This HIPAA Security policies and procedures manual was prepared for the exclusive use of City of St. Petersburg to assist City of St. Petersburg in complying with the federal Standards for Security of Individually Identifiable Health Information under Title II of the Health Insurance Portability and Accountability Act of 1996 (known as HIPAA). Any reproduction or other use for commercial or other purposes is not permitted without the express written permission of Buck Consultants (Buck). Because Buck is a consulting firm and does not practice law, we strongly recommend that the HIPAA Security policies and procedures manual and its intended usage be reviewed by City of St. Petersburg legal counsel. The contents of the HIPAA Security policies and procedures manual have been prepared based upon sources, materials and information believed to be reliable and accurate. Buck gives no representation or warranties as to the accuracy of the information set forth in the HIPAA Security policies and procedures manual and accepts no responsibility or liability for any error, omission or inaccuracy in such information other than in relation to information which Buck would be expected to have verified based on generally accepted industry practices. Buck does not assume responsibility for any updates to the HIPAA Security policies and procedures manual that might become necessary as a result of City of St. Petersburg subsequent plan or administrative changes or as a result of any relevant regulatory developments or changes in applicable law.
# Table of Contents

Chapter 1 - Introduction ................................................................. 1  
  Purpose of the security policy manual........................................ 1  
  How to obtain a copy of the manual ........................................... 2

Chapter 2 - Administrative Safeguards ........................................ 3  
  Overview ....................................................................................... 3  
  Section 1 - Security Management Process .................................... 4  
    A. Risk Analysis ......................................................................... 4  
    B. Risk Management .................................................................. 5  
    C. Sanction policy ...................................................................... 5  
    D. Information System Activity Review ..................................... 5
  Section 2 - Assigned Security Responsibility ................................ 6
  Section 3 - Workforce Security ................................................... 6  
    A. Authorization and/or Supervision .......................................... 6  
    B. Workforce Clearance Procedure ......................................... 7  
    C. Termination Procedures ....................................................... 7
  Section 4 - Information Access Management ................................ 8  
    A. Isolating Healthcare Clearinghouse Functions ....................... 8  
    B. Access Authorization .......................................................... 8  
    C. Access Establishment and Modification ............................... 8
  Section 5 - Security Awareness and Training ............................... 9  
    A. Security Reminders and Training ......................................... 9  
    B. Protection from Malicious Software ..................................... 10  
    C. Log-in Monitoring ............................................................... 10  
    D. Password Management ....................................................... 10
  Section 6 - Security Incident Procedures ..................................... 11  
    Response and Reporting ........................................................... 11
  Section 7 - Contingency Plan ....................................................... 12  
    A. Data Backup Plan ................................................................. 12  
    B. Disaster Recovery Plan ........................................................ 12  
    C. Emergency Mode Operation Plan ......................................... 13  
    D. Testing and Revision Procedures ......................................... 13
E. Applications and Data Criticality Analysis ......................................................... 14
Section 8 - Evaluation ............................................................................................ 14
Section 9 - Business Associate Contracts and Other Arrangements Policy .......... 15
Written Contracts or Other Arrangements ............................................................... 15

Chapter 3 - Physical Safeguards ........................................................................... 16
Purpose .................................................................................................................. 16
Standards .............................................................................................................. 16
Section 1 - Facility Access Controls ..................................................................... 16
A. Contingency Operations .................................................................................. 16
B. Facility Security Plan ....................................................................................... 18
C. Access Control and Validation Procedures .................................................... 19
D. Maintenance Records ...................................................................................... 20
Section 2 - Workstation Use .................................................................................. 20
Section 3 - Workstation Security .......................................................................... 20
Section 4 - Device and Media Controls ................................................................. 21
A. Disposal ........................................................................................................... 21
B. Media Re-Use .................................................................................................. 21
C. Removable Media and Media Accountability .................................................. 21
D. Data Backup and Storage ................................................................................. 22

Chapter 4 - Technical Safeguards ....................................................................... 23
Overview .............................................................................................................. 23
Purpose ................................................................................................................. 23
Standards .............................................................................................................. 23
Section 1 - Access Control .................................................................................... 23
A. Unique User Identification .............................................................................. 23
B. Emergency Access Procedure ......................................................................... 24
C. Automatic Logoff ............................................................................................. 24
D. Encryption and Decryption .............................................................................. 25
Section 2 - Audit Controls ..................................................................................... 25
Section 3 - Integrity ............................................................................................... 25
Mechanism to Authenticate Electronic Protected Health Information .................. 25
Section 4 - Person or Entity Authentication .......................................................... 26
Section 5 - Transmission Security ................................................................. 26
A. Integrity Controls .................................................................................. 26
B. Encryption ............................................................................................ 26

Chapter 5 - Policies and Procedures and Documentation Requirements 28
Policies and Procedures ............................................................................. 28
Documentation ......................................................................................... 28

Appendices .................................................................................................. 30-41
Chapter 1 - Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the US Department of Health and Human Services (HHS) to adopt national standards for safeguards to protect the Confidentiality, Integrity, and Availability of Protected Health Information (PHI).

The HIPAA Security Rule protects only electronic PHI (ePHI), whether it is:

- electronically created;
- electronically received;
- “at rest” or maintained in a storage device, such as a computer hard drive, disk, CD, or tape; or
- “in transit” via the Internet, etc. (for example, email, FTP, EDI, IVR, and fax-back Systems that transmit PHI).

PHI that was not in electronic form before transmission is not ePHI. This includes information shared by person-to-person telephone calls, copy machines, paper-to-paper fax machines, or voice mail. De-identified information is not ePHI.

The HIPAA Security Rule requires Covered Entities to implement processes to safeguard ePHI against unauthorized access or modification. City of St. Petersburg has developed Administrative, Physical, and Technical Safeguards that will reasonably protect ePHI from intentional and unintentional uses or Disclosures that violate the HIPAA Security Rule.

As with PHI under the Privacy Rule, under the HIPAA Security Rule, City of St. Petersburg must protect the ePHI of its participants and their family members in accordance with HIPAA and state law. City of St. Petersburg generally will use ePHI only for health plan payment activities and operations, and in other limited circumstances, such as when it is required for law enforcement and public health activities.

When ePHI is shared with Business Associates providing services to the Plan, they are required to agree in writing to maintain procedures that protect the ePHI from improper uses and disclosures in accordance with HIPAA.

Purpose of the security policy manual

This manual consists of five (5) sections as follows:

Chapter 1 – Introduction presents an overview of the HIPAA Security Rule, the purpose of this manual and its organization.

Chapter 2 – Administrative Safeguards describes the security policies for administrative safeguards.

Chapter 3 – Physical Safeguards describes the security policies for physical safeguards.
Chapter 4 – Technical Safeguards describes the security policies for technical safeguards.

Chapter 5 – Policies and Procedures and Documentation Requirements describes the security policies for requirements for group health plans and for policies and procedure and documentation requirements.

