# UTAH COUNTIES INDEMNITY POOL
# OPERATIONS—IT AND COMPUTER SECURITY POLICY

## SECTION A EFFECTIVE DATE AND FREQUENCY OF REVIEW

1. The effective date of this policy is January 1, 2024. Computer and email usage procedures and responsibilities have previously been addressed in the Personnel Standards of Conduct Policy adopted by the Board on April 21, 2022.

2. This policy should be reviewed annually by the Board.

3. This policy should also be reviewed by the Board any time that changes to laws or rules governing information technology and computer security of interlocal agencies are amended or recommendations are made by the UCIP CEO, which would require review and update to this policy.

4. Failure to review this policy in the frequency stated shall not nullify, void, limit or waive this policy or any action taken under this policy.

5. This policy is considered to be amended at the time any new federal or state law becomes effective, which conflicts with this policy, but only to the extent necessary to come into compliance with new law.

## SECTION B PURPOSE

1. This policy of the Board relates to Information Technology and Computer Security.

2. This policy establishes basic rules for use of UCIP's computer systems including the Internet and email.

3. This policy establishes standards for the creation and protection of passwords used to conduct UCIP business.

4. This policy establishes guidelines for reporting unusual activity on UCIP computer systems and reporting cybersecurity incidents or privacy or security events.

## SECTION C AUTHORITY

1. The Board has authority to adopt this policy under the UCIP Interlocal Agreement and Bylaws.

## SECTION D APPLICABILITY AND SCOPE

1. This policy applies to all decisions regarding cybersecurity measures and protocols as approved by the Board.

2. This policy applies to all personnel of UCIP who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at the UCIP offices, has access to the UCIP network, or stores any UCIP information.

## SECTION E DEFINITIONS

1. Board: the Board of Directors of the Utah Counties Indemnity Pool.

2. CEO: the Chief Executive Officer of the Utah Counties Indemnity Pool.

3. Content Filtering: protection against illegal, inappropriate or objectionable attachments, downloads, malware, phishing, scanning, viruses, etc.

4. Critical Information: data that UCIP deems essential to continue its daily business.

5. Cyber-Attacks: social engineering, phishing, malware, spoofing, denial-of-service, identity-based, code interjection, etc.

6. Cybersecurity: the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this protection.

7. Director: a member of the Board of Directors of the Utah Counties Indemnity Pool.

8. IT: Information Technology.

9. Member: each of the Participating Members of UCIP as listed in the Coverage Addendum.

10. Sensitive Information: data that must be protected against unauthorized disclosure.

11. UCIP: the Utah Counties Indemnity Pool.

## SECTION F POLICY STATEMENTS

1. It is the policy of the Board to secure Critical and Sensitive Information and data stored on UCIP computer systems.

2. It is the policy of the Board to assure UCIP employees annually receive cybersecurity awareness training.

3. It is the policy of the Board to have a qualified IT professional to maintain the security and protection of UCIP computer systems against cybersecurity incidents, events and cyber-attacks.

4. It is the policy of the Board to have a formal disaster recovery plan and business continuity plan that guides UCIP employees in setting the priority of UCIP's computer systems restoration to recover from a cybersecurity incident that impacts UCIP's business operations.

5. It is the policy of the Board that all Internet use must comply with applicable state and federal laws.

**SECTION G PROCEDURES AND RESPONSIBILITIES**

1. Critical and Sensitive Information includes credentials to log-in to UCIP's accounting system, claims system, website administrative access, member schedules, state and federal websites, benefits websites, and financial websites. These credentials may be stored in the password manager Keychain Access.

2. UCIP shall identify vendors that store UCIP's Critical and Sensitive Information on their websites and/or networks.

3. UCIP's Critical and Sensitive Information shall be backed-up, stored and encrypted offline on a different logical or physical network such as a cloud backup to support recovery from a catastrophic cybersecurity incident. In addition, Critical and Sensitive Information shall be backed-up no less than twice weekly, stored and encrypted on a physical hard-drive. Access to back-ups shall be limited. One physical back-up hardware shall be stored offsite and one physical back-up hardware shall be stored onsite locked in a fireproof box.

4. UCIP employees shall use multi-factor authentication when logging-in to their UCIP computer.

5. UCIP employees shall receive mandatory cybersecurity awareness training annually. Training will include the expectations of UCIP employees to recognize common cyber-attacks and the process of reporting possible cybersecurity incidents or other types of cyber-attacks.

6. Any UCIP employee suspecting or noting a security incident, data breach or potential system compromise, or malicious activity shall immediately contact the CEO or UCIP's IT professional.

7. UCIP shall report privacy or security events or cybersecurity incidents to insurance carriers, law enforcement and incident support vendors.

8. UCIP employees shall timely apply maintenance and cybersecurity patches to software on UCIP computer systems.

9. UCIP's IT professional shall install cybersecurity tools and systems that monitor who is utilizing the UCIP network, when they are on the network and what network resources they are using.

10. UCIP's IT professional shall implement tools to automatically monitor, log and report unusual and unauthorized activities that occur on UCIP computer systems.

11. UCIP's IT professional shall install email Content Filtering and web Content Filtering and web Content Filtering to identify unauthorized activity, malicious attachments and other prohibited activity that may negatively impact UCIP computer systems and network.

12. UCIP shall maintain software and hardware that is supported by the manufacturer or vendor on all UCIP computer systems.

13. UCIP employees use a password manager to organize and manage passwords securely on UCIP computer systems. Safeguards to select passwords include:

a. Using different passwords for different accounts;

b. Using multi-factor authentication;

c. Length and complexity;

d. Passwords that are hard to guess but easy to remember;

e. Passwords must not be revealed to others, with the exception of the CEO in accordance with the Business Continuity/Disaster Recovery Policy; and

f. Passwords must not be inserted in e-mail messages or other forms of electronic communication.

14. The usage of UCIP computer systems, Internet and e-mail by UCIP employees are outlined in accordance with the Personnel—Standards of Conduct Policy.

15. When receiving emails, UCIP employees shall use techniques provided in their cybersecurity awareness training to identify suspicious emails and shall not click on any links or attachments until the source of the email is confirmed to be legitimate.

**SECTION H REVISION HISTORY**

1. Adopted: January 1, 2024

## SECTION I APPENDICES

1. Critical and Sensitive Information Stored With Vendors Listing