



CureMD

Acceptable Use of Assets, Applications & Network Services (AUP)



Contents

1. Overview.....	3
2. Purpose.....	3
3. Scope	3
4. General Use and Ownership.....	3
5. Unacceptable.....	3
6. Clear Desk and Clear Screen Policy.....	5
7. Access to Home Drives	5
8. Issue Tracking System.....	6
9. Equipment Borrowing.....	6
10. Power Management	6
11. Enforcement	6

1. Overview

The Acceptable Use Policy (AUP) is designed to foster a secure, efficient, and legally compliant work environment. This policy does not intend to impose restrictions that conflict with CureMD's culture of openness, trust, and integrity. However, it is necessary to protect CureMD, its employees, partners, and stakeholders from illegal or harmful actions, whether intentional or unintentional. CureMD's Internet, Intranet, and Extranet systems—including but not limited to computer equipment, software, operating systems, storage media, and network accounts (e.g., email, web browsing, FTP)—are company property. These systems are intended for business purposes to serve the interests of CureMD and its clients during normal operations.

Effective security is a collective responsibility, requiring the participation and support of every individual who interacts with CureMD's information and systems. Each user must understand these guidelines and adhere to them accordingly.

2. Purpose

This policy outlines the acceptable use of IT equipment and resources at CureMD. The rules set forth are intended to protect the company and its employees from risks such as virus infections, network breaches, service interruptions, and legal liabilities resulting from inappropriate use.

3. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at CureMD, including personnel affiliated with third parties. It governs the use of all equipment owned or leased by CureMD.

4. General Use and Ownership

- While CureMD strives to provide a reasonable expectation of privacy, users should be aware that any data created on corporate systems is the property of CureMD.
- Authorized personnel may monitor equipment, systems, and network traffic at any time to ensure compliance with this policy and for security and maintenance purposes.
- Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information is strictly prohibited and will result in disciplinary action.


5. Unacceptable Use

Users are prohibited from engaging in activities that are illegal under local, state, federal, or international law while using CureMD's resources. The following activities are strictly prohibited:

5.1. System and Network Activities

The following actions are considered security breaches and are forbidden:

- Violating copyright, trade secret, patent, or other intellectual property rights.
- Unauthorized copying, distribution, or use of copyrighted or proprietary materials, including CureMD's client information, to or from unauthorized recipients or domains.

	Version # 1.5
	Title: Acceptable Use of Assets, Applications & Network Services (AUP)

- Exporting software, technical information, or encryption technology in violation of applicable laws.
- Introducing malicious software into the network or servers, such as viruses, worms, Trojan horses, or email bombs.
- Sharing your account credentials with others or allowing unauthorized use of your account.
- Using CureMD computing assets to download, view, or transmit inappropriate content, such as obscene or explicit material.
- Making fraudulent offers of products or services using a CureMD account.
- Disrupting network communications or conducting unauthorized access to data or systems. This includes, but is not limited to, activities such as network sniffing, ping floods, packet spoofing, denial of service attacks, and forging routing information for malicious purposes.
- Performing port scanning or security scanning without prior authorization from IT.
- Engaging in network monitoring activities that intercept data not intended for your use, unless such activities are part of your job duties and explicitly approved by IT.
- Using programs, scripts, or commands to interfere with or disable another user's session, whether locally or over the network.
- Disclosing information about CureMD employees to unauthorized external parties.
- Connecting non-business-related servers to CureMD's network. Only servers required for CureMD's business operations are allowed.

5.2. Email and Communication Activities

The following email and communication practices are prohibited:

- Sending unsolicited emails (spam) or advertising materials to individuals who have not requested them.
- Engaging in any form of harassment via email, telephone, or paging, whether through inappropriate language, excessive frequency, or large message sizes.
- Forging email header information or using unauthorized email addresses.
- Soliciting responses for any email address other than your own with the intent to harass or collect replies.
- Creating or forwarding chain letters or similar schemes.
- Sending unsolicited emails from CureMD's network to advertise any service hosted by or connected to CureMD.

Email Signature Requirement:

Emails containing confidential information must include the following confidentiality notice:

"This email and any attachments may contain confidential or proprietary information. If you are not the intended recipient, please notify the sender immediately and delete this message. Unauthorized use, copying, or distribution is prohibited."

5.3. Internet Usage

The following internet activities are prohibited:

- Posting CureMD-related material on publicly accessible websites, including but not limited to YouTube, Google Docs, Facebook, RapidShare, Hotmail, Google Drive, Dropbox, or similar services.
- Using software or proxy sites to bypass CureMD's website filtering mechanisms.
- Downloading software from the internet without prior approval.
- Accessing websites that contain offensive, sexually explicit, terrorist-related, or otherwise inappropriate material.
- Visiting non-work-related websites. Only work-related sites should be accessed, and violations will be subject to disciplinary action.

5.4. Electronic Gadgets

Bringing or using electronic gadgets on CureMD premises without prior approval from the Systems or InfoSec departments is strictly prohibited. Prohibited devices include, but are not limited to:

- Laptops
- Cameras
- CDs/DVDs
- USB drives, SD cards, MMC cards, or any other flash-based storage devices
- Any portable storage devices (e.g., notebooks, PDAs)


6. Clear Desk and Clear Screen Policy

To ensure the confidentiality and security of sensitive information, all users are required to follow these guidelines:

- When leaving a meeting room, always erase any sensitive information from whiteboards, screens, or other surfaces to prevent unauthorized access.
- Secure any confidential, sensitive, or critical business documents by locking them away or shredding them when no longer needed.
- Log off or lock your workstation when unattended to prevent unauthorized access. All screen savers must be password protected.
- If working on sensitive information and a visitor is present at your desk, lock your screen to prevent unauthorized viewing.
- Avoid placing sensitive or confidential data on your desktop screen to minimize the risk of unauthorized disclosure.
- Copying and printing technology must only be used for authorized business purposes. Users must immediately collect printed documents and ensure that sensitive information is not left unattended on printers or copiers.

7. Access to Home Drives

CureMD provides all staff with a network (H:) drive for the purpose of backing up data used in day-to-day operations. This drive is for official use only. Any misuse that violates the company's information security policies will result in disciplinary action.

	Version # 1.5
	Title: Acceptable Use of Assets, Applications & Network Services (AUP)

8. Issue Tracking System

For quality control and tracking purposes, the IT department provides an Issue Tracking System. All IT-related issues/requests must be generated through this ticketing system. Requests submitted outside this system will not be processed. To access the Issue Tracking System, use the following link. If you encounter an access denied message, request access from the IT department or your team lead/manager. Access requests are a one-time process. It is advisable to bookmark below URL in your Internet Explorer favorites.

<http://cmdlhrsp02:1111/Lists/Issue%20Tracking/MyItems.aspx>

9. Equipment Borrowing

All equipment, such as laptops and projectors, must be reserved with the IT department at least 24 hours in advance to ensure availability. Borrowers must check out and return equipment through the IT department. Borrowers are responsible for the equipment during the loan period and must return it in the same condition as when it was issued.

10. Power Management

Sustainable IT practices are integral to CureMD's commitment to environmental responsibility. To support cost savings and sustainability efforts, CureMD personnel should adhere to the following guidelines at the end of each shift:

- Sign out of your workstation to ensure all running processes are properly closed, preventing unnecessary resource consumption.
- Turn off all attached peripherals.
- Turn off monitors, LCDs, or LEDs if you will be away from your desk for 20 minutes or longer.

11. Enforcement

Any user found in violation of this policy will be subject to disciplinary action, up to and including termination of employment.