Acceptable Use Policy

Table of Contents

1. Overview

Cactus Communications Private Limited, including all its global affiliates and group companies ("CACTUS / "Company" / "we" / "us" / "our" is committed to protecting its Users (as defined below) and CACTUS from illegal or damaging actions by individuals, either knowingly or unknowingly.

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

Effective security is a team effort involving the participation and support of every User who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct his/her activities accordingly.

2. Purpose

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

3. Scope

This Policy applies to all employees, directors, volunteers, contractors, consultants, freelancers, interns, trainees and personnel affiliated with CACTUS whether associated directly or on behalf of third parties, whether part-time, full-time or telecommuting) (hereinafter collectively referred to as "Users"). This Policy applies to all equipment that is owned or leased by CACTUS.

4. Policy

4.1 General Use and Ownership

- While CACTUS' network administration 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 CACTUS. Because of the need to protect CACTUS's network, management cannot guarantee the confidentiality of personal information stored on any network device belonging to CACTUS.
- Users are responsible for exercising good judgment regarding the reasonableness of personal use. Users should be guided by the IT/Security Policy on personal use, and if there is any uncertainty, Users should consult their manager or Information Security Manager.
- Users must promptly report the theft, loss, or unauthorized disclosure of CACTUS's confidential or proprietary information to their manager or Information Security Manager.
- Users should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of CACTUS's systems.
- Users should not intentionally access, create, store, or transmit material which CACTUS may deem to be offensive, indecent, or obscene.
- For security and network maintenance purposes, authorized individuals within CACTUS may monitor equipment, systems, and network traffic at any time, as per CACTUS's audit Policy. Apart from this, CACTUS also reserves the right to audit networks and systems periodically to ensure compliance with this policy.

4.2 Security and Proprietary Information

- The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined in the non-disclosure agreements. Users should take all necessary steps to prevent unauthorized access to confidential information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level and user level passwords should be changed every 180days.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging- off when the host will be unattended.
- Postings by Users from a CACTUS email address should contain a

disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CACTUS, unless posting is in the course of business duties.

- All hosts used by the Users that are connected to the CACTUS Internet/Intranet/Extranet, whether owned by the User or CACTUS, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
- Users are permitted to use only those network and host addresses issued to them by the CACTUS IT team and should not attempt to access any data or programs contained on CACTUS systems for which they do not have authorization or explicit consent.
- All remote access connections made to the internal CACTUS networks and/or environments must be made through approved CACTUS-provided virtual private networks (VPNs).
- Hardware, software, network services, and support provided by the organization for VPN or remote usage are for the exclusive purpose of performing or fulfilling job responsibilities. Use of these resources is contingent on Users' agreement to comply with this policy and directions for and/or restrictions of use of these resources as determined by IT personnel.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

5. Unacceptable Use

- The following activities are, in general, prohibited. Users may be exempted from these restrictions during 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 a User of CACTUS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CACTUS-owned resources.
- The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

6. 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 CACTUS.

- 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 CACTUS 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., 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 CACTUS 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 CACTUS account.
- Making statements about discounts/compensations, 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 CACTUS 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.
- 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 CACTUS's Users to parties outside CACTUS.
- Mobile devices should not be used to store personally identifiable information, other legally protected types of data, or any other sensitive or proprietary information.

7. Email and Communications 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 CACTUS's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CACTUS or connected via CACTUS's network.
- Posting the same or similar non-business-related messages to large numbers of usenet newsgroups (newsgroup spam).
- Users are responsible for the accounts assigned to them and for the actions taken with their accounts.

8. Blogging

- Blogging by Users, whether using CACTUS'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 the CACTUS's systems to engage in blogging is acceptable, if it is done in a professional and responsible manner, does not otherwise violate CACTUS's policy, is not detrimental to CACTUS's best interests, and does not interfere with an employee's regular work duties. Blogging from CACTUS's systems is also subject to monitoring.

- CACTUS's confidential information policy also applies to blogging. As such, Users are prohibited from revealing any CACTUS confidential or proprietary information, trade secrets or any other material covered by CACTUS's confidential information policy when engaged in blogging.
- Users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of CACTUS and/or any of its Users. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by policies at CACTUS.
- Users may also not attribute personal statements, opinions, or beliefs to CACTUS when engaged in blogging. If a User is expressing his or her beliefs and/or opinions in blogs, the User may not, expressly, or implicitly, represent themselves as an employee or representative of CACTUS. Users assume all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, CACTUS trademarks, logos, and any other intellectual property of CACTUS may also not be used in connection with any blogging activity.

9. Enforcement

Non-Compliance: Any User found to have violated this Policy may be subject to disciplinary action as defined under CACTUS' Disciplinary Policy, up to and including termination of employment / contract.

Compliance Measurement: CACTUS IT team will verify compliance to this Policy through various methods, including but not limited to, business tool reports, internal and external audits, and monitoring and reviewing the Policy periodically.

10. Security Breach

“Security Breach” shall mean the unauthorized acquisition, access, use or disclosure of information/data which compromises the security or privacy of CACTUS, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

In the event of a Security Breach, User should immediately report such breach to the Information Security Manager.

All Users must report any weaknesses in CACTUS’s computer security and any incidents of possible misuse or violation of this Policy to their immediate supervisor and/or CACTUS IT team or Information Security Manager at itsupport@cactusglobal.com.

All incidents that come to notice shall be promptly and thoroughly inspected. Inspections shall be conducted by trained IT individuals who have proper knowledge and expertise against the reported incident.

We aim to arrive at a time-bound resolution (generally within 90 days) while keeping the parties informed of progress. The Company ensures that the doer rectifies their action going forward.
The Company aims to maintain comprehensive records of all complaints and investigation outcomes securely.

11. Communication & Training

It is our commitment to ensure that this Policy is available and understood by the Users through proper communication. Appropriate and periodical training on this Policy will be provided to employees to educate them about the principles and requirements of this Policy.

12. Raising a concern

If any Associates of the Company wishes to raise a concern regarding any violation of this Policy; they can report it to the IT/ISMS team via e-mail (itsupport@cactusglobal.com) or phone +91-22-67148800).

13. Monitoring and Review

CACTUS will establish appropriate measures, to ensure compliance with the relevant policies, procedures, and controls.

CACTUS will monitor the effectiveness and review the implementation of this Policy regularly, considering its suitability, adequacy, and relevance. Any improvements identified will be made as soon as possible. CACTUS reserves the right to amend, suspend or terminate this Policy at any time, at its sole discretion, with or without notice.