The manual will be accessible to City of St. Petersburg workforce members who have access to ePHI. Workforce members can obtain more information from City of St. Petersburg’s Security Official.

How to obtain a copy of the manual

Contact Brian Campbell to obtain a copy of the manual.
Chapter 2 - Administrative Safeguards

Overview
The HIPAA Security Rule’s administrative safeguards require documented policies and procedures governing day-to-day operations, managing the behavior of employees in relation to electronic protected health information (ePHI), and managing the selection, development, implementation, and use of security controls.

In the following sections, we discuss each of the nine standards included under the Administrative Safeguards. Note that each of the standards may contain one or more implementation specifications, and that the implementation specifications may be either required or addressable.

Section 1 – Security Management Process
The Security Management Process forms the foundation for all of the other standards by requiring a covered entity to prevent, detect, and correct security violations. This standard requires a risk analysis, ongoing risk management, implementation of a sanction policy to address violations of the entity’s policies and procedures, and an information services activity review.

Section 2 – Assigned Security Responsibility
This standard requires that a covered entity designate a single individual with overall responsibility for the development and implementation of the policies and procedures governing the security of its ePHI.

Section 3 – Workforce Security
A covered entity must implement workforce security measures to assure that all personnel with access to ePHI have the appropriate access authority and clearances, and to prevent access by those who do not.

Section 4 – Information Access Management
This standard requires establishment, adoption, and maintenance of documented policies and procedures defining access control for all personnel authorized to access ePHI and prescribing how access is granted and modified.

Section 5 – Security Awareness and Training
This standard requires that the covered entity implement a security awareness and training program for all personnel with access to ePHI.

Section 6 – Security Incident Procedures
This standard requires the implementation of policies and procedures to handle security incidents.

Section 7 – Contingency Plan
This standard requires that the covered entity have a contingency plan for responding to emergencies that affect systems containing ePHI, as well as related facilities and operations.

Section 8 – Evaluation
This standard requires that the covered entity demonstrate and document ongoing compliance with its security policy through periodic technical and non-technical evaluations. These evaluations are based on the requirements of the HIPAA Security Rule, and also address the covered entity’s response to environmental or operational changes.

**Section 9 – Business Associate Contracts and Other Arrangements**

As defined in the HIPAA Security Rule, a covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on its behalf, only if the covered entity obtains a written contract or other documented arrangement with the business associate. The contract or documented arrangement must provide satisfactory assurances that the business associate will appropriately safeguard the protected information. While many covered entities developed business associate agreements while pursuing HIPAA privacy compliance, it is likely that these agreements will need to be reviewed and perhaps revised to achieve HIPAA security compliance. In addition, there may be additional business associates to consider for HIPAA Security that may not apply to HIPAA Privacy.

Each of these standards and the associated implementation specifications are outlined in detail in the following sections.

**Section 1 - Security Management Process**

A. **Risk Analysis**

City of St. Petersburg currently uses a documented risk analysis process to ensure cost-effective security procedures to mitigate expected losses. All systems or application repositories containing ePHI are identified and documented, potential threats or vulnerabilities are identified, each repository is assigned a level of risk, and, as appropriate, the risk will be mitigated. The current risk/threat analysis is in Section V of the Risk Assessment Report.

City of St. Petersburg annually conducts a risk assessment to identify threats and vulnerabilities, likelihood of threat occurrence, estimated cost, and mitigating controls.

City of St. Petersburg has identified the following ePHI-containing applications/systems, types of information and unique identifiers, and uses of that information:

<table>
<thead>
<tr>
<th>Applications containing ePHI</th>
<th>Ofcie365 - Email, MS Office/Network files, Oracle apps and DB, and S: drive scanner drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePHI identifiers identified</td>
<td>Names, Social Security numbers, Specific dates, Telephone numbers, Email addresses, Geographic identifiers smaller than a state (e.g. zip code), and Employee numbers</td>
</tr>
<tr>
<td>ePHI categories identified</td>
<td>Appeals information, Auditing, Claims history, Claims information/medical bills, Coordination of benefits, Data analysis (e.g., audit information, rate setting), COBRA information or communications, Customer advocacy/call center, EAP information, Eligibility information, Enrollment/disenrollment information,</td>
</tr>
</tbody>
</table>
Explanation of benefits (EOB), Health FSA information (reimbursements, data for non-discrimination testing, etc.), Individual enrollment statements, Information accessible through insurer’s website, and Stop-loss information

Reference(s):
HIPAA Security Rule
CFR §164.308(a)(1)(ii)(A)
Standard: Security Management Process
Implementation Specification: Risk Analysis (Required)

B. Risk Management

City of St. Petersburg implements security measures and mitigating controls sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level for any threats identified as significant risk to the organization as determined by a comprehensive and thorough risk analysis.

These measures include conducting a risk analysis annually, updates to the disaster recovery plan three times per year, and communicating security awareness best practices to employees. In addition, security awareness emails are sent monthly to all users, archives of the newsletters are stored on the intranet, and reviews are conducted with new employees’ policies and procedures regarding system access.

Reference(s):
HIPAA Security Rule
CFR §164.308(a)(1)(ii)(B)
Standard: Security Management Process
Implementation Specification: Risk Management (Required)

C. Sanction Policy

It is the policy of City of St. Petersburg that all workforce members with City of St. Petersburg are expected to abide by all policies included in City of St. Petersburg’s Security Manual. Workforce members who fail to comply with the security policies and procedures will result in disciplinary measures. See the corporate disciplinary action policy (Personnel Management section) for the sanction process.

City of St. Petersburg will not apply sanctions against employees who file a complaint with an entity about a security violation.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(1)(ii)(C)
Standard: Security Management Process
Implementation Specification: Sanction Policy (Required)

D. Information System Activity Review

It is the policy of City of St. Petersburg to monitor all computer systems for security-related events.
The Department of Technology Services (DoTS) is responsible for overall systems activity process, procedures and results. Information systems activity is reviewed daily.

City of St. Petersburg reviews the following exception reports and logs: Failed logins.

Reference(s):
HIPAA Security Rule
CFR §164.308(a)(1)(ii)(D)
Standard: Security Management Process
Implementation Specification: Information System Activity Review (Required)

Section 2 - Assigned Security Responsibility

It is the policy of City of St. Petersburg to appoint a security official who will be responsible for enforcement of the HIPAA Security Rule within City of St. Petersburg, including developing, implementing, and maintaining policies and procedures that meet the requirements of the HIPAA Security Rule. City of St. Petersburg’s security officer is as follows:

- **Name:** Brian Campbell
- **Title:** ITSO
- **Email:** brian.campbell@stpete.org
- **Phone:** 727-892-5503

All of City of St. Petersburg’s staff, employees, workforce, offices, and departments been notified of the name and office to contact with a security problem.

City of St. Petersburg maintains a complete security official job description that accurately reflects the security duties and responsibilities.

A job description for this position is in Appendix D of the Risk Assessment Report.

If City of St. Petersburg Security Official is unable to meet the requirements or responsibilities under the Security Rule, or is no longer affiliated with City of St. Petersburg, then a new Security Official will be assigned.

