CYBERSECURITY BASELINE POLICY

description

The Cybersecurity baseline policy is for people who have received access to IT technology and information assets.

Policy Number

FH-IT.100

Supersedes

none

Purpose

A) This Cybersecurity Policy establishes a baseline and formal set of rules by which those people who are given access to Froedtert Health technology and information assets must abide.

B) The Policy serves several purposes. The main purpose is to inform Froedtert Health Users: employees, contractors, business partners and other authorized users of their obligatory requirements for protecting the technology and information assets of Froedtert Health. The Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

C) The Cybersecurity Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of Froedtert Health computer systems and data.

Definitions

A) Chief Information Officer: The formal head of the entire IT department for Froedtert Health.

B) Externally accessible to public: The system may be accessed via the Internet by persons outside of Froedtert Health without a logon id or password. It is possible to "ping" the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.

C) Froedtert Health User: Employees, contractors, business partners and other authorized users of Froedtert Health systems and information assets.

D) Information Owner: Departmental and functional leadership are the owners of information associated with their business processes. Information Owners are responsible for identification and classification of information assets, implementing controls, ensuring compliance with those controls.

E) Internally accessible only: Users of the system must have a valid logon ID and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a “ping” from the Internet. A private intranet Web Server is an example of this type of system.

F) IT Security Officer: An employee of IT shall be designated as the IT Security Officer for Froedtert Health.

G) IT: Information Technology

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

I) Privileged Access: Privileged accounts are valid credentials with elevated, non-restrictive access used to gain access and manage systems.

Policy

A) It is the obligation of all users of Froedtert Health systems to protect the technology and information assets of Froedtert Health. This information must be protected from unauthorized access, theft, loss and destruction. The technology and information assets of Froedtert Health are made up of the following components:

a) Computer hardware, CPU, disk, Email, web, application servers, PC systems, application software, system software, etc.
b) System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
c) Application Software: used by the various departments within Froedtert Health. This includes custom written software applications, and commercial off the shelf software packages.
d) Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

B) Information Asset Inventory and Classification
a) An information classification policy and standard must exist to identify information handling requirements based upon sensitivity and criticality. An information asset inventory must be maintained and information assets must be classified according to the information classification standard.

C) Information Classification
a) Information should be classified in terms of its value, legal requirements, sensitivity, retention and criticality to Froedtert Health. Classification should be based upon the potential impact to Froedtert Health in terms of Legal violations, exposure, unwanted publicity or loss (actual monetary loss, loss of potential or future revenue, loss of

business customers or clients) in the event such information is lost, stolen, or released without proper authorization, or disclosed without permission. Based on the classification level, the policy and standard define the class of protection requirements for information assets.

b) The information classification policy and standards are the minimum requirements which must be met. An information owner may select a more restrictive protection control(s) on their data at their discretion or as required by locally applicable legal requirement(s).

Level	Classification	Target Audience	Estimate Amount
1	Green (Open)	• Available to the public without any special restrictions.	25-35% of data
2	Yellow (Sensitive)	• Available to Froedtert Health Users, business partners and contractors that have authorized access to FH systems with no to minimal added levels of restriction. • Client confidential information received from customers or business partners.	70-75 % of data
3	Red (Restricted)	• In addition to Level 2 protection: Highly restrictive distribution/access.	5-10% of data

c) Green (Open) : Data that does not fall into any of the other information classifications. This data may be made generally available without specific information owner's designee or delegate approval. Examples include, but are not limited to, advertisements, job opening announcements, Froedtert Health catalogs, regulations and policies, faculty publication titles and press releases.

d) Yellow (Sensitive) : Data whose loss or unauthorized disclosure would impair the functions of Froedtert Health, cause significant financial or reputational loss or lead to likely legal liability. Examples include, but are not limited to, research work in progress, research protocols, financial information, strategy documents and information used to secure Froedtert Health's physical or information environment.

e) Red (Restricted): Data in any format collected, developed, maintained or managed by or on behalf of Froedtert Health, or within the scope of Froedtert Health activities, that are subject to specific protections under federal or state law or regulations, under applicable contracts. Examples include, but are not limited to medical records, social security numbers and or credit card numbers.

D) Responsibilities

a) Information owners are responsible for appropriately classifying data.

b) Information custodians are responsible for labeling data with the appropriate classification and applying required and suggested safeguards.

c) Information users are responsible for complying with data use requirements.

d) Information users are responsible for immediately referring requests for public records to Froedtert Health Relations Division – Office of Public Affairs or to the Office of the Vice President and General Counsel.

E) Acceptable Use

a) Every user of Froedtert Health computing assets must use reasonable care, as outlined in the "Email & Internet Usage Policy". User accounts of Froedtert Health are to be used primarily for business purposes. Unauthorized use may be in violation of the law, and can be punishable by law.

b) Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of Froedtert Health.

c) Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Froedtert Health systems for which they do not have authorization.

d) Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the Froedtert Health Users' manager and/or Froedtert Health IT designee.

e) Users shall not download unauthorized software from the Internet onto their PCs or workstations.

F) Use of the Internet

a) Froedtert Health will provide Internet access to Froedtert Health Users who are connected to the internal network and who has a business need as outlined in the "Email & Internet Usage Policy". Froedtert Health Users must obtain permission from their supervisor and file a request through the "APS" Access Provisioning System.

G) Monitoring Use of Computer Systems

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

H) Information Technology Risk Management

a) Periodic Information Technology risk assessments must address risks to the confidentiality, integrity, and availability of information.

I) Application and System Security

a) Project management and systems development lifecycle processes must ensure that applications and systems are assessed for risk and implemented according to application and system security standards. Technical vulnerabilities must be regularly identified and managed.

b) Security Awareness

An information security awareness curriculum must be maintained and delivered to all Froedtert Health Users on an annual basis at a minimum.

J) Vulnerability Management

a) Network and system vulnerabilities must be assessed internally on a monthly basis at a minimum. An independent third-party vulnerability assessment must be performed on an annual basis. Assessments must address the classification of the associated information assets and remediation must be prioritized based upon both the severity of the vulnerability and the business impact of the assets.

K) Vendor Security Management

Reviews of vendor security practices must be conducted prior to executing contracts involving red (restricted) or yellow (sensitive) information. Vendor security reviews must include evaluation of the vendor's organizational controls and/or technologies depending on the nature of the relationship, service provided and information shared.

L) Security Incident Management
Criteria and means for detecting security incidents must be defined. All identified and suspected information security incidents must be reported and investigated. Users are required to report any weaknesses in Froedtert Health computer security, any incidents of misuse or violation of policy to their immediate supervisor.

M) Business Continuity and Disaster Recovery
Business continuity requirements must be evaluated and contingency plans must be developed for those information assets whose availability is deemed critical to the organization.

N) Access Control
a) Access control policies and procedures must be defined to ensure that access to information and physical assets is properly authorized and maintained. Access control must address:
b) The establishment of identities
c) Roles/privileges/authorization
d) Role administration
e) Segregation of duties
f) User administration
g) Logging and monitoring of user access
h) Periodic reviews of user access

O) Human User Logon and Password Management
a) All users will be required to have a unique logon ID and password for access to systems. The user's password must be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other person whatsoever. All users must comply with the following rules noted in the "Information Integrity Policy".:
b) Password must not be easily guessable or found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective.
c) Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
d) Password must be changed regularly.
e) User accounts will be frozen after a specified number of failed logon attempts.
f) Logon IDs and passwords will be suspended after specified number of days of inactivity.

g) Users are not allowed to access password files on any system or network device. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

h) Regular users will not be allowed privileged access to logon as a System Administrator. Users who require privileged access to production systems must request a Firefighter account as outlined elsewhere in this document.

i) Froedtert Health User network and system accounts will be deactivated as soon as possible if the Froedtert Health User is suspended, placed on leave or if their employment has been terminated with Froedtert Health.

j) Supervisors / Managers shall immediately contact Froedtert Health Human Resources to report changes in Froedtert Health User status that requires termination or modification of IT access privileges.

k) Froedtert Health Users who forget their password must call the IT Service Desk to have a new password assigned to their account. The Froedtert Health User's identity must be validated by the helpdesk prior to receiving the password.

l) Froedtert Health Users will be responsible for all transactions occurring during Logon sessions initiated by use of the Froedtert Health Users password and user ID. Froedtert Health Users shall not logon to a computer and then allow another individual to use the computer; or otherwise share system access under one account.

P) System Administrator Access
a) System Administrators, network administrators, and security administrators will have privileged and monitored access to systems and network devices as approved and required to fulfill the duties of their job. This access is identified

as “Administrator Access”.

b) All system administrator access will be Removed immediately after any Froedtert Health User with such responsibility has been terminated from Froedtert Health.

Q) Firefighter (Emergency) Access

a) Firefighter accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by Froedtert Health and require the permission of the user’s Froedtert Health IT Manager. Firefighter accounts must be monitored, reviewed regularly and expire within a defined period. Once expired, these accounts will not be automatically renewed without written permission.

R) Connecting to Third-Party Networks

a) This policy is established to ensure a secure method of connectivity provided between Froedtert Health and all third-part companies and other entities required to electronically exchange information with Froedtert Health.

b) “Third-party” refers to vendors, consultants and business partners doing business with Froedtert Health, and other partners that have a need to exchange information with Froedtert Health. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of Froedtert Health. The third-party of Froedtert Health will ensure that only authorized users will be allowed to access information on Froedtert Health network. The third-party will not allow Internet traffic or other private network traffic to merge with or flow into the network.

c) A third-party network connection is defined as:

i) A configuration of communications equipment and communication links by network cabling or satellite which enables computers and terminals from a 3rd party to be geographically separated while still connected to each other.

ii) This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed based on risk.

iii) All requests for third-party connections must be submitted via a written request and be approved by Froedtert Health IT.

S) Connecting Devices to the Production Network

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

b) Users shall not attach to the production network: non-Froedtert Health computers that are not authorized, owned and/or controlled by Froedtert Health. Users are specifically prohibited from attaching any form of networking and or computing devices to Froedtert Health production network (ie; wireless access points, personal laptops, etc).

c) NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD’s.

T) Remote Access

a) Only authorized persons may remotely access Froedtert Health network. Remote access is provided to those employees, contractors and business partners of Froedtert Health that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connections can either be a remote PC to the network or a remote network to a Froedtert Health network connection. The only acceptable method of remotely connecting into the internal network is by using a secure ID.

U) Unauthorized Remote Access and Remote Administration

a) Additionally, users may not install personal software designed to provide remote access or remote control of a PC,

mobile device or workstation. This type of remote access bypasses authorized methods of remote access and poses a threat to the security of the entire network.

V) Mobile Device Management

a) Every mobile device user must use reasonable care, as outlined in the “Mobile Device Procurement and Usage Policy”. Protection of sensitive and controlled information against physical theft or loss, electronic invasion, or unintentional exposure is provided through a variety of means, which include user care and a combination of technical protections such as authentication and encryption that work together to secure electronic data on Mobile Devices.

W) Cybersecurity Policies

a) All information security objectives of Froedtert Health must be mandated and authorized by policy or recommended by a guideline and directed by a standard.

b) All information security policies and standards must be reviewed every three years to ensure they remain up to date and relevant in light of dynamic business priorities and risks.

X) Metrics and Reporting

Metrics for evaluating the efficacy of the Information Security Program must be defined and evaluated on an annual basis at a minimum.

Y) Incident Response

Policies and procedures must be in place to help ensure appropriate detection, response and recovery from malicious incidents that threaten the confidentiality, availability and or integrity of Froedtert Health information assets . Furthermore, all Froedtert Health Users must report incidents in a timely manner.

Z) Penalty for Security Violations

a) Froedtert Health takes the issue of information security seriously. Individuals who use the technology and information resources of Froedtert Health are subject to disciplinary measures up to and including discharge as well as criminal prosecution if they violate this policy. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cybersecurity Baseline Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against a Froedtert Health User shall be administrated in accordance with any appropriate rules or policies and Froedtert Health Policy Manual.

Reference Details

- 164.308 Administrative Safeguards
- 164.310 Physical Safeguards
- 164.312 Technical Safeguards

Issuing Authority

FH Corporate Policy Committee

Distribution

Froedtert Health

Reference Type

HIPAA

category

Information Technology,