



# QUADRANT TECHNOLOGIES

## Acceptable Usage Policy

Version 2.1

### Revision History

Version #	Date (DD-MMM-YYYY)	Details of the Changes	Modified By	Reviewed & Approved By
1.0	1 Sep 2020	First Release	SK Javed	Sridhar Reddy
1.0	10 Oct 2021	Reviewed No Changes Made	SK Javed	Sridhar Reddy
1.0	5 Oct 2022	Reviewed No Changes Made	SK Javed	Sridhar Reddy
1.0	4 July 2023	Reviewed No Changes Made	SK Javed	Sridhar Reddy
2.0	24 Oct 2023	2.3 Laptop/Desktop System Usage	Manu Mitragotri	Sridhar Reddy
2.1	26 Mar 2024	2.3 Laptop/Desktop System Usage	Manu Mitragotri	Sridhar Reddy

## Contents

---

1	Purpose and Scope .....	3
1.1	Overview .....	3
1.2	Purpose .....	3
1.3	Scope .....	3
2	Policy Standards .....	3
2.1	General use and Ownership .....	3
2.2	Security and Proprietary Information.....	4
2.3	Laptop/Desktop System Usage .....	4
2.3.1	Fault Logging.....	5
2.4	Management Rights to Review .....	6
2.5	Unacceptable Use.....	6
2.5.1	System and Network Activities.....	6
2.5.2	Email and Communication Activities .....	7
2.5.3	Blogging and Social Media .....	8
3	Compliance .....	8
4	Non-Compliance .....	9

## **1 Purpose and Scope**

---

### **1.1 Overview**

- Chief Information Security Officer (CISO)'s intention for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Quadrant's established culture of openness, trust and integrity.
- CISO is committed to protecting Quadrant's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, exposing to risks including virus attacks, compromise of network systems and services.
- All computer equipment, software, operating systems, storage media, network accounts providing electronic mail, browsing, and FTP, are the property of Quadrant.
- These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

### **1.2 Purpose**

- This policy addresses Quadrant's intent to safeguard computing resources from Internet and email based threats.
- This policy shall underline appropriate user etiquette for workstation, Internet and email usage and define procedures for safeguards from Internet and email borne threats.
- This policy aims to be a concise document intended to be distributed to all Quadrant employees.
- The purpose of this policy is to outline the acceptable use of computer equipment at Quadrant.
- These rules are in place to protect the employee and Quadrant.

### **1.3 Scope**

- This Policy applies to all Employees, Contractors, Vendors, Employees of Third Parties associated with Quadrant and Consultants having business relationships with Quadrant.
- This policy covers logical and physical boundaries of Quadrant.
- This policy covers all Quadrant's network, Operations area, IT systems, data and authorized users, Public users within logical and physical boundaries.

## **2 Policy Standards**

---

### **2.1 General use and Ownership**

- Quadrant's proprietary information stored on electronic and computing devices whether owned or leased by Quadrant, the employee or a third party, remains the sole property of

Quadrant. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Quadrant proprietary information.
- Users may access, use or share Quadrant proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Quadrant may monitor equipment, systems and network traffic at any time, per CISO's Audit Policy.
- Quadrant reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 2.2 Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Remote Working Policy.
- System level and user level passwords must comply with the Password Protection Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### 2.3 Laptop/Desktop System Usage

- Users should only use company issued laptop/desktop for their official computing needs.
- Users are responsible for protecting the confidentiality/availability/integrity of their systems data.
- The assigned user of the system has to maintain full responsibility of the security of the system issued to him/her.
- Users for whom their Laptop are given, must carry it to office all the times and to be producing for verification by the IT department when needed.
- Users are requested not to remove the Asset Identification and Licensing sticker attached to the assets.

