CureMD

CureMD Acceptable Use Policy (AUP) of Assets, Applications and Network Services

Contents

OVERVIEW

The intentions for publishing an Acceptable Use Policy are not to impose restrictions those are contrary to company established culture of openness, trust and integrity. CureMD is committed to protecting its employees, partners and the company from illegal or destructive actions by individuals, either intentionally or un-intentionally.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing email, WWW browsing, and FTP, are the property of company. These systems are to be used for business purposes in serving the interests of the company, and for our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every company related user to understand these guidelines, and to conduct their activities accordingly.

PURPOSE

The purpose of this policy is to outline the acceptable use of IT equipment at CureMD. These rules are in place to protect the employee and company. Inappropriate use, exposes the company to risks including virus attacks, compromise of network systems and services and legal issues.

SCOPE

This policy applies to employees, contractors, consultants, temporary employees and other workers at the company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the company.

GENERAL USE AND OWNERSHIP

- While CureMD desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of CureMD.
- For security and network maintenance purposes, authorized individuals within the company may monitor equipment, systems and network traffic at any time or on a periodic basis to ensure compliance with this policy.
- Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of any information is strictly prohibited and will lead to appropriate disciplinary action.

UNACCEPTABLE USE

The following activities are, in general, prohibited and under no circumstances is any user

Authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company owned or related party resources.

The lists below, covers the activities which fall into the category of unacceptable use. Such activities would be considered a security breach and evoke punitive actions.

1. System and Network Activities

Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CureMD.

- Never leave your workstation / computer / laptop unlocked and unattended while when you are away from your desk.
- Always shutdown your workstation / computer /laptop before you leave at day end.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CureMD or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of International or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., malware, viruses, worms, Trojans, e- mail bombs, etc.).
- Revealing allocated account/accounts password/s to others or allowing use of your account/s by others. This includes family and other household members.
- Using a CureMD computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any CureMD account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Port scanning or security scanning, installation of certain services is expressly prohibited unless prior approval from IT is obtained.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purpose.
- Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.   Any such activity, which is part of normal duty/project requirement, needs prior and explicit approval from IT.
- Only CureMD business related servers are allowed to connect through provided facilities. All other remote desktop connections will be considered security breach.

2. Email and communication activities

- The official email facility accessible through CureMD infrastructure should be used for legitimate official purposes only.
- Usage of web email service through CureMD or related Infrastructure.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who have not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other such schemes of any type.
- Use of unsolicited email originating from within CureMD' s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CureMD or connected via CureMD' s network.
- Instant Messenger facility will be available only to the managers and team leads of the all departments. This facility will also be available to anyone who is working on the important assignment but this will be conditional and will need to have proper justification with approval for this. The reason for restricting this facility to the managers and team leads is that so the people can better concentrate on their tasks and do not waste their time in other activities through communicator. If they will want to interact with someone from other department they can use the facility of phone, email etc.

3. Internet Usage

- Users must not place any CureMD related material in publicly accessible Internet sites like but not limited to YouTube, Google doc, Facebook, Rapid share, Hotmail, Google Drive, Drop box etc. and similar services.
- Use software or proxy sites for bypassing the web site filtering mechanism.
- Download software from the internet without prior approval.
- Access of web sites including but not limited to offensive, sexually explicit, terrorist, and morally inappropriate material.
- Only work-related websites are allowed to be visited. Any employee found visiting the following website categories will be guilty and management can act for violation.

Please note that the policy is not limited to the following groups only.

BY CONTENT/ TOPIC	BY INFORMATION
- General - Jobs - Mobile/Handheld - News - Entertainment - Sports - Social Network - Real Property - Television - Gaming - Streaming - Pornographic - Cloud Drives	- Blog - Personal Email (Hotmail, Yahoo, Gmail etc.)

4. ELECTRONIC GADGETS

Carrying or attaching any Electronic Gadgets inside CureMD premises without prior permission from Systems department is strictly prohibited. Devices include but not limited to;

a) Cameras
b) CD/DVD
c) USB/SD/MMC/ or any flash-based disks
d) Any portable storage devices (Notebooks, PDAs, etc.)

CLEAR DESK AND CLEAR SCREEN

User will be accountable for all terminal activities and transactions/transmissions made through his/her network username whether or not he/she was present at the time.

USERS MUST ENSURE THE FOLLOWING WHILE PERFORMING THEIR OPERATIONAL TASKS;

a) Confidential, sensitive or critical business information, on paper, should be locked away when not required or shred using the Paper Shredder inside the office.
b) Terminals should be left logged off or protected with a screen locking mechanism, (i.e. ctrl, alt, Del and enter, lock computer) when unattended. All screen-savers must be password protected.
c) If working on sensitive information, and you have a visitor at your desk, it is advised to lock your screen to prevent the contents being read.

COMPUTER EQUIPMENT WHICH IS LOGGED ON AND UNATTENDED CAN PRESENT A TEMPTING TARGET FOR UNSCRUPULOUS STAFF OR THIRD PARTIES ON THE PREMISES;

a) Unauthorized access of an unattended workstation can result in harmful or fraudulent entries, e.g. modification of data, fraudulent e-mail use, etc.
b) Access to an unattended workstation could result in damage to the equipment, deletion of data and / or the modification of system / configuration files.

ACCESS TO HOME DRIVES

All CureMD staff is provided with a network drive H: (Home) drive with the purpose to back up your data which is used for day to day operations. This drive shall be used for official purposes only and any act or incident that could violate Companies Information Security requirements originating from its usage shall be dealt with appropriate disciplinary actions.

ISSUE TRACKING SYSTEM

For quality control and tracking purposes the IT department provides all team members with an Issue Tracking System and it is mandatory for all staff members to generate a ticket in the mentioned system for IT related issues. No request besides the ones properly entered in the Issue Tracking System will be entertained by the IT department. Please visit the following link to access the Issue Tracking System; and if you get an access denied message then please send

a request to the IT department or your team lead/Manager. Access request will be a one-time process and this URL is already added to your Internet Explorer Favorite Links.

- http://cmdlhrspp02:2222/SiteDirectory/IT/Lists/Issue%20Tracking/MyItems.aspx

POWER MANAGEMENT

Sustainable IT is an important piece in the overall corporate focus to help improve the company environment. To create cost savings and improve company environment, CureMD personnel should also play an important role by following these instructions.

a) Turn off workstations and monitors at the end of the shift.
b) Turn off attached peripherals at the end of their shift.
c) Turn off monitors/LCDs/LEDs when leaving their seat for 10 minutes or more

If for any reason, anyone needs to leave their system ON after their shift ends, please **inform** DC Systems dc.systems@curemd.com through email with reason.

ENFORCEMENT

Any user who is found to be in violation of these rules shall be subject to disciplinary action.