Reference(s):
HIPAA Security Rule
CFR §164.308(a)(2)
Standard: Assigned Security Responsibility
Implementation Specification: Assigned Security Responsibility (Required)

Section 3 - Workforce Security

A. Authorization and/or Supervision
It is the policy of City of St. Petersburg to ensure that all workforce members be adequately supervised and/or have authorization when working with ePHI or in locations where ePHI resides. The list of individuals and/or groups of individuals that are authorized to access ePHI, titled "Access Control List", is found in Appendix B of the Risk Assessment Report. If an employee who is not included in the Access Control List temporarily needs Access, he or she must be supervised by someone that has such Access and the technical skills to appropriately supervise said employee. The list will be maintained by the Security Official, who gives user attestation reports to Director of HR for ePHI-containing systems or applications.

Reference(s):
HIPAA Security Rule
CFR §164.308(a)(3)(ii)(A)
Standard: Workforce Security
Implementation Specification: Authorization and/or Supervision (Addressable)

B. Workforce Clearance Procedure

It is the policy of City of St. Petersburg to verify applicant information and perform background checks on individuals hired to perform work pertaining to ePHI. The following background checks are used:

- Identity checks (Social security number verification)
- Education and credential verification
- Professional license verification
- Military service verification
- Employment and reference verification
- Drug and alcohol testing
- Criminal history
- Credit reports
- Social Media
- Polygraph for all security-related employees

Reference(s):
HIPAA Security Rule
CFR §164.308(a)(3)(ii)(B)
Standard: Workforce Security
Implementation specifications: Workforce Clearance Procedure (Addressable)

C. Termination Procedures

It is the policy of City of St. Petersburg to terminate all computer and facility access for any employee leaving the service of City of St. Petersburg. If a City of St. Petersburg employee who has Access to ePHI
is terminated or resigns, the former employee's computer accounts will be disabled. This includes remote access. This will be done ahead of time or no later than 24 hours after termination.

City of St. Petersburg’s procedure to recover access control devices from workforce members upon termination is as follows: IT is immediate; HR Benefits timely. A checklist is implemented. The process for employees terminated with cause is highly orchestrated.

Benefits management reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(3)(ii)(C)
Standard: Workforce Security
Implementation specifications: Termination Procedures (Addressable)

Section 4 - Information Access Management

A. Isolating Healthcare Clearinghouse Functions

Not applicable; City of St. Petersburg does not perform clearinghouse functions.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(4)(ii)(A)
Standard: Information Access Management
Implementation specifications: Isolating Health Care Clearinghouse Functions (Required)

B. Access Authorization

City of St. Petersburg maintains a record of employees who require Access to ePHI and the scope of such Access necessary to perform health plan administrative functions.

The access control list is in Appendix B of the Risk Assessment Report.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(4)(i), 164.308(a)(4)(ii)(B)
Standard: Information Access Management
Implementation specifications: Access Authorization Policy (Addressable)

C. Access Establishment and Modification

It is the policy of City of St. Petersburg to assign one unique user ID to each employee and to grant a level of access to the level needed to do his/her job. This will be done through assignment of roles. System administrators will assign user roles/permissions for each User ID so each user will be able to accomplish the functions he/she is authorized to perform.

City of St. Petersburg annually reviews and updates the list of access policies and procedures.
City of St. Petersburg quarterly reviews access control lists, including remote access authorizations, to verify that the list is accurate and has not been inappropriately altered.

City of St. Petersburg has formally documented the standards used to grant a staff member, employee, or workforce member user access to a workstation, laptop, transaction, program, process, and other tools and mechanisms that receive, store, or transmit ePHI.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(4)(ii)(C)
Standard: Information Access Management
Implementation specifications: Access Establishment and Modification (Addressable)

Section 5 - Security Awareness and Training

A. Security Reminders and Training

It is the policy of City of St. Petersburg to provide up-to-date and comprehensive security reminders and awareness training for all workforce members that work with ePHI at minimum annually or during onboarding for any new employee that has access to ePHI.

City of St. Petersburg retains individual training records indefinitely.

City of St. Petersburg will develop and distribute security reminders at appropriate intervals, such as security best practices, notification regarding possible viruses, and reminders regarding procedures for reporting potential security incidents. City of St. Petersburg will use delivery methods such as email, newsletters, videos, etc. All employees with access to ePHI will be required to view security training media when offered and may be required to take a test regarding security issues.

Security reminders include but are not limited to:

- Security policies and revisions to information security policies or procedures
- Information security controls and processes
- Significant risks to company information systems and data
- Security best practices (e.g. how to choose a good password, how to report a security incident)
- Information security legal and business responsibilities (e.g. HIPAA, business associate contracts)
- New information security controls
- Changes made to significant security controls
- Changes to information security legal or business responsibilities
- New threats or risks that arise against the Organization
• Changes to the HIPAA Privacy and HIPAA Security Rules

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(5)(i), 164.308(a)(5)(ii)(A)
Standard: Security Awareness and Training
Implementation Specifications, Security Reminders (Addressable)

B. Protection from Malicious Software

City of St. Petersburg uses anti-virus software on every workstation within the organization and at Internet gateways and firewalls to scan email attachments and other downloaded files. All virus signature files are routinely updated.

In addition, all users are instructed not to open emails unless the attachment was expected in the course of business or was sent by someone known to the recipient.

City of St. Petersburg uses the following additional processes and procedures related to malicious software: Restricted website access and download restrictions.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(5)(ii)(B)
Standard: Security Awareness and Training
Implementation Specifications, Protection from Malicious Software (Addressable)

C. Log-in Monitoring

It is the policy of City of St. Petersburg to monitor log-in attempts on City of St. Petersburg systems. City of St. Petersburg maintains procedures for monitoring login attempts and reporting discrepancies. City of St. Petersburg uses the following processes and procedures related to tracking/monitoring login related activities: Failed logins reviewed as needed.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(5)(ii)(C)
Standard: Security Awareness and Training
Implementation Specifications, Log-in Monitoring (Addressable)

D. Password Management

It is the policy of City of St. Petersburg for employees to create secure passwords for logging in to electronic systems. City of St. Petersburg’s password policy includes the following:

• Have at least one upper case letter, one lower case letter, one numeral, and one symbol
• Passwords cannot contain the username
• Should be at least 10 characters in length (system-level passwords should be at least 15 characters in length)
• Change passwords at least as frequently as every 70 days
• Change all system-level passwords (e.g., administrator, application administration accounts, etc.) at least as frequently as every 70 days
• Passwords cannot be re-used until at least seven subsequent passwords have been utilized
• New user accounts will be established with an initial password that is pre-expired, requiring the account holder to select a new password upon initial use
• The password to a user account may be reset only at the request of the account holder
• Passwords must be reset manually or by calling the help desk
• After five or more successive invalid login attempts have been made to a particular user account, the account is to be disabled for 24 hours
• Passwords shall not be sent through email unless encrypted
• Account holders should not share their passwords with others, including administrative assistants and secretaries

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(5)(ii)(D)
Standard: Security Awareness and Training
Implementation Specifications: Password Management (Addressable)

Section 6 - Security Incident Procedures

Response and Reporting

City of St. Petersburg will adhere to the guidelines set forth in its written security incident policies and procedures.