- Self-servicing of laptop/desktop and changes to hardware/software configuration without IT department approval is strictly prohibited.
- Users will bear the servicing cost of physical damages done to the company Assets. The Company does not charge for regular wear and tear of assets but does expect the employee to handle company assets with care such that the life of asset is prolonged. Any wear and tear beyond the normal expected rate will be charged to the employee as such.
- Users can mention necessary specifications needed for their job function before taking handover from the IT Department.
- Only legally valid and business-related Applications Software to be installed. No unlicensed software or applications may be used in the organization.
- Employees may not take the notebook computer for repair to any external agency or vendor at any point of time.
- Any software bought from outside vendors or contractors should be installed only after proper permission from the IT Department has been obtained.
- All business files should be stored in the central file server in their respective departments' folders. Access will be provided only based on NEED TO KNOW principle.
- Critical information with classification CONFIDENTIAL or RESTRICTED should be stored in local laptop/desktop after management approval and should be strictly password protected. All such data / files should also be backed up to secured zone on file server.
- If any system is used by multiple users, no sensitive information should be stored in it.
- Systems assigned to third parties or contractors should not have any sensitive information stored in it.
- Using Laptop/Desktop without installation of company approved Antivirus client software is strictly prohibited.
- Using Laptop/Desktop without domain controller authentication is strictly prohibited.
- Laptop/Desktop should always be in locked condition when not in use. Users will ensure the Laptop/Desktop is protected from unauthorized usage and access to information.
- Users will only use Quadrant's provided laptops for accessing client accounts (including email, Slack or any other client's applications) and refrain from using any public or personal devices to access the same. Violating this policy may result in disciplinary consequences.

### 2.3.1 Fault Logging

- Any laptop given to the IT department for repair, for such laptops, the ownership of the security shall lie with the IT department till the laptop is handed back to the user.
- In the case of theft/missing of laptops, the incident is to be reported to the IT department immediately and users shall agree to the necessary corrective actions taken.
- All the system faults should be logged through email or verbal and rectified in a systematic manner and records should be maintained for the same.

## **2.4 Management Rights to Review**

- The Management reserves the right to, without prior notice, examine e-mail, personal file folders, Web browser Book Marks, Cache files etc. to ensure adoption to Quadrant Policies or Procedure as per legal requirements.
- All the e-mails are Quadrant property and are liable to be read, intercepted and if necessary, deleted.
- Quadrant may also disclose e-mail messages sent or received to law enforcement officials without prior notice to the employees who may have sent or received such messages. Users should restrict their communications to business matters in recognition of this electronic monitoring.
- The Management must, however, explicitly authorize monitoring of e-mail for the above-mentioned reasons. Unless specifically delegated, the task of monitoring e-mail messages by all other employees is prohibited. Quadrant should ensure backup of e-mail messages stored in the server, as per the backup guidelines.

## **2.5 Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Under no circumstances is an employee of Quadrant authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Quadrant-owned resources.

### **2.5.1 System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

- Violations 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 Quadrant.
- 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 Quadrant or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Quadrant business, even if you have authorized access, is 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., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Quadrant 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 Quadrant account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee 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 purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to CISO is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Quadrant network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Quadrant employees to parties outside Quadrant.

### 2.5.2 Email and Communication Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did 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", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Quadrant's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Quadrant or connected via Quadrant's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### 2.5.3 Blogging and Social Media

- Blogging by employees, whether using Quadrant's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Quadrant's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Quadrant's policy, is not detrimental to Quadrant's best interests, and does not interfere with an employee's regular work duties. Blogging from Quadrant's systems is also subject to monitoring.
- Quadrant's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Quadrant confidential or proprietary information, trade secrets or any other material covered by Quadrant's Confidential Information policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Quadrant and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Quadrant's Non-Discrimination and Anti-Harassment policy.
- Employees may also not attribute personal statements, opinions or beliefs to Quadrant when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Quadrant. Employees assume any and all risk associated with blogging.

## 3 Compliance

---

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the policy owner.



## **4 Non-Compliance**

---

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.