Acceptable Use Policy

Our customers trust us, and they expect us to protect the data and resources they've shared with us. Part of how we'll uphold that trust is through pre-established policies so we don't need to make key decisions in critical moments.

Below, we explain the sections of our acceptable use policy: what each protects against, why a customer may care, and why we think each is important. We don't mean for the Acceptable Use Policy to intimidate, but we do aim for it to be clear.

General Use and Ownership

This section explains policy around separating work activities from personal activities as much as possible. Understand that the systems you use for work, including a company-provided laptop, have a *much lower expectation of privacy* than systems you own. You may use your company devices for reasonable personal use, but those devices are not yours because:

- If the company is sued, all its devices are subject to discovery, which means opposing counsel will have access to your data.
- When we troubleshoot our systems, company administrators may have access to your data.
- We may terminate an employee, which may include giving another employee access to the terminated employees' devices and accounts.
- If we are breached, outside investigators will likely inspect all use of an account and/or device, no matter its purpose.

Please limit personal use of company-provided devices as much as possible and remember that corporate devices are not your personal property. Our policies are strict so that we do not have to make judgment calls on a case-by-case basis in high-stress situations.

Security and Proprietary Information

This section describes behaviors the company expects of you, including password hygiene and the use of multi-factor authentication.

Acceptable Use

The first part of this section details the consequences for malicious, negligent, and/or delinquent behavior. Neither intentionally harm others nor break laws.

The section's second part emphasizes that your employment by the company does not make you one of the company's public representatives. Instead, public communication and brand are controlled centrally at the company. While email and social media are mentioned specifically, please be conservative overall in how you represent yourself as an employee.

Policy Compliance

This section details the information security team's role in measuring, enforcing, and making exceptions to the policy and the potential consequences, including termination, for policy violations.

Acceptable Use Policy

1. Overview

Reveal's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Reveal's established culture of openness, trust and integrity. Instead, the team is committed to protecting Reveal's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Reveal. 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.

Effective security is an organizational effort involving the participation and support of every employee and affiliate who deals with Reveal information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

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

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Reveal, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

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

4. Policy

4.1 General Use and Ownership

4.1.1 Proprietary information stored on electronic and computing devices whether owned or leased by Reveal, the employee or a third party, remains the sole property of Reveal. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Policy.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

4.1.3 You may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. 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.

4.1.5 For security and network maintenance purposes, authorized individuals within Reveal may monitor equipment, systems and network traffic at any time, per the company's auditing practices, details of which are documented in relevant technology and security-related policies.

4.1.6 Reveal reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Asset Management Policies.

4.2.2 Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

4.2.3 Postings by employees from an email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Reveal, unless posting is in the course of business duties.

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

4.2.5 Employees must use multi-factor authentication to authenticate to corporate accounts whenever available.

4.2.6 Employees must use a password manager to avoid insecure or shared passwords with accounts.

4.2.7 Employees must encrypt their devices if asked, and must not interfere or otherwise reduce the level of encryption on their devices.

4.2.8 Employees must install OS updates onto their devices if asked or prompted. Employees should also be proactive about applying OS updates to their devices.

4.2.9 Employees must use antivirus software to protect the integrity and confidentiality of their laptops if asked, and must not interfere or otherwise prohibit antivirus activities on their devices.

4.3 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 authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Reveal-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.

4.3.1 System and Network Activities: the following activities are strictly prohibited, with no exceptions:

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 the company.
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 the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. 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.
6. Using a 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.
7. Making fraudulent offers of products, items, or services originating from any account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Reveal Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

10. Port scanning or security scanning is expressly prohibited unless the Security team is notified in advance. Reveal Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

11. 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. Reveal Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

12. Circumventing user authentication or security of any host, network or account. Reveal Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

13. Introducing honeypots, honeynets, or similar technology on the network.

14. Interfering with or denying service to any user other than the employee's host (for example, distributed denial of service (DDoS) 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, employees to parties outside Reveal.

4.3.2 Email and Communication Activities: When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to Reveal management.

1. 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).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. 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.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Posting the same or similar non-business-related messages to large numbers of newsgroups or mailing lists (newsgroup spam).

7. Use of unsolicited email originating from within Reveal's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via Reveal's network.

4.3.3 Blogging and Social Media

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

2. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Reveal's Data Protection policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Reveal 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 Reveal's Code of Conduct.

4. Employees may also not attribute personal statements, opinions or beliefs to Reveal 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 Reveal. Employees assume any and all risks associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Reveal's trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The CTO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the CTO in advance, and if applicable, documented in the Reveal Risk Register.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- Asset Management Policy - Endpoints
- Data Protection Policy
- Information Security Policy
- Password Policy
- Responsible Disclosure Policy
- System Access Policy
- Code of Conduct

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

Responsibility

The CTO is responsible for ensuring this policy is followed.

Last updated: 2021-06-20