

# **Rocky Mountain Risk Insurance Group/Rocky Mountain Risk**

**POLICY NO. E-2**

**DATE: November 11, 2020**

---

## **Subject: USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS**

---

1. Use of the Internet and electronic communications shall not be considered private communications and may be subject to monitoring at any time. Employees shall have no expectation of privacy when using Rocky Mountain Risk electronic communication systems.

2. Electronic communication sent or received by either of the Board of Directors, the Rocky Mountain Risk Insurance Group, or Rocky Mountain Risk employees may constitute a public record subject to retention under state and federal law. Such electronic communication may also be subject to public inspection under the state open records law.

3. Whenever the Rocky Mountain Risk Insurance Group or Rocky Mountain Risk is a party in litigation or reasonably anticipates being a party in litigation, Board members and Rocky Mountain Risk Insurance Group or Rocky Mountain Risk in possession of electronic documents, e-mail and/or other evidence relevant to the litigation or reasonably anticipated litigation shall retain all such documents, e-mails and other evidence until otherwise directed by the Executive Director or designee.

4. To ensure compliance with applicable law and Rocky Mountain Risk Insurance Group and Rocky Mountain Risk policy, the Rocky Mountain Risk Insurance Group and Rocky Mountain Risk retains the right to review, store and disclose all information sent over Rocky Mountain Risk Insurance Group and Rocky Mountain Risk electronic communication systems for any legally permissible reason, including but not limited to determining whether the information is a public record, whether it contains information discoverable in litigation and to access Rocky Mountain Risk Insurance Group and Rocky Mountain Risk's information in the employee's absence.

5. Upon sending or receiving an electronic communication, all users shall segregate or store those communications that are public records. Public records are those that evidence the Rocky Mountain Risk Insurance Group and Rocky Mountain Risk's functions, policies, decisions, procedures, operations or other activities of the Rocky Mountain Risk Insurance Group and Rocky Mountain Risk or that contain valuable Rocky Mountain Risk Insurance Group or Rocky Mountain Risk's data. Electronic communication on Rocky Mountain Risk Insurance Group and Rocky Mountain Risk computers or Rocky Mountain Risk Insurance Group and Rocky Mountain Risk electronic communication systems shall be retained only as long as necessary. Such electronic communication shall be deleted on a routine basis unless otherwise required to be retained by Rocky Mountain Risk Insurance Group or Rocky Mountain Risk policy or state or federal law.

6. Improper use of the Internet or electronic communications may result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may be grounds for disciplinary action, up to and including termination, and/or legal action.

7. Staff shall use Rocky Mountain Risk computers in a responsible, ethical and legal manner. Examples of unacceptable uses include, but are not limited to, accessing, creating, transmitting or forwarding material:

7.1 that promotes violence or destruction of property or concerns the manufacturing of destructive devices or weapons;

7.2 that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion;

7.3 that plagiarizes the work of another without express consent;

7.4 that uses inappropriate or profane language likely to be offensive to others;

7.5 that harasses, threatens, demeans, or promotes violence or hatred against another person or group in violation of the Rocky Mountain Risk Insurance Group's nondiscrimination policies; or

7.6 that is in violation of any federal or state law or Rocky Mountain Risk Insurance Group policy, including but not limited to copyrighted materials and material protected by trade secret.

8. Staff shall not use another person's password or any other identifier, gain or attempt to gain unauthorized access to Rocky Mountain Risk Insurance Group computers or systems, use unauthorized software or read, alter, delete or copy electronic communications of other users.

9. Staff may be subject to disciplinary action for violation of this policy.