Health Care District
PALM BEACH COUNTY

Acceptable Use Policy

Policy #:	ITSEC022	Effective Date:	2/15/2024
Business Unit:	Information Technology	Original Effective Date:	2/15/2024
Approval Group:	IT Security		

PURPOSE

Non-authorized use of corporate systems exposes the company to risk. It is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to establish guidelines for the acceptable use of company information technology resources within the organization. By delineating permissible and prohibited actions, the policy aims to safeguard sensitive data, uphold legal compliance, and mitigate risks associated with unauthorized usage.

This policy will be enforced, and violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

SCOPE

This policy applies to all Workforce Members of the Health Care District of Palm Beach County and its affiliates (the “District”), including but not limited to, Lakeside Medical Center, E.J. Healey Rehabilitation and Nursing Center, School Health, Primary Care Clinics, Pharmacy, Aeromedical, Trauma and Managed Care. The scope of this policy includes use and access of all corporate information and resources, including, but not limited to, computer systems, printers, email, network infrastructure, and the corporate Internet connections.

DEFINITIONS

Blogging: The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging: A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing: A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access: Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media: Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

Workforce Members: Persons who work for or under the direct control of the District including employees, students, residents, interns, staff, volunteers, contractors or other third parties whether or not they are paid by the District.

POLICY

This Policy sets the parameters for use of communication resources, particularly electronic resources, such as e-mail, Internet services, applications, file shares, databases, digital media, and other electronic means ("Electronic Communications") to promote efficient and effective communication in the course of conducting Company business. Electronic Communications and information made available through Company IT systems are Company property, and their primary purpose is to facilitate Company business. Employees must not use external e-mail or systems to conduct Company business. Users have the responsibility to use Electronic Communications in a professional, ethical, and lawful manner in accordance with the Company's Code of Conduct.

Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Bandwidth Usage

Excessive use of company bandwidth or other computer resources is not permitted.

- Definition: Bandwidth refers to the capacity of the network to transmit data. Excessive use implies consuming a disproportionate amount of this capacity.
- Importance: Efficient bandwidth utilization is crucial for maintaining optimal network performance and ensuring that all users have fair and equitable access to network resources.
- Examples of Excessive Use:
    - Constantly downloading large files during peak hours.
    - Engaging in bandwidth-intensive activities, such as streaming high-definition video, for non-work-related purposes.

Blogging and Social Networking

Blogging and social networking by selected employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking are allowed from the corporate computer network if:

- Requested and authorized.

- It is done in a professional and responsible way not harm the reputation of HCDPBC, its partners, or employees.
- Confidential data is not disclosed.
- Performed by authorized employees on behalf of the company's official business.

Additional guidelines regarding the proper and acceptable use of social media are applied in accordance with the Privacy Policy# HCDPRIV225 - Social Media Policy and Procedure.

Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, electronic security policies, technical controls, or escalating privileges is expressly prohibited.

Confidentiality

Confidential data, including but not limited to patient health records, financial information, and proprietary research or data, is limited to a "need-to-know" basis and should not be indiscriminately shared. Underscoring the paramount importance of confidentiality serves as a critical safeguard for the organization's reputation and trust. Obligations to protect sensitive data must align with established legal frameworks, such as HIPAA, reinforcing stringent measures in place to ensure the confidentiality, integrity, and availability of company data. Confidential data must not be:

- Shared or disclosed in any manner to non-employees of the company or individuals that are not in the need to know.
- Shall not be posted on the Internet or any publicly accessible systems.
- Shall be transferred in a secure manner as outlined in the "Physical Security" policy.

Copyright Infringement

The use of the company's computer systems and networks must adhere to copyright laws, ensuring that no illegal or unauthorized copyrighted content is downloaded, uploaded, or otherwise handled. Violations of this acceptable use policy include, without permission from the copyright owner:

- Copying and Sharing: Prohibits copying and sharing of images, music, movies, or other copyrighted material through peer-to-peer (P2P) file sharing or unlicensed CDs and DVDs.
- Posting or Plagiarizing: Explicitly prohibits posting or plagiarizing copyrighted material without proper authorization.
- Unauthorized Downloads: Employees are not permitted to download copyrighted files that have not been legally procured.
-

Note: This list is not exhaustive; copyright law applies to a wide range of works beyond what is specifically mentioned here.

E-mail Use

In pursuit of fostering a workplace environment that prioritizes the security and efficiency of communication, the following email best practices have been established:

- Exclusive Use of HCD Email: By conducting all business activities exclusively through the designated HCD email platform, the organization aims to establish a secure and standardized communication channel. This approach enhances data security and streamlines information exchange within a controlled environment.
- Prohibition of External Email Services: Strict avoidance of external email services, such as Gmail, Yahoo, AOL, etc., for business-related correspondence is mandated. This measure is implemented to uphold the integrity of data security and maintain organizational control over communication channels.
- Reference to Communications Policy: The inclusion of a reference to the company's Communications Policy ensures that employees have access to detailed and nuanced guidance on email usage. This comprehensive policy outlines protocols and procedures, contributing to the overall efficiency and effectiveness of communication practices.

Network Access

To safeguard data security and maintain the integrity of job functions, the following network access policy is established:

- Access Restriction: Users are prohibited from accessing network data, files, and information that are not directly related to their assigned job function.
- Limited Access Implications: The mere existence of access capabilities does not imply permission to utilize this access. Users are expected to access only the information necessary for the successful execution of their job responsibilities.

Instant Messaging

In an effort to maintain controlled and secure communication channels, the following policy governs the use of Instant Messaging (IM):

- Prohibition of External IM Software: The use of Instant Messaging software operating outside the corporate network is strictly prohibited. This includes, but is not limited to, IM platforms such as AOL, Yahoo, Facebook, and Google instant messengers.
- Authorized Company IM Software: Only company-provided Instant Messaging software is authorized for communication. Usage is permissible only for personnel deemed appropriate by

Business Unit Managers and with proper written approval, as outlined in the "Communications Policy."

Additional responsibilities on the use of instant messaging and secure texting by workforce members to communicate confidential data, including but not limited to, protected health information (PHI) and personally identifiable information (PII) is outlined in Policy# ITSEC-0001 - Instant Messaging and Secure Texting Policy and Procedure

Monitoring and Privacy

In the interest of safeguarding security and ensuring adherence to company policies, the following policy governs monitoring and privacy on the corporate network:

- No Expectation of Privacy: Users are advised that they should expect no privacy when utilizing the corporate network or company resources. This includes the transmission and storage of files, data, and messages.
- Right to Monitor: The company expressly reserves the right to monitor all use of the computer network. This monitoring encompasses the interception and review of emails or other messages sent or received, as well as inspection of data stored on personal file directories, hard disks, and removable media.

Non-Company-Owned Equipment

To uphold network security and compliance standards, the following governs the use of non-company-owned equipment, including Bring Your Own Device (BYOD), on the company's corporate network:

- Prohibition of Non-Company-Owned Equipment: The use of non-company-provided equipment, including BYOD, is expressly prohibited on the company's corporate network.
- Exception for Guest Networks: This policy does not extend to wired and/or wireless guest networks, where non-company-owned equipment may be permissible.

Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

Peer-to-Peer File Sharing

P2P networking is not allowed on the corporate network under any circumstance.

Personal Storage Media

Personal storage devices represent a serious threat to data security and are prohibited on the company's network.

Remote Desktop Access

Use of remote desktop software and/or services is allowable if it is provided by the company. Remote access to the network must conform to the company's "IT Infrastructure Access and Authentication Policy".

Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify their supervisor who in turn must notify IT Department personnel and/or follow any applicable guidelines as detailed in the corporate "Incident Response Policy". In addition, users must not withhold information relating to a security incident or interfere with an investigation. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact the company's information security.

All workforce members have the responsibility to report all known or suspected data privacy and information security breaches in accordance with Policy# HCDPRIV220 - Reporting of Information Privacy and Security Breaches Policy and Procedure.

Software Installation

Installation of non-company-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software. Malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts and/or have a negative impact on system performance.

Streaming Media

Streaming media can use a great deal of network resources and must be used carefully. Streaming media is allowed for job-related functions only.

Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user shall not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.

- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages and/or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network traffic sniffing, data monitoring, keystroke logging, password capture, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unauthorized/unapproved, unlicensed, or "pirated" software and hardware.
- Log into or attempt to log into company systems or assets that the user does not have explicit rights to do so.
- Engaging in denial of service or “hacking” activities of internal or external systems.
- Any form of online gambling.
- Reveal passwords designated for company use of any kind. This includes family, friends, or other members of the household when working from home or remote locations.

Use for Illegal Activities

No company-owned or company-provided computer systems may be knowingly or unknowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions include, but are not limited to, the following:

- Unauthorized Port Scanning.
- Unauthorized Network Hacking.
- Unauthorized Packet Sniffing.
- Unauthorized Packet Spoofing.
- Unauthorized Denial of Service.
- Unauthorized Wireless Hacking.
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system.
- Acts of Terrorism.
- Identity Theft.
- Spying.
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues.

- Downloading, storing, or distributing copyrighted material, the company will take all necessary steps to report and prosecute any violations of this policy.

Web Browsing

The Internet is a network of interconnected computers, servers, network equipment, and peripheral devices. The user shall recognize this when using the Internet for job related purposes and understand that it is a public domain. The user can encounter information, even inadvertently, which the user may find offensive, sexually explicit, or inappropriate. The user must utilize the Internet for job related purposes at their own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

ENFORCEMENT

This policy is enforced by the AVP, IT & Business Intelligence and/or Executive Leadership. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

EXCEPTIONS

Exceptions to this policy are granted by submitting the appropriate request through an individual Department Manager, verified by the IT Security Director, with recommendation to the AVP, IT & Business Intelligence for final approval.

RELATED DOCUMENTS

Related Policy Document(s)	HCDPRIV225 - Social Media Policy and Procedure HCDPRIV220 - Reporting of Information Privacy and Security Breaches Policy and Procedure ITSEC-0001 - Instant Messaging and Secure Texting Policy and Procedure
Related Forms	
Reference(s)	
Last Revision	
Revision Information/Changes	

APPROVALS	
Reviewer approval	[Reviewers]
Reviewer approval date	[Date Review Completed]
Final approver	[Approvers]
Final approval date	2/20/2024

This policy is only intended to serve as a general guideline to assist staff in the delivery of patient care; it does not create standard(s) of care or standard(s) of practice. The final decision(s) as to patient management shall be based on the professional judgement of the health care providers(s) involved with the patient, taking into account the circumstances at that time. Any references are to sources, some parts of which were reviewed in connection with formulation of the policy/procedure. The references are not adopted in whole or in part by the hospital(s) or clinic(s) / provider(s).

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.