Acceptable Use Policy

DOCUMENT OWNER	Executive Leader of IT Department	EFFECTIVE DATE	09/27/2022	REVISION CYCLE	12 Months

INTRODUCTION

Purpose

The Acceptable Use Policy ("Policy") establishes the acceptable and unacceptable use of electronic devices and information resources at Rocky Mountain Institute ("RMI" or "Company"). Inappropriate use exposes RMI to various information security risks including malware, compromised systems or services, data breaches, and associated operational, legal, and regulatory risks. RMI is committed to protecting RMI's employees, contractors, consultants, temporary employees, and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

For the purpose of this Policy, technology includes, but is not limited to computers, laptops, mobile devices, internet, software, information systems, email, chat, telephones, voice mail and related electronic devices and equipment ("Company Technology"). Users of Company Technology must respect the rights of other users, respect the integrity of the Company Technology and observe all relevant laws and regulations.

Scope and Exclusions

This Policy applies to the use of any electronic devices and information resources to conduct RMI business or interact with Company Technology, whether owned or leased by RMI, the employee, or a third party.

This Policy applies to all RMI employees and any consultants, temporary employees or contractors ("Users") who make use of Company Technology.

Terms and Definitions

TERM	DEFINITION
Honeynet	Decoy network containing honeypots separate from the production network and configured with vulnerabilities for the purpose of luring and distracting attackers.
Honeypot	Decoy network device isolated from the production network and configured with vulnerabilities for the purpose of luring and distracting attackers.
Smishing	Form of phishing using SMS (text messaging).
Torrenting	Downloading and uploading files using the peer-to-peer (P2P) network and BitTorrent protocol.
Vishing	Form of phishing using voice (phone calling).

Roles and Responsibilities

PARTY	ROLES/RESPONSIBILITIES
Executive Leader of IT	-Responsible for the IT program at RMI and the implementation of the information security program, including this Policy. -Responsible for the annual review, updates, and content of this Policy. -Communicates changes to this Policy.
All RMI Users	-Responsible for adhering to this Policy and escalating any actual or potential violations to the IT function.

POLICY STATEMENT

General Use and Ownership

All Users are required to comply with the following guidelines:

1. Users are responsible for exercising good judgment regarding the appropriate use of Company Technology.
2. Users should expect no privacy when using the Company network or Company Technology, including email or chat.
3. The Company reserves the right to audit all its networks and systems on a periodic basis to ensure compliance with this Policy.
4. All information, electronic, and computing devices that connect to the Company network must comply with the Information Security Policy.
5. Account passwords for Company systems must comply with the password parameters in the Information Security Policy.
6. Users must exercise caution when opening attachments or clicking on links in emails from unknown or suspicious senders.
7. Users must take reasonable efforts to engage in safe Internet browsing habits.
8. Personal use of Company Technology is permitted as long as it does not violate any of the requirements of the Information Security Policy, impact job performance, or entail any of the activities in the "Unacceptable Use" section.

Reporting Security Incidents

If any User discovers or suspects a security incident or breach of any security policy, the User must immediately notify the IT department. Examples of incidents requiring notification include, but are not limited to:

- Suspected or known compromise of Company login credentials (e.g., username, email address, password);
- Suspected or known unauthorized disclosure of Company data;
- Suspected or known malware infection;
- Loss or theft of any Company device, ID badge, or equipment – including any personal device used to access Company data and resources;
- Any attempt by any person to obtain a User's password or any Company sensitive data through any means (e.g., phishing, smishing, vishing); and
- Any suspected or known cyber attack that affects the confidentiality, integrity or availability of Company data and resources according to the Information Security Policy.

Users must use discretion when communicating security incidents and report information only to their supervisor or directly to the IT department. Users may not withhold any information relating to the security incident or interfere in any way with incident investigations or resolution.

Unacceptable Use

The activities listed below are unacceptable uses of Company Technology. Users are prohibited from engaging in any of these activities.

These lists are not exhaustive. Users must use their best judgment and avoid activities that could present information security risks or strains on Company Technology, even if the activity is not expressly prohibited.

In addition, these lists should be read in conjunction with the Information Security Policy and other information security-related written guidelines and training materials.

More fundamentally, Users are prohibited from using Company Technology in connection with any activity that is illegal under any applicable law or regulation, whether or not the activity is expressly prohibited under this or any other RMI policy or procedure.

If any User has a question about whether an activity is acceptable or prohibited, they must consult the IT Department. Questions of law must be referred to legal@rmi.org.

Prohibited System and Network Activities

1. Engaging in any activity that disrupts the workplace environment or creates a hostile workplace.
2. Viewing or disseminating illicit, offensive, sexually explicit, or inappropriate content on Company devices and networks.
3. Circumventing or tampering of any device, network, account, or security control. This includes unauthorized escalation of privileges.
4. Accessing data, a server, or an account for any purpose other than conducting Company business, even if the User has authorized access.
5. Revealing a User's account password to others or allowing use of the User's account by others. This includes family and other household members when working from home.
6. Making fraudulent offers of products, items, or services originating from any Company account.
7. Introducing malicious programs or data into the Company network or servers.
8. Installing onto any Company-issued device any application without approval of the IT Department.
9. Installing or distributing unlicensed or "pirated" software.
10. Unauthorized downloading, copying, or accessing of copyrighted content.
11. Peer-to-peer file sharing or engaging in "torrenting".
12. Streaming of audio, video, or any content that negatively impacts the performance of the Company network and information resources. This includes excessive use of Company bandwidth and other information resources that may degrade network performance. Large file downloads or other bandwidth- intensive tasks must be performed during times of low Company-wide usage.
13. Introducing honeypots, honeynets, or similar technology on the Company network.
14. Connecting devices to the Company network that are not Company provided. This excludes personal devices connected to the guest Wi-Fi network.
15. Port or protocol scanning, network reconnaissance or monitoring, or any type of security scanning unless explicit consent is granted by the Director of IT.
16. Interfering with or denying service to any user, electronic device, or information resource (e.g., denial of service attack).

Prohibited Email, Social Networking, and Communication Activities

1. Disclosing any Company confidential or proprietary information, trade secrets, or intellectual property unless (a) the disclosure is for a legitimate business purpose and consistent with the User's authorized job responsibilities, and (b) the User employs appropriate secure communication protocols.
2. Making discriminatory, disparaging, defamatory, vilifying, sexist, racist, abusive, obscene, threatening, or harassing comments.
3. Sending unsolicited email messages, including "junk mail" or other advertising material to individuals who did not specifically request it ("spamming").
4. Unauthorized use or forging of email header information to impersonate or "spoof" a user or account.
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.

6. Making any communication that may harm or tarnish the image, reputation, and/or goodwill of the Company and/or its personnel.
7. Engaging in any personal usage that negatively impacts the Company network, information resources, or the User's job performance.
8. When blogging or commenting on social media, attributing personal statements, opinions, or beliefs to the Company or representing oneself as a Company representative without prior approval of the executive responsible for marketing.

Non-Adherence and Exception Handling

Any User found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment with the Company. Exceptions to this Policy must be approved by the leaders of the IT department or their designees.

DOCUMENT GOVERNANCE

Version History

VERSION	STATUS	STATUS DATE	DESCRIPTION OF CHANGES	AUTHOR
2.0	New Draft	09/19/2022	Created	Andrei Cazan
2.0	Published	09/27/2022		Andrei Cazan