Information Systems and Assets Acceptable Use Policy

Purpose

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

Scope

This Policy applies to the use of information, electronic and computing devices, and network resources to conduct Real's business or interact with internal networks and business systems, whether owned or leased by Real, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Real are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Real's policies and standards, and local laws and regulations. Exceptions to this policy are documented in section 6.

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

Policy and Procedures

1. **General Use and Ownership**
    1. Real's proprietary information stored on electronic and computing devices whether owned or leased by Real, the employee or a third party, remains the sole property of Real. You must ensure through legal or technical means that proprietary information is secured and protected.
    2. You have a responsibility to promptly report the theft, loss, or other unauthorized disclosure of Real's proprietary information to the CTO or their designee.
    3. You may access, use, or share Real's proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
    4. You are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, you should consult your supervisor or manager.
    5. For security and network maintenance purposes, Real reserves the right to audit networks, computer equipment, and systems on a periodic basis to ensure compliance with this Policy.
    6. Keep passwords secure and do not share accounts. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
    7. Postings by you using a Real email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of Real, unless posting in the course of business duties.

    8. You must use extreme caution when opening emails with attachments or links, where the sender may have been spoofed and is sending malware.

2. **Unacceptable Use**
    1. The following activities are, in general, prohibited. You may be exempt from these restrictions during the course of your 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).
    2. Under no circumstances are you authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Real’s owned resources.
    3. The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.
        1. 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 Real or the end user.
        2. 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 Real or the end user does not have an active license is strictly prohibited.
        3. Accessing Real’s data, a server, or an account for any purpose other than conducting Real’s 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 the export of any material that is in question.
        4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojans, rootkits, etc.).
        5. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
        6. Using a Real computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
        7. Searching or viewing inappropriate content while using Real’s property and systems.
        8. Making fraudulent offers of products, items, or services originating from any Real account.
        9. Effecting security breaches or disruption 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, email spoofing, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited, unless these duties are within the scope of regular duties.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Introducing honeypots, honeynets, or similar technology on the Real network, unless part of an employee's job duties.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. 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.
16. Providing information about, or lists of, Real's employees to parties outside Real.

Email and Cloud Storage Activities

1. When using Real's resources to access and use the Internet, employees must realize they represent Real. Whenever employees state an affiliation to Real, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of Real".
2. Real employees shall have no expectation of privacy in anything they store, send, or receive on Real's email system.
3. The Following activities are strictly prohibited, with no exceptions:
    1. Sending unauthorized unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
    2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
    3. 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.
    4. Creating or forwarding "chain letters, "Ponzi", or other "pyramid" schemes of any type.
    5. Automatically forwarding Real emails to third-party email systems. Individual messages, which are forwarded by the user, must not contain Real confidential or other sensitive information.
    6. Use of third-party email or cloud storage systems such as, but not limited to, Yahoo, Live, Hotmail, personal Gmail, and Exchange to conduct Real business.

4. **Blogging and Social Media**
    1. Blogging by you, whether using Real's property and systems or your personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited or occasional use of Real systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate this Policy, is not

detrimental to Real’s best interests and does not interfere with your regular work duties. Blogging from Real’s systems is also subject to monitoring.

   2. You shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of Real and/or any of its employees. You are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by this Policy.
   3. You may also not attribute personal statements, opinions, or beliefs to Real when engaged in blogging. If you are expressing your beliefs and/or opinions in blogs, you may not, expressly or implicitly, represent yourself as an employee or representative of Real.
   4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Real’s trademarks, logos, and any other Real intellectual property may also not be used in connection with any personal blogging activity.

5. **Compliance and Non-Compliance with Policy**
   1. **Compliance Measurement:** Real will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.
   2. **Non-Compliance:** An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In addition to this, employees may be subject to criminal prosecution under federal, state, or local laws; civil liability; or both for unlawful use of any IT System.

6. **Exceptions**

Any exception to the policy must be approved by the CTO or their designee.