Information Security Policy

Information Security Policy

Policy Number: 0020001 Revision Number: 01
Effective Date: 1/1/2019
Last Revised Date: 5/3/2019
Responsible Office:

Status
□ Draft
□ Under Review
□ Approved
☒ Obsolete

Executive Summary

The Information Security Policy exists in order to provide the organizations staff with a current set of clear and concise principles for protecting Information in all of its forms. These policies provide direction for the appropriate protection of the organization's information and assets.
The Information Security Policy has been created as a component of an overall Information Security Program ("ISP") for the organization. The ISP outlines the organization's mission and objectives as they relate to information security, outlines details that are responsible for information security, documents policies relating to information security, indicates how the program is to be communicated and how people in the organization must be trained on their responsibilities, and includes a roadmap of how the program is to be carried out. In addition, the program includes strategies for its ongoing evaluation and adjustment, addressing of compliance issues, and management reporting.

Purpose and Guiding Principles

The purpose of this policy is to provide general guidance and specific recommendations for the protection of PDR-Team Ltd. information technology resources and the protected health information stored on those resources. Additionally Personally Identifiable Information (PII) that exists in hard form is also protected by this policy. These information security measures are intended to protect the organization's information and assets and to preserve the privacy of PDR-Team Ltd.'s customer data.

The broad goal of information security at PDR-Team Ltd. is to maintain Confidentiality, Integrity, and Availability of data. To achieve this goal, PDR-Team Ltd. has identified a set of core security principles. The policy will, in turn, be supported by detailed operational procedures. These simple principles make up the foundations of a strong security posture.

- **Universal Participation** – Every component of an organization could be a potential avenue of entry for unauthorized intruders. Thus a strong security infrastructure requires the cooperation of all parties in the organization. *Everyone* is responsible for security.
- **Risk-Based security** – An organization's security is defined by the unique risks it faces. These risks should be identified regularly and should remain the primary focus of any security policy or program.
- **Deny All That is Not Explicitly Permitted** – Anything not explicitly allowed is denied.
- **Least-Privilege** – Users and systems should only have minimum level of access necessary to perform their defined function. All unnecessary levels of access should be restricted unless explicitly needed.
- **Defense-in-Depth** – Overall security should not be reliant upon a single defense mechanism. If an outer security perimeter is penetrated, underlying layers should be available to resist the attack.
- **Compartmentalization** – If one compartment is compromised, it should be equally difficult for an intruder to obtain access to each subsequent compartment.
- **Secure Failure** – When a system's confidentiality, integrity, or availability is compromised, the system should fail to a secure state.
- **Defense through Simplicity** – A simple system is more easily secured than a complex system, as there is a reduced chance for error.
- **Dedicated Function** – Systems should be single-purposed to avoid potential conflicts or redundancies that could result in security exposures.
- **Need-to-Know** – Information will only be circulated to those parties that require it in order to perform their defined business function.
- **Effective Authentication and Authorization** – Firmly established identity and role-based authorization are essential to making informed access control decisions.
- **Audit Integrity** – Audit log events that are generated may not be altered by the entity that generated the event.

Scope

This policy applies to all departments within the organization. It covers all PDR-Team Ltd. information technology resources, that store or process PII. All creation, processing, communication, storage, distribution and disposal of PDR-Team Ltd. PII is covered by this policy. Each employee of PDR-Team Ltd., contractor and other related third parties are bound by the guiding principles, statement of policy and related procedures outlined in this policy.

Statement of Policy

The Information Security Policy exists in order to provide the organizations staff with a current set of clear and concise information security policies. These policies provide direction for the appropriate protection of the organization's information and assets.

The Information Security Policy has been created as a component of an overall Information Security Program ("ISP") for the organization. The ISP outlines the organization's mission and objectives as they relate to information security, outlines details that are responsible for information security, documents policies relating to information security, indicates how the program is to be communicated and how people in the organization must be trained on their responsibilities, and includes a roadmap of how the program is to be carried out. In addition, the program includes strategies for its ongoing evaluation and adjustment, addressing of compliance issues, and management reporting.

The Information Security Policy has been reviewed, approved, and is endorsed by PDR-Team Ltd. management.

The Information Security Policy applies to all PDR-Team Ltd. employees, contractors, and any third-party providers that support any of the PDR-Team Ltd.'s services.

The Information Security Policy document contains rules and requirements that must be met in the delivery and operation of the PDR-Team Ltd.'s services. More detailed ***standards*** and specific ***procedures*** must be developed as adjuncts to this Information Security Policy to provide implementation level details for carrying out specific operational tasks. The procedures must be the instrument by which these «Organiztion Name» Security Policies are converted into action.

The Information Security Policy must be located in a central repository that is accessible to all PDR-Team Ltd. employees and related third parties.

The Information Security Policy must be distributed to all new and existing PDR-Team Ltd. employees for review. All PDR-Team Ltd. employees, contractors and third party providers are required to sign an agreement representing the fact that they have reviewed, and agree to adhere to, all policies within the Information Security Policy document.

Exceptions to the Information Security Policy must be authorized by PDR-Team Ltd. management. Please refer to for exception ***process*** details.

Procedures

Within this Section, the phrases “**must**” and “**recommended**” have specific meanings where highlighted in **boldface**. If a Covered Entity correctly adheres to the guidelines given as “**must**”, then it can be considered as meeting the requirements for this policy. If they also adhere to the guidelines given as “**recommended**”, then they can be considered to be meeting the minimum requirements to be in accordance with generally accepted information security practices.

A. Each Covered Entity **must** designate a HIPAA Security Officer.

B. Each Covered Entity **must** conduct a risk assessment on at least an annual basis to quantify and understand potential threats and vulnerabilities of PHI and EPHI.

C. It is **recommended** that each Covered Entity regularly perform self-assessments and/or audits to detect security vulnerabilities and non-compliance to PDR-Team Ltd.’s security policies and procedures. Upon discovery, each department **must** initiate corrective actions to ensure that compliance with these policies and procedures is restored.

D. Each Covered Entity **must** implement reasonable and appropriate controls to protect the confidentiality, availability and integrity of PHI and EPHI. These controls **must** consist of administrative, physical and technical safeguards.

E. Before conducting business with any third party that stores or processes EPHI, the Covered Entity **must** have a signed Business Associate Contract in place that outlines provisions with which the third party must comply to protect the organization’s EPHI.

F. No employee owned assets may be used to store or process EPHI.

G. All PDR-Team Ltd. employees **must** abide by clear desk and clear screen policies by appropriately securing PHI and EPHI when the workspace is unattended.

H. Physical access to Information Systems that store or process EPHI **must** be controlled in a way that prevents unauthorized physical access.

I. All PDR-Team Ltd. personnel **must** be positively identified before being granted access to Information Systems that store or process EPHI.

J. Any and all repairs, alterations or relocations of Information Systems that store or process EPHI **must** be fully documented for review by the HIPAA Security Officer.

K. Any and all reuse, disposal or recycling of media that was used to store EPHI **must** be done in a manner by which any data remaining on the media is positively destroyed.

L. Any and all access to PDR-Team Ltd. EPHI **must** be:

   a. Authorized by the appropriate Data Owner
   b. Consistent with the rule of least privilege
   c. Granted to unique users
   d. Authenticated in a way which positively identifies the user
   e. Reviewed on at least an annual basis and revoked when no longer needed to perform necessary job duties.
   f. Logged for review by the HIPAA Security Officer

M. All accounts used to access EPHI **must** be protected with an appropriately strong password

N. All Information Systems that store or process EPHI must time out after a period of inactivity. It is **recommended** that this include password protected screen savers, network activity timeouts and application time limits as appropriate.

O. All Covered Entities **must** monitor Information Systems that store or process EPHI for security events.

P. Any security events must be reported to the HIPAA Security Officer and addressed in a manner that is in line with both the organization's policies and the law.

Q. All Covered Entities **must** develop appropriate Business Continuity and Disaster Recovery Plans that include Information Systems used to store and process EPHI. These plans **must** include at least the following:

   a. Maintenance of backup copies of EPHI.
   b. Periodic testing of the backup copies for integrity and availability
   c. Appropriate testing of business continuity and disaster recovery plans on at least an annual basis

R. It is **recommended** that each Covered Entity encrypt stored EPHI.

S. Each Covered Entity **must** encrypt EPHI in transit over the Internet or any other network available to unauthorized personnel.

Roles and Responsibilities

Senior Management

PDR-Team Ltd. senior management is responsible for:

A. Promulgating and enforcing the policies, standards, procedures, and guidelines for the protection of IT resources and information.

B. Furnishing necessary funding and other resources or limiting and eliminating services to ensure continued compliance with this policy.

C. Appointing an Information Security Coordinator and/or establishing departmental computer support and system administrators. Providing appropriate training and resources to the person(s) responsible for information security-related tasks.

D. Specifying and applying sanctions consistent with Human Resources policies to individuals and divisions that break provisions of this policy, either willfully, accidentally, or through ignorance.

E. Designating Data Stewards for each significant collection of business information, who in turn are responsible for determining the value of their information and implementing appropriate security measures as specified in the Data Access Policy.

F. Sponsoring internal awareness and training programs to familiarize employees, contractors and third-party providers with the security policy, procedures and recommended practices.

G. Defining guidelines and intervals for the review and update of this policy and to reassess existing risks and to identify potential new risks to PDR-Team Ltd. assets and information.

Security Officer

The Security Officer is responsible for:

A. Understanding relevant security and privacy procedures

B. Understanding how PII is used within the organization and any third party providers.

C. Development and implementation of appropriate procedures to support this policy.

D. Ensuring that users receive appropriate Education and Awareness Training as sponsored by Senior Management.

E. Ensuring that any and all exceptions to this policy are formally documented.

F. Coordinating with stakeholders to identify, evaluate and understand risks to PII

G. Coordinating with stakeholders and interested parties to respond to breaches of PII whether suspected or realized.

PDR-Team Ltd. has appointed as the organization’s Security Officer.

Employees

Each PDR-Team Ltd. employee is responsible for understanding and complying with the policies and procedures relating to information technology security and for fully cooperating with the information security staff at all levels to protect PDR-Team Ltd.’s PII.

Each employee must become familiar with PDR-Team Ltd.’s Acceptable Use Policy.

PDR-Team Ltd. computer and communications systems must be used for business purposes only. Incidental personal use is permissible if the use (a) does not consume more that a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, and (c) does not preempt any business activity. Examples of permissible incidental use include – the occasional use of electronic mail (email) or web access for other than official purposes.

Using PDR-Team Ltd. systems to download, use, or re-distribute unlicensed or inappropriate software, copyrighted movies, copyrighted music, or pornographic materials, place the Institute at risk and will not be tolerated. Conduct in violation of this policy may result in sanctions as provided in the Computer and Network Usage Policy. Report all actual or suspected instances of security or policy violations in accordance with the Incident Reporting section of this policy.

Compliance

Any person who uses PDR-Team Ltd.’s information or assets to store or process PII consents to all provisions of this policy and agrees to comply with all of its terms and conditions, as well as with relevant state and federal laws and regulations. Users have a responsibility to use these resources in an effective, ethical and lawful manner. Any violation of this policy may result in disciplinary or administrative sanctions including loss of privileges, monitoring of use and up to and including termination depending on the severity and intent of offense. Additionally, non-compliance with this policy resulting in loss or disclosure of data may result in personal civil and/or criminal liability.

Policy Modifications

This policy may be changed by PDR-Team Ltd. Senior Management at any time, but typically will be modified in response to newly identified threats or risks. Changes to this policy will be communicated and distributed to all affected parties.