# Contents

# 1. Summary

It is Utility Safety Partners' (USP) responsibility and obligation to ensure that all IT is used only for its intended purpose and that information contained or transmitted via USP systems is protected from unauthorised access, unauthorised use or corruption.

Section 6.1(a) of USP's User Agreement states:

> *(a) Sufficient security with respect to the System shall be provided to preclude or prevent loss of alteration of, or access to any Data provided to the Supplier by the User;*

This policy outlines the protections in place to prevent unauthorised access to USP systems and data, as well as response plans in the event of a cyber breach.

# 2. Target Audience

This policy applies to all employees of Utility Safety Partners, IT vendors and software providers, and business partners who share data and protected information with USP.

# 3. Purpose

This policy defines and governs the appropriate and inappropriate usage of USP digital assets and IT systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network access, e-mail, Internet browsing, etc.

It is the responsibility of USP and its partners to ensure the confidentiality, integrity and availability principles of digital assets and IT systems are maintained.

# 4. Policy Objectives

Identify security measures which USP has in place to identify risk and to protect assets and systems.

Identify policies and procedures in place to ensure responsible usage and protection of software and systems.

Identify policies and procedures which govern USPs response to security breaches or cyber threats.

# 5. Policy statements

In partnership with Shing Digital (Third-party IT vendor, ISEDC Cybersecure Canada certified), USP maintains the following system protections:

- Hardware Protection
  - Dual-cascading Firewalls controlling all network access
  - Secure Web Gateways: FortiGate VPN-only access to file servers

  - Endpoint platform protection
  - Cloudflare protection and real-time information backups
  - Geo-redundant server systems
  - 24/7 Managed detection and response
  - Arctic Wolf cyber threat protection
  - Datto backup protection for all data
  - Managed Data Leak protection (with Netwrix auditor and reporting)
- Access Control
  - Cloud Data protection gateways
  - Password Policy in place for all employees
  - Microsoft Entra ID identity and access management
  - Access to digital information is restricted to employees or third parties with an operational requirement.
  - Access to member data is only provided to employees with an operational requirement.
  - Stored member data is restricted to one local server and back-up server
  - Live member data is kept by our software provider in a restricted Canadian server environment behind AWS cloud protection.
  - LastPass password management for employees with control access
  - MFA and SSO login controls
  - Proofpoint protection for all email accounts
  - Internet usage policy for all employees
  - Process in place to remove all access from employees leaving the company
- Cyber Incident Response Policy
  - Identifies responsible parties
  - Policy identifies potential and actual threats by threat level category
  - Actions and responsibilities outlined for each threat level event
  - Communication responsibilities identified in the event of a successful attack
  - Cybersecurity insurance policy in place
  - Scheduled cybersecurity drills to identify gaps
  - Annual cybersecurity training provided for all staff
- Third party SaaS vendors
  - Agreements require cybersecurity plan in place for vendor
  - Agreements require minimum uptime
  - Agreements require redundancy and continuity plan

## 6. Effectiveness review

IT vendor to use a third party to conduct annual Penetration Test to identify and correct vulnerabilities.

Access to real-time and quarterly security and incident reports to identify system vulnerabilities/effectiveness and employee behaviour which may expose network to threat.

System security components are reviewed with our IT vendor quarterly to identify additional requirements and track progress on USP's technology roadmap. Between 2019 and 2024, USP has added components to move from "Bare Minimum" to "Proactive" on Shing Digital's cybersecurity maturity scale

# 7. Accompanying Documents

Detailed policy and system documentation is available to internal staff only.

Version Control

| Date (MM-DD-YY) | Completed by: | Approved by: | Briefly describe changes | Version of final copy |
|---|---|---|---|---|
| 09-27-24 | S.Kirk | | Document created | V1 |
| 10-16-24 | | M. Sullivan | Version Approved | V1 |