E-Commerce Safety Policy

Purpose

This E-Commerce Safety Policy establishes the standards, procedures, and responsibilities required to maintain a secure, reliable, and trustworthy online shopping environment for customers, employees, vendors, and business partners. The purpose of this policy is to protect sensitive information, reduce security risks, ensure compliance with applicable laws and regulations, and maintain customer confidence in all digital commerce operations.

---

1. Customer Data Protection

Our company is committed to protecting all customer information collected through our e-commerce platforms. Personal information, payment details, shipping information, and account credentials will only be collected for legitimate business purposes.

1.1 Data Security Measures

- All sensitive customer data must be encrypted during transmission using secure encryption protocols.
- Customer payment information will never be stored in unsecured systems.
- Access to sensitive information is restricted to authorized personnel only.
- Systems containing customer information must be protected with passwords, firewalls, and security monitoring tools.
- Employees are prohibited from sharing customer information without proper authorization.

1.2 Payment Processing

- All payment transactions must be processed through trusted and secure payment gateways.
- Fraud prevention and transaction monitoring systems will be utilized to identify suspicious activity.
- The company reserves the right to hold or cancel transactions that appear fraudulent or unauthorized.

2. Website & Platform Security

RDWY Global will maintain secure and reliable e-commerce systems to minimize risks associated with cyber threats, unauthorized access, malware, and data breaches.

2.1 Security Standards

- E-commerce platforms must receive regular security updates and maintenance.
- Antivirus, anti-malware, and cybersecurity monitoring tools must remain active at all times.
- Administrative access to websites and backend systems will be limited to authorized personnel.
- Multi-factor authentication is strongly recommended for all administrative accounts.

2.2 Monitoring & Incident Response

- The company may monitor website activity to detect unauthorized access or suspicious behavior.
- Any suspected data breach or cybersecurity incident must be reported immediately to management.
- In the event of a security breach, the company will take appