care resource

Your Community's Source for Healthcare

ACCEPTABLE USE

Policy Number

4005.005

Policy Category

Information Services

Target Audience

All Care Resource Employees

Overview

This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor. Unacceptable use of these resources can place Care Resource, its staff, clients/patients and/or data at risk.

Purpose

Since inappropriate use of corporate systems exposes Care Resource to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

Policy

The policy includes any use of corporate information resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection.

Network Access

As the user will be given access to the corporate network, Internet, and other IT resources, Care Resource expects the user to use these resources in a responsible manner.

Web Browsing and Internet Usage

The Internet is a network of interconnected computers that Care Resource has little control over. The user must recognize this when using the Internet and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate, or that may be illegal in some jurisdictions.

User should use the Internet to accomplish Care Resource business only. While on company time, user may not use the internet for personal business. Care Resource is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

Personal Use

Care Resource recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet including, and not limited to, personal subscription and commerce services, shopping, media streaming and any other use that is not related to company business is not permitted.

Peer-to-Peer File Sharing

Peer-to-Peer (P2P) file sharing/networking is not allowed on the corporate network under any circumstance.

Streaming Media

Streaming media can use a great deal of network resources, slow down others activities and thus is not allowed without approval.

Blogging

Blogging by Care Resource's employees is subject to the terms of this policy, whether performed from the corporate network, personal systems, or other external systems. The user is asked to recognize that information posted on a blog immediately becomes public information and thus to exercise extreme discretion in the type of information posted. In no blog or website, including blogs or sites published from personal or public systems, shall internal company business matters be discussed, confidential data released, or material detrimental to Care Resource published.

As long as company policies, as specified herein, are followed, Care Resource allows the publishing and use of blogs for authorized personnel only. When done from the corporate network or during business hours, blogging must be business related. The user assumes all risks associated with blogging.

Instant Messaging

The user should recognize that instant messaging technology, unless specific encryption measures are taken, is an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data. Unencrypted confidential data must never be sent via instant messaging technologies.

Bandwidth Usage

Excessive use of company bandwidth or other computer resources, where not required by job function, is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide bandwidth usage, such as after regular business hours.

Care Resource may restrict bandwidth for certain services deemed non-critical to company operations, or as it sees fit to preserve network functionality.

Social Networking/Social Media

Social networking creates risks for Care Resource in two ways: 1) in the potential sharing of company confidential, private, or embarrassing information, and 2) the potential for an attacker to use posted information to craft a social engineering attack on Care Resource. The user is asked to recognize that information posted on social networking sites is public information and to exercise extreme discretion in the type of information posted. No confidential information or company secrets are to be posted on social networking sites. The user must not publish any information detrimental to Care Resource, or that would cause embarrassment to Care Resource, on social networking sites.

As long as company policies, as specified herein, are followed, Care Resource allows reasonable use of social networking sites from its network and/or during business hours to only authorized personnel. This use must be business related. The user assumes all risks associated with social networking.

Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This section is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable.

Prohibited Actions

The user may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law (see section “Use for Illegal Activities” for more information).

- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to Care Resource.

- Download, store, or distribute violent, pornographic, obscene, lewd, or offensive material.

- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages 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.

- Reveal personal or network usernames or passwords to others, including co- workers, family, friends, or other members of the household when working from home or remote locations.

Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or the escalation of privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent company security systems is expressly prohibited. This includes disabling or tampering with any company supplied security software, such as antivirus/anti- malware software, firewall software, or remote access software.

Use for Illegal Activities

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

- Unauthorized Port Scanning.

- Unauthorized Network Hacking, including: packet sniffing, port scanning, packet spoofing, denial of service (DoS), 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.

- Cybercrime, extortion, or Identity Theft.

- Downloading, storing, or distributing any material prohibited by law.

- Downloading, installing, or distributing unlicensed or "pirated" software.

- Sending unsolicited bulk email or other messages deemed illegal under applicable regulations.

Where illegal activities are discovered, Care Resource will take all necessary steps to report the activities to the relevant authorities and will cooperate with any resulting prosecution.

Overuse

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

Copyright Infringement

Care Resource's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the Acceptable Use Policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material via peer-to-peer file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above.

Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. Care Resource reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received; inspection of data stored on personal file directories, hard disks, and removable media; and monitoring of Internet/network usage.

Responsible Computer and Network Use

Care Resource expects users to use the network responsibly. Personal usage of company computer systems is not permitted.

Device/Equipment Assignment

Care Resource will provide and allocate equipment for employees to fulfill their job functions. Staff will be assigned either a desktop or a laptop computer. To obtain both a desktop and a laptop computer, department manager/director must make a request for approval.

Non-Company-Owned Equipment

Non-company-provided computer equipment is expressly prohibited from being connected to Care Resource's network. Examples of this are: laptops, notebooks, tablet computers, network devices, smartphones, etc.

Removable Media

Personal (non-company-owned) storage devices represent a serious threat to data security and are expressly prohibited from being connected to Care

Resource's network. Examples of this are: USB drives, flash storage, media players, etc.
Storage media supplied by Care Resource is allowed, however guidelines on confidential/ePHI, such as those found in the Confidential Data and Mobile Device Policies, must be strictly followed.

Software Installation

Installation of non-company-supplied software applications 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 or have a negative impact on system performance.

Reporting of a Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. 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, keycard, or two-factor authentication token
- 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.
Users must treat a suspected security incident as confidential information and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

Users should recognize that if an incident includes confidential information, particularly if the information involves ePHI, the Sanction Policy details disciplinary actions.
Incidents not involving confidential information will be handled at the discretion of the Information Security Manager as well as appropriate supervisory and/or management personnel.

Applicability of Other Policies

This document is part of Care Resource'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 necessary.

Enforcement

This policy will be enforced by the Information Security Manager and/or Senior Management Team. 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, Care Resource may report such activities to the applicable authorities.

Approved by:

- Print and Sign Name Rick Siclari, MBA- CEO

Effective Date

- 2/23/2021

Revised Date

- 8/8/2023

Reviewed Date

- 8/9/2023

Distribution Date

- 8/29/2023