# CYBERSECURITY AND DATA PRIVACY POLICY OF INVENT VENTURES, INC.

## I. Purpose

This Cybersecurity and Data Privacy Policy ("Policy") outlines Invent Ventures Inc.'s ("the Company") commitment to protecting the confidentiality, integrity, and availability of its information systems and data, including personal, proprietary, and financial information. The purpose of this Policy is to ensure that all employees, contractors, and third parties understand and comply with the Company's cybersecurity and privacy standards, in alignment with applicable regulations and best practices.

## II. Scope

This Policy applies to all Company personnel, including employees, contractors, consultants, interns, and any third parties who access or process Company data or systems. It covers all data, whether stored digitally or physically, and all information systems, including networks, devices, cloud services, and applications used by the Company.

## III. Data Privacy

The Company is committed to safeguarding personal and sensitive information, including but not limited to financial, health, identity, and blockchain-related user data. The following principles guide our data privacy practices:

- Data will only be collected for legitimate business purposes and with appropriate consent where required.
- Access to personal data is limited to individuals with a business need-to-know.
- Data subjects will be informed of their rights, including access, correction, and deletion, in accordance with applicable data protection laws such as GDPR, CCPA, or others.
- Personal data shall not be sold or shared with third parties without a lawful basis and appropriate safeguards.

## IV. Cybersecurity Practices

The Company implements industry-standard practices and technologies to protect against unauthorized access, data breaches, and cyber threats:

- All systems must be protected by strong authentication methods and regularly updated with security patches.
- Employees must use Company-approved tools and devices and comply with device security guidelines.
- All data must be encrypted in transit and at rest where feasible.
- Regular security awareness training is mandatory for all staff.
- Incident response procedures are in place to address potential data breaches or attacks.
- All Internet and Network activity is monitored and logged to detect and respond to anomalies in real-time and to ensure that such use is strictly used for business purposes.
- Prohibited activities include unauthorized software installation, file-sharing, using company devices for illegal activities, or attempting to circumvent security controls.
- Employees or other authorized users will be subject to specific rules for password creation and management such as the use of multi-factor authentication and prohibiting sharing of passwords

**V. Third-Party Security**

Vendors and partners who access Company data or systems must demonstrate adherence to data protection standards consistent with this Policy. Contracts must include data security terms, and periodic audits or assessments may be conducted.

**VI. Reporting and Incident Response**

All employees must promptly report any suspected or actual data breach, system compromise, or policy violation to the Information Security Officer (ISO) or designated compliance contact. The Company will follow its Incident Response Plan, including investigation, mitigation, and required regulatory disclosures.

**VII. Compliance and Disciplinary Action**

Violations of this Policy may result in disciplinary action, up to and including termination of employment or contract. Non-compliance may also lead to legal liability and regulatory penalties for the Company and individuals involved.

**VIII. Policy Review and Updates**

This Policy will be reviewed annually and updated as needed to reflect changes in technology, business practices, or legal requirements. Updates must be approved by the Board of Directors or delegated committee.