Employees will report suspected physical security incidents to the following individual via e-mail, telephone, or work order:

Name: Wade R. Schaeffer
Title: Building Maintenance Coordinator
Email: 727-893-7370
Phone: WRSchaef@stpete.org

Employees will report suspected cybercriminal attacks, virus attacks, or other technical compromises to the following individual via e-mail, telephone, or work order:
Name: TS Help Desk
Email: 727-893-7200
Phone: 7200@stpete.org

In the event of a security incident, the Security Officer (or his or her designee) will:

- assess the severity of the compromise;
- if feasible, make a backup of the infected system(s) or application(s) to prevent attacker from removing evidence of his or her activities;
- if feasible, determine if the hacker has left any programs or files on the infected system(s); and
- check all logs for any suspicious activity.

City of St. Petersburg has implemented procedures for security incidents, including preparation, detection and analysis, containment, eradication, and recovery.

City of St. Petersburg has prioritized key functions to determine what would need to be restored first in the event of a disruption.

City of St. Petersburg trains personnel in their incident response roles and responsibilities with respect to the information system.

A sample security incident policy can be found in Appendix E of the Risk Assessment Report.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(6)(i), 164.308(a)(6)(ii)
Standard: Security Incident Procedures
Implementation Specification: Response and Reporting (Required)

Section 7 - Contingency Plan

A. Data Backup Plan

It is the policy of City of St. Petersburg to create and maintain exact retrievable backups of all electronic files and to maintain a process for recovering ePHI in the case of an emergency situation. City of St. Petersburg uses the following methods to recover lost ePHI: Backup is at multiple centers.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(7)(ii)(A)
Standard: Contingency Plan
Implementation Specifications: Data Backup Plan (Required)

B. Disaster Recovery Plan
A disaster is an event, or set of events, that result in the inability of City of St. Petersburg to provide the information services needed for ongoing operations. Disaster conditions can occur at a variety of levels ranging from the “very minor” isolated hardware outage to the complete loss of services.

It is the policy of City of St. Petersburg to create and maintain a disaster recovery plan addressing the preservation of data systems, applications, and networks.

City of St. Petersburg has outlined scenarios that could result in the loss of a critical service involving the use of ePHI and identified preventive measures that can be done for each scenario.

The most recent risk analysis is found in Section V of the Risk Assessment Report.

Wade Schaeffer manages, maintains, and updates City of St. Petersburg’s contingency plan.

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(7)(ii)(B)
Standard: Contingency Plan
Implementation Specifications: Disaster Recovery Plan (Required)

C. Emergency Mode Operation Plan

It is the policy of City of St. Petersburg that, in the event of a disaster, the Disaster Recovery Team (DRT) will assess the current situation and develop an action plan to rectify existing problems. City of St. Petersburg uses the following mechanisms to support continued data processing needs:

- Multiple centers
- Subscription service
- HP Continuity Services (cold site)

Reference(s):
HIPAA Security Rule
CFR § 164.308(a)(7)(ii)(C)
Standard: Contingency Plan
Implementation Specifications, and Emergency Mode Operation Plan (Required)
City of St. Petersburg Contact List for Emergency Personnel

D. Testing and Revision Procedures

It is the policy of City of St. Petersburg to periodically review and test the disaster recovery plan. City of St. Petersburg is responsible for the compilation, regular maintenance, and testing of disaster recovery plans for systems handling information for ePHI-containing systems and applications.

City of St. Petersburg will prepare, maintain, and test the disaster recovery Plan for recovery and continued data processing service after a disaster or emergency. City of St. Petersburg uses the following disaster recovery plan tests:
• **Full-interruption test** -- Operations are shut down at the primary site and shifted to the recovery site in accordance with the disaster recovery plan (for localized and catastrophic testing at least once per year)

Reference(s):
- HIPAA Security Rule
- CFR § 164.308(a)(7)(ii)(D)
- Standard: Contingency Plan
- Implementation Specifications: Testing and Revision Procedures (Addressable)

E. Applications and Data Criticality Analysis

It is the policy of City of St. Petersburg to review all ePHI-containing applications to determine the “Mission Critical” systems and the impact if the system is lost or unavailable.

City of St. Petersburg has identified hardware, software, and personnel that are critical to City of St. Petersburg’s daily business operations.

City of St. Petersburg can tolerate disruption to these operations, material, or services for an extended period of time (72 hours).

Reference(s):
- HIPAA Security Rule
- CFR § 164.308(a)(7)(ii)(E)
- Standard: Contingency Plan
- Implementation Specifications: Applications and Data Criticality Analysis (Addressable)

Section 8 - Evaluation

It is the policy of City of St. Petersburg to perform periodic technical and non-technical evaluations, based on the standards set forth in the HIPAA Security Rule, to ensure that the City of St. Petersburg’s policies and procedures are updated to meet a pre-specified set of security standards as warranted by changes in the City of St. Petersburg’s environmental or operational conditions affecting the security of ePHI.

City of St. Petersburg uses the following security policies to specify that security evaluations will be repeated when environmental and operational changes, such as technology updates, are made that affect the security of ePHI: Evaluations are conducted annually.

City of St. Petersburg includes penetration testing as part of its periodic security evaluations.

City of St. Petersburg has documented all known security gaps between the identified risks and its corresponding mitigating security controls, as well as its justification for any accepted risks.

Reference(s):
- HIPAA Security Rule
- CFR § 164.308(a)(8)
- Standard: Evaluation
- Implementation Specifications: Evaluation (Required)
Section 9 - Business Associate Contracts and Other Arrangements Policy

Written Contracts or Other Arrangements

It is the policy of City of St. Petersburg to ensure that all business associates properly safeguard ePHI created, received, maintained, or transmitted on City of St. Petersburg’s behalf by having up-to-date and executed Business Associate Agreements.

City of St. Petersburg periodically reviews and re-evaluates your list of business associates to determine who has access to ePHI in order to assess whether your list is complete and current.

The list of City of St. Petersburg business associates can be found in Appendix A of the Risk Assessment Report.

Reference(s):
HIPAA Security Rule
CFR § 164.308(b)(4); CFR § 164.314(a)(2)(i); CFR § 164.314(a)(2)(ii)
Standard: Business Associate Contracts and Other Arrangements
Implementation Specifications: Written Contract or Other Arrangement (Required)
Chapter 3 - Physical Safeguards

Purpose

Physical Safeguards include security measures, policies, and procedures that City of St. Petersburg implements to protect its electronic Information Systems and related facilities and equipment from natural and environmental hazards, unauthorized intrusion, and other threats. These physical safeguards are in addition to standard safeguards that address fire, water damage, utility failure, and structural damage to a facility.

