, and regulatory bodies as appropriate.
i. In consultation with the City Attorney and/or breach response team, make forensic and log analysis and other information available to appropriate law enforcement.

**6.4 Breach Notification.** Applicable law may require the City to report security incidents that result in the exposure or loss of certain kinds of information or that affect certain services or infrastructure to various authorities, affected individuals or organizations whose data was compromised. Any external notification shall be made by or with consultation from the City Attorney and/or breach response team. **Do not act on your own or make any external notifications without the express authorization of the City Attorney and other department supervisors.**

## 7. User Access Management and Access Control.

a. Access control systems are in place to protect the interests of all users of the City computer systems by providing a safe, secure, and readily accessible environment in which to work.
b. The City will provide all employees with access to information necessary to carry out job responsibilities in as effective and efficient manner as possible.
c. Access to the City computer systems is controlled through a formal user registration process beginning with a formal notification from HR or from Payroll.
d. Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
e. Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
f. There is a standard level of access, other services can be accessed when specifically authorized by Department Directors.

g. The job responsibilities of the user dictate the level of access the employee has.
h. Access to the City computer systems is provided by the IT Department and can only be started after proper procedures are completed.
i. The allocation of privilege rights (e.g., local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization only provided by the IT Department.
j. Access rights will be accorded following the principles of least privilege and need to know.
k. Every user should attempt to maintain the security of information at its classified level even if technical security mechanisms fail or are absent.
l. Users electing to place information on digital media or storage devices may only do so as set forth in this Policy.
m. You are obligated to report instances of non-compliance to the IT Department and or Your immediate supervisor.
n. No access to any City technology resource and/or services will be provided without prior authentication and authorization of a user's City Windows Active Directory account.
o. Password issuance, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
p. Access to Confidential Information will be limited to authorized persons whose job responsibilities require access. Requests for modification of access permissions shall be submitted to the IT Department and must be made in writing.
q. Users are expected to become familiar with and abide by this Policy.
r. Access for remote users shall be subject to authorization by the IT Department. No uncontrolled external access shall be permitted to any network device or system on the City network.
s. As soon as an individual leaves employment with the City, all of his or her system login credentials must be immediately revoked.
t. As part of the employee termination process, Human resources and direct supervisors shall inform the IT Department of all terminations within twenty-four (24) hours of the employee's separation from City employment.

**Appendix A – Agreement to Comply Form – Agreement to Comply with Information Security Policy**

_____

**Employee Name (printed)**

_____

**Department**

I have read, understand, and agree to comply with the Information Security Policy of the City of Panama City Beach. I agree to take all reasonable precautions to assure that the City Confidential Information, or information that has been entrusted to the City by third parties, will not be disclosed to unauthorized individuals. At the end of my employment with the City, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use Confidential Information for my own purposes, nor am I permitted to provide Confidential Information to third parties without express authorization or in accordance with this Policy or applicable law.

I have access to a copy of the Information Security Policy, and I understand how it impacts my job with the City. As a condition of continued employment, I agree to abide by this Policy. I understand that non-compliance may be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of this Information Security Policy to my supervisor or the IT Department as set forth in this Policy.

_____

**Employee Signature**

_____

**Date**