Physical Safeguards define the physical operations (processes) that control access to the Facility when City of St. Petersburg is implementing the plans developed under the Administrative Safeguards outlined in the Security Rule at CFR § 164.308.

Standards

Physical Safeguards include four standards. These standards are detailed in following sections of this Manual and include:

Section 1 – Facility Access Controls
Policies and procedures that limit physical access to electronic Information Systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

Section 2 – Workstation Use
Policies and procedures that specify the proper Workstation functions to be performed, the manner in which those functions are to be performed, and the characteristics of the physical surroundings of Workstations that can access ePHI.

Section 3 – Workstation Security
Physical Safeguards for all Workstations that can access ePHI designed to restrict access to authorized Users.

Section 4 – Device and Media Controls
Policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a Facility, and the movement of these items within the Facility.

Section 1 - Facility Access Controls

A. Contingency Operations

Only authorized personnel will be permitted access to City of St. Petersburg facilities during a time of emergency. In addition, City of St. Petersburg has implemented the following fire suppression and environmental detection controls for its facilities:
Municipal Service Center

- Automatic dial-up alarm
- Fire detectors: Heat-sensing
- Fire detectors: Smoke-actuated
- Fire extinguishing Systems: Dry pipe
- Fire extinguishing Systems: Wet pipe
- Fire extinguishing Systems: Fixed fire hoses
- Fire extinguishing Systems: Hand-held fire extinguishers
- Hardware grounded
- Heat-resistant and waterproof containers for backup media and vital non-electronic records
- Heating, ventilation, and air conditioning (HVAC)
- Humidity controls
- Offsite storage of backup media, non-electronic records, and system documentation (replicated at the Water Resources building)
- Plastic tarps that may be unrolled over IT equipment
- Preaction
- Water sensors in the computer room ceiling and floor
- Emergency lighting

Water Resources

- Automatic dial-up alarm
- Emergency master system shutdown switch
- Fire detectors: Smoke-actuated
- Fire extinguishing Systems: Dry pipe
- Fire extinguishing Systems: Wet pipe
- Fire extinguishing Systems: Hand-held fire extinguishers
- Hardware grounded
- Heating, ventilation, and air conditioning (HVAC)
• Humidity controls
• Offsite storage of backup media, non-electronic records, and system documentation
• Preaction
• Emergency lighting
• Server room is protected by HFC-227ea fire extinguishing system

Refer to Chapter 2 (Administrative Safeguards), Section 7 (Contingency Plan) of this policy manual for policy on Contingency Operations. Specifically within that section, refer to Section 7B (Disaster Recovery Plan) and Section 7C (Emergency Mode Operation Plan).

Reference(s):
HIPAA Security Rule
CFR § 164.310(a)(2)(i)
Standard: Facility Access Controls
Implementation Specifications: Contingency Operations (Addressable)

B. Facility Security Plan

It is the policy of City of St. Petersburg to safeguard City of St. Petersburg facilities and their equipment from unauthorized physical access, tampering, and theft.

City of St. Petersburg uses the following access controls for its facilities:

Municipal Service Center

• Guards
• Building check-in (maintenance contractors only)
• Security lighting
• Security alarm
• Closed circuit television (digital records maintained for 90 days)
• Sound detector
• Door or window contact sensors
• Locked doors - keys
• Locked doors - combination/key pad (interior only)
• Locked doors - card swipe
• Magnatomitors at all public entry points

Water Resources
• Building check-in
• Floor receptionist and sign-in
• Fences
• Security lighting
• Security alarm
• Closed circuit television
• Locked doors - keys
• Locked doors - card swipe
• Identification badges
• Control to the general building is established by swipe card access.
• Server room access is limited to required staff by swipe card

City of St. Petersburg has determined that the following types of locations require access controls to safeguard ePHI: Directors authorize access.

Reference(s):
HIPAA Security Rule
CFR § 164.310(a)(1), 164.310(a)(2)(ii)
Standard: Facility Access Controls
Implementation Specification: Facility Security Plan (Addressable)

C. Access Control and Validation Procedures

It is the policy of City of St. Petersburg to limit access to City of St. Petersburg facilities. City of St. Petersburg’s visitor access controls and safeguards for the Water Resources facility include the following:

• Staff required to have their ID badge visible at all times.
• Staff to have appropriate credentials to enter areas where ePHI is located.
• Visitors required to sign in and sign out when entering and leaving a facility.
• Visitors required to provide identification when entering a facility.
• Visitors issued a temporary badge or token.
• Visitors not permitted access outside of normal business hours.
• Log of visitor's name, business, purpose of visit, and who visited maintained for an extended period of time. Access logs are maintained in digital format and reviewed as needed. Records are maintained in accordance with Florida Record Retention laws.
City of St. Petersburg maintains physical access logs for the Water Resources facility in digital format and reviews them as needed. Records are maintained in accordance with Florida Record Retention laws.

The Municipal Service Center facility has all of the above visitor access controls for its data center. For the HR/Benefits area, electronic protections such as locking screen savers with passwords are implemented.

Reference(s):
HIPAA Security Rule
CFR § 164.310(a)(2)(iii)
Standard: Facility Access Controls
Implementation Specification: Access Control and Validation Procedures (Addressable)

D. Maintenance Records

City of St. Petersburg will maintain a log of repairs and modifications to all physical security safeguards at its facilities, including hardware, locks, doors, and walls. City of St. Petersburg will track the following information:

Municipal Service Center

Written log, contains name, where accessed, reason for access.

Water Resources

Work performed on servers is tracked in our Asset Management system. Records are maintained in accordance with Florida Record Retention laws.

Reference(s):
HIPAA Security Rule
CFR § 164.310(a)(2)(iv)
Standard: Facility Access Controls
Implementation Specification: Maintenance Records (Addressable)

Section 2 - Workstation Use

City of St. Petersburg procedures for the proper use of City of St. Petersburg-owned workstations that access ePHI.

City of St. Petersburg includes all types of computing devices in its inventory of workstations, such as laptops, PDAs, tablets (e.g. iPads), smart phones, and others.

Reference(s):
HIPAA Security Rule
CFR § 164.310(b)
Standard: Workstation Use (Required)

Section 3 - Workstation Security
City of St. Petersburg has implemented the following safeguards for workstations that are used to access ePHI to ensure privacy and security:

- Require a password to start-up and return from a screen saver (5, 10, or 15 minutes).
- Workstation monitors must be situated in a manner that prohibits unauthorized viewing.
- To the extent possible, equipment is located in areas that have some degree of physical separation from the public, such as lock doors and no windows, and, where possible, face away from public view.

Reference(s):
HIPAA Security Rule
CFR § 164.310(c)
Standard: Workstation Security (Required)

Section 4 - Device and Media Controls

A. Disposal

It is the policy of City of St. Petersburg to properly dispose of media containing ePHI. Procedures for media disposal include the following: Physical destruction done internally. Drives are wiped, reformatted, and redeployed.

Reference(s):
HIPAA Security Rule
CFR § 164.310(d)(2)(i)
Standard: Device and Media Controls
Implementation Specification: Disposal (Required)

B. Media Re-Use

It is the policy of City of St. Petersburg to remove all ePHI from electronic devices before the device is made available for re-use. Procedures include the following: Physical destruction done internally. Drives are wiped, reformatted, and redeployed.

Reference(s):
HIPAA Security Rule
CFR § 164.310(d)(2)(ii)
Standard: Device and Media Controls
Implementation Specification: Media Re-use (Required)

C. Removable Media and Media Accountability

It is the policy of City of St. Petersburg to maintain an updated inventory and a record of the movement of hardware and software containing ePHI, both inside the organization and when it leaves any facility. Procedures include the following: Asset tags, serial numbers, and internal machine name inventory.

E PHI data is never placed on portable devices such as laptop computers and flash drives.
D. Data Backup and Storage

It is the policy of City of St. Petersburg to backup all critical ePHI-containing applications and data and to maintain off-site storage of these systems.

Reference(s):
HIPAA Security Rule
CFR § 164.310(d)(1), 164.310(d)(2)(iii)
Standard: Device and Media Accountability
Implementation Specification: Accountability (Addressable)
Chapter 4 - Technical Safeguards

Overview

Purpose

Technical Safeguards address technology and the policies and procedures for its use that protect ePHI and control access to it.

Technical Safeguards are designed to guard against unauthorized access to ePHI maintained in a system or transmitted over a communications network. The Technical Safeguards contain the following five security standards that specify how to use technology to protect ePHI and, in particular, to control access to ePHI.

Standards

The five standards contained in the Technical Safeguards are detailed in the following sections and include:

Section 1 – Access Control
Technical policies and procedures for electronic Information Systems that maintain ePHI to grant and allow access only to those persons or software programs that have appropriate access rights.

Section 2 – Audit Controls
Procedural mechanisms and/or processes that record and examine activity in Information Systems that contain or use ePHI.

Section 3 – Integrity
Policies and procedures to protect ePHI from improper or unauthorized alteration or destruction.

Section 4 – Person or Entity Authentication
Procedures to verify that a person or entity seeking access to ePHI is who he/she/it claims to be.

Section 5 – Transmission Security
Technical security measures to guard against unauthorized access to ePHI transmitted over an electronic communications network.

Section 1 - Access Control

A. Unique User Identification

City of St. Petersburg uses the following access control policies to ensure only authorized users have access to ePHI and identified all ePHI-containing applications, systems, networks, or data: Identity-based.
It is the policy of City of St. Petersburg to assign a unique user ID for each employee requiring access to City of St. Petersburg computer systems.

Anonymous users will not be permitted access to City of St. Petersburg computer systems.

City of St. Petersburg has the following procedure for workforce members who access ePHI from a remote location: VMware view for those authorized and written remote access policies are utilized and enforced.

No user shall have access to ePHI over unencrypted and/or unsecured communication channels.

Reference(s):
HIPAA Security Rule
CFR § 164.312(a)(2)(i)
Standard: Access Control
Implementation Specification: Unique User Identification (Required)

B. Emergency Access Procedure

It is the policy of City of St. Petersburg to maintain, plan, and test the continuity plan for recovering and continuing data processing service before/after an emergency has occurred. Procedures are as follows:

- The Disaster Recovery Team (DRT) will be initiated to access the current situation and develop and action plan.
- Only authorized personnel will be allowed access during an emergency situation, e.g., fire, flood, or earthquake.
- The Information Security Officer will be responsible for providing technical guidance for all information systems contingency planning efforts.
- IT Section will train all workers in their section on their responsibilities in case of activation of this plan.
- IT Section will maintain a file of all contingency plans.
- People rotate on and off of the disaster recovery team.

Emergency Access Procedures are covered in Chapter 2 (Administrative Safeguards), Section 7 (Contingency Plan).

Reference(s):
HIPAA Security Rule
CFR § 164.312(a)(2)(ii)
Standard: Access Control
Implementation Specification: Emergency Access Procedure (Required)

C. Automatic Logoff
It is the policy of City of St. Petersburg to automatically disconnect electronic sessions after a predetermined period of inactivity. The procedures are as follows:

- A screen saver with a password activates after a certain period of inactivity (setting of 5, 10, or 15 minutes).
- The VMware view concentrator is limited to an absolute connection time of 24 hours.

Reference(s):
HIPAA Security Rule
CFR § 164.312(a)(2)(iii)
Standard: Access Control
Implementation Specification: Automatic Logoff (Addressable)

D. Encryption and Decryption

It is the policy of City of St. Petersburg that all ePHI is encrypted. Encryption procedures are as follows: Symantec Endpoint, SSL, and Private side networking.

All laptops are encrypted. CS Audit is done regularly and a Varonis full scrub has been done of nonstructured data.

Reference(s):
HIPAA Security Rule
CFR § 164.312(a)(2)(iv)
Standard: Access Control
Implementation Specification: Encryption and Decryption (Addressable)

Section 2 - Audit Controls

It is the policy of City of St. Petersburg to implement audit controls to record any alterations, changes, deletions, modifications, creations, and/or additions to records containing ePHI.

City of St. Petersburg reviews and analyzes information system records for indications of inappropriate or unusual activity as follows: CS Audit is done regularly and a Varonis full scrub has been done of nonstructured data.

Reference(s):
HIPAA Security Rule
CFR § 164.312(b)
Standard: Audit Controls
Implementation Specification: Audit Controls (Required)

Section 3 - Integrity

Mechanism to Authenticate Electronic Protected Health Information

All ePHI data housed in Oracle eBusiness and corresponding Oracle databases is being monitored by CS Audit for authorized access and data level modification. Additional integrity controls are in place on all
identified non-structured ePHI data stores, they are a combination of digital signatures, file auditing, and/or check sum technologies.

Reference(s):
HIPAA Security Rule
CFR § 164.312(c)(2)
Standard: Integrity
Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information (Addressable)

Section 4 - Person or Entity Authentication

It is the policy of City of St. Petersburg to authenticate all users and entities seeking access to City of St. Petersburg computer systems.

City of St. Petersburg uses the following authentication controls:

- Strong passwords

City of St. Petersburg uses the following technical access controls:

- Identity-based

Reference(s):
HIPAA Security Rule
CFR §164.312(d)
Standard: Person or Entity Authentication, (Required)

Section 5 - Transmission Security

A. Integrity Controls

All ePHI data housed in Oracle eBusiness and corresponding Oracle databases is being monitored by CS Audit for authorized access and data level modification. Additional integrity controls are in place on all identified non-structured ePHI data stores, they are a combination of digital signatures, file auditing, and/or check sum technologies.

Reference(s):
HIPAA Security Rule
CFR §164.312(e)(2)(i)
Standard: Transmission Security
Implementation Specification: Integrity Controls (Addressable)

B. Encryption

City of St. Petersburg uses the following encryption algorithms and mechanism for ePHI transmission: Symantec Endpoint, SSL, and Private side networking.

City of St. Petersburg has staff who are skilled in the use of encryption and/or are trained to properly use encryption.
Reference(s):
HIPAA Security Rule
CFR § 164.312 (e)(2)(ii)
Standard: Transmission Security
Implementation Specification: Encryption (Addressable)
Chapter 5 - Policies and Procedures and Documentation Requirements

Policies and Procedures

City of St. Petersburg has reasonable and appropriate policies and procedures in place that comply with the standards and implementation specifications of the HIPAA Security Rule. City of St. Petersburg has procedures for periodic re-evaluation of security policies and procedures and updates them when necessary.

City of St. Petersburg evaluates its HIPAA Security Procedures in the event that one or more of the following events occur:

- Changes in the HIPAA Security Regulations or Privacy Regulations
- New federal, state, or local laws or regulations affecting the privacy or security of ePHI
- Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures
- A serious security violation, breach, or other security incident occurs

City of St. Petersburg reviews its HIPAA Security Procedures periodically, and updates them as needed, to ensure that departments follow such Procedures and that these procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security Policies.

Reference(s):
HIPAA Security Rule
164.316(a)
Standard: Policies and Procedures

Documentation

City of St. Petersburg maintains the following policies and procedures to comply with the HIPAA Security Rule:

- Includes HIPAA Security language in plan documents.
- Documents decisions concerning the management, operational, and technical controls selected to mitigate identified risks.
- Makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
- Retains required documentation of policies, procedures, actions, activities, or assessments required by the HIPAA Security Rule for six years from the date of its creation or the date when it last was in effect (whichever is later).
• Reviews documentation periodically and updates as needed in response to environmental or operational changes affecting the security of ePHI.

Reference(s):
HIPAA Security Rule
164.316(b)(1)
Documentation
# I. Appendix

## Appendix A: Business Associate list

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Agreement date</th>
</tr>
</thead>
<tbody>
<tr>
<td>United HealthCare</td>
<td>8/30/2018</td>
</tr>
<tr>
<td>MetLife Dental</td>
<td>6/17/2017</td>
</tr>
<tr>
<td>Compsych – EAP</td>
<td>3/31/2016</td>
</tr>
</tbody>
</table>
## Appendix B: Access control list

<table>
<thead>
<tr>
<th>Name/job title</th>
<th>Role of person who accesses PHI</th>
<th>Justification for access to PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vicki Grant, Benefits Mgr.</td>
<td>Benefits Administration</td>
<td>Health Plan Administration</td>
</tr>
<tr>
<td>Jason Hall, Benefit Spvr.</td>
<td>Benefits Administration</td>
<td>Health Plan Administration</td>
</tr>
<tr>
<td>Monica Parrish, Analyst</td>
<td>Benefits Administration</td>
<td>Health Plan Administration</td>
</tr>
<tr>
<td>Marilyn Tellado, Analyst</td>
<td>Benefits Administration</td>
<td>Health Plan Administration</td>
</tr>
<tr>
<td>Morgan Morrow, Analyst</td>
<td>Benefits Administration</td>
<td>Health Plan Administration</td>
</tr>
<tr>
<td>Elisabeth Trujillo, Personnel Tech.</td>
<td>Benefits Administration</td>
<td>Payment</td>
</tr>
<tr>
<td>Anne Fritz, Finance Dir</td>
<td>Finance Department</td>
<td>Payment</td>
</tr>
<tr>
<td>Tom Hoffmann, Controller</td>
<td>Finance Department</td>
<td>Payment</td>
</tr>
<tr>
<td>Paul Woodarek, Payroll Spvr.</td>
<td>Finance Department</td>
<td>Payment</td>
</tr>
<tr>
<td>Oracle Analysts – can see enrollments on test DBs</td>
<td>Department of Technology Svcs.</td>
<td>Other</td>
</tr>
<tr>
<td>All employees/managers who have access to employee paycheck information (Statement of Earnings)</td>
<td>Other Departments</td>
<td>Other</td>
</tr>
<tr>
<td>ICS</td>
<td>Department of Technology Svcs.</td>
<td>IT support</td>
</tr>
<tr>
<td>Production Control</td>
<td>Department of Technology Svcs.</td>
<td>IT support</td>
</tr>
<tr>
<td>ebusiness</td>
<td>Department of Technology Svcs.</td>
<td>IT support</td>
</tr>
</tbody>
</table>
Appendix C: Job Description for Privacy Officer

Position title:

Privacy Officer

Role:

The Privacy Official oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to City of St. Petersburg’s policies and procedures covering the privacy of, and access to, health information in compliance with federal and state laws and the company’s information privacy policies relating to group health plans covering the company’s employees and their dependents.

Duties:

The Privacy Official shall:

- Provide development guidance and assist in the identification, implementation, and maintenance of Plan information on privacy policies and procedures in coordination with Workforce members and legal counsel.

- Perform initial and periodic information privacy risk assessments and conduct related ongoing compliance monitoring activities.

- Ensure that the Plan has and maintains appropriate privacy Authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

- Oversee, direct, deliver, or ensure delivery of initial and ongoing privacy training and orientation to relevant employees, Business Associates and other appropriate third parties.

- Participate in the development, implementation, and ongoing compliance monitoring of all Business Associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.

- Establish a mechanism to track access to PHI, within the purview of the Plan and as required by law and to allow qualified individuals to review or receive a report on such activity.

- Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Plan’s privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

- Ensure compliance with privacy policies and consistent application of sanctions for failure to comply with privacy policies.
• Initiate, facilitate and promote activities to foster information privacy awareness within the company.

• Review all system-related information security plans to ensure alignment between security and privacy practices.

• Work with all workforce members to ensure full coordination and cooperation under the Plan’s policies and procedures and legal requirements.

• Maintain current knowledge of applicable federal and state privacy laws, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.

• Cooperate in any compliance reviews or investigations.
Appendix D: Job Description for Security Official

**Position title:**

Security Official

**Description:**

The HIPAA Security Officer is responsible for the ongoing management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational healthcare information systems.

**Actions and accountabilities:**

- Responsible for implementing, managing, and enforcing information security directives as mandated by HIPAA.
- Ensure the ongoing integration of information security with business strategies and requirements.
- Ensure that the access control, disaster recovery, business continuity, incident response, and risk management needs of the organization are properly addressed.
- Lead information security awareness and training initiatives to educate workforce about information risks.
- Perform ongoing information risk assessments and audits to ensure that information systems are adequately protected and meet HIPAA certification requirements.
- Work with vendors, outside consultants, and other third parties to improve information security within the organization.
- Lead an incident response team to contain, investigate, and prevent future computer security breaches.

**General skills and experience requirements:**

- Experienced in the management of both physical and logical information systems
- Strong technical skills (application and operating system hardening, vulnerability assessments, security audits, TCP/IP, intrusion detection systems, firewalls, etc.)
- Outstanding interpersonal and communication skills
- Must possess a high degree of integrity and trust along with the ability to work independently
- Excellent documentation skills
- Ability to weigh business risks and enforce appropriate information security measures
- In-depth knowledge of the HIPAA Security Rule and other government technology laws
- CISSP (Certified Information Systems Security Professional) certification
Appendix E: Security incident procedures

Sample security incidents response for computer viruses and worms

Individuals and information technology support professionals are expected to:

Prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring
Take immediate action to prevent the spread of any acquired infections from any computers under their control

Sample reporting and responses to it security incidents by individuals

Staff should attempt to stop any IT security incident as it occurs. Disconnecting it from the organization's network will stop any potentially threatening activities.

Staff should report suspected IT security incidents to an information technology support professional. IT professionals will help assess the problem and determine how to proceed, including consideration of actions to repair the system, restore service, preserve evidence of the incident, and identify corrective steps to prevent similar security incidents from reoccurring.

Following the report, staff should comply with directions provided by IT support staff or the IT Security Response Team.

Sample security incidents response by it security professionals

Information technology support professionals have additional responsibilities for IT security incident handling and reporting for both the systems they manage personally for their departments and the systems of users within their departments. In the case of an IT security incident, IT support staff should:

Respond quickly to reports from individuals
Take immediate action to stop the incident from continuing or recurring
Preserve appropriate forensic evidence
Restore the system to service using last known secure backups of the system
Check and preserve logs of any suspicious activities

The IT Security Response Team or Security Official will notify the HIPAA Privacy Official in the event that a security incident results in the improper disclosure, use, or access of an individual's ePHI, and will work with the Privacy Official (or his or her designee) to satisfy any PHI breach reporting required under HIPAA

Sample post security incident lessons learned

Following an IT security incident, a post security incident report shall be prepared by the IT Security team. This report shall include the following information:
Summary of the Incident

Incident Handling Actions

- Log of actions taken by all handlers
- Contact information for all involved parties
- List of evidence gathered

Incident Handler Comments

Cause of the Incident (e.g., improperly configured application, non-patched host)

Cost of the Incident

Business Impact of the Incident

Sample it security incident planning and training

IT professionals tasked with responsibility for responding to IT security incidents shall review, every six months, NIST SP 800-61, Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology.

Sample planning & training updating

The security incident response plan will be reviewed and, if appropriate, revised:

Within 12 months of its most recent revision
After confirmed security incident
After any failed test of the security incident response plan
Appendix F: Security maintenance policy

City of St. Petersburg will maintain a log of all repairs to equipment. The log will be kept by Brian Campbell.

The logs will be retained for a period of seven years.

The following items will be tracked in the maintenance log:

Person who requested the repair
Job begin date
Job end date
Cost of repair
Person performing repairs
Equipment being repaired
Description/location of repair job
Appendix G: Security maintenance log

<table>
<thead>
<tr>
<th>Person who requested the repair</th>
<th>Job begin date</th>
<th>Job end date</th>
<th>Cost of repair</th>
<th>Person performing repairs</th>
<th>Equipment being repaired</th>
<th>Description/location of repair job</th>
</tr>
</thead>
</table>
Appendix H: Security integrity control language

Sample integrity control/encryption policy guidelines

Implementation of encryption and decryption and/or other integrity controls is not justified at this time due to the cost, administrative burden and the level of risk associated with City of St. Petersburg ePHI. In addition, in lieu of encryption or integrity controls, City of St. Petersburg utilizes the following tools, techniques and processes (when appropriate) to support the assurance of the confidentiality and integrity of all identified electronic protected health information (ePHI):

- Enforcement of password policy
- Security awareness training
- Review of failed login attempts
- Password protection of ePHI containing data files
- Careful review of record counts and file control totals
- Enforcement of workstation security
- Identification of scenarios that may result in modification of the ePHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors)
- Report any suspicious activity immediately to network administrator, security officer, and help desk
- Review Windows Explorer "File Details" and other logs to determine the last modifier of a file
Appendix I: Security remote access policy

The purpose of this Policy is to define standards for connecting to City of St. Petersburg’s network from any remote host, untrusted host, and remote network, including untrusted hosts on City of St. Petersburg’s intranet. These standards are designed to minimize the potential exposure to City of St. Petersburg from damages, which may result from unauthorized use of City of St. Petersburg resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical City of St. Petersburg internal systems, etc.

This Policy applies to all City of St. Petersburg employees, contractors, vendors and agents with a City of St. Petersburg-owned or personally owned computer or workstation used to connect to the City of St. Petersburg network. This Policy applies to remote access connections used to do work on behalf of City of St. Petersburg, including but not limited to, reading or sending email and viewing intranet web resources.

Policy:

It is the responsibility of City of St. Petersburg employees, third-party contractors, vendors and agents with remote access privileges to City of St. Petersburg's networks to ensure that unauthorized users are not allowed access to internal City of St. Petersburg networks and associated content.

Access to the City of St. Petersburg Trusted Network will only be allowed from Trusted Users and other special ITS administered subnets.

A virtual private network (VPN) connection must be established during the off-site remote access of City of St. Petersburg information technology resources (switches, printers, routers, computers, etc.).

All network activity during a VPN session is subject to City of St. Petersburg policies.

Secure remote access must be strictly controlled. Control will be enforced via password authentication.

At no time should any City of St. Petersburg employee or provide his or her login or email password to anyone, not even family members.

Remote Users must ensure that their Remote Hosts used to access City of St. Petersburg IT Resources meet all security expectations specified in the End User Security Guidelines prior to accessing any City of St. Petersburg IT Resource.

All hosts that are connected to City of St. Petersburg internal networks via remote access technologies must use the most up-to-date anti-virus software. Information on this software can be obtained from the City of St. Petersburg Technical Support group. This includes personal computers.

Redistribution of the City of St. Petersburg VPN Installer or associated installation information is prohibited.
All users of the City of St. Petersburg VPN shall only connect to or have access to machines and resources that they have permission and rights to use.

The Information Security Department will be contacted when the use of a VPN is not viable, when additional controls are required, or for "pass list" requests.

It is the responsibility of Remote Users to take reasonable precautions to ensure their remote access connections are secured from interception, eavesdropping, or misuse.

All Remote Users are expected to only remotely access data in accordance with City of St. Petersburg IT policies.

General access to the Internet for recreational use by immediate household members is discouraged through the City of St. Petersburg Dial-in Modem Network. The City of St. Petersburg employee is responsible for ensuring the family member does not violate any City of St. Petersburg policies, does not perform illegal activities, and does not use the access for outside business interests. The City of St. Petersburg employee bears responsibility for the consequences should the access be misused.

Do not save or store City of St. Petersburg sensitive or restricted data on the Remote Host used to access City of St. Petersburg IT Resources.

Where applicable, all Remote Users are also responsible for following any guidelines issued by the HIPAA Privacy Compliance Office for remote access to Protected Health Information accessed within the course of the Remote User’s job function at City of St. Petersburg.

Anyone found to have violated this Policy may have his/her network access privileges temporarily or permanently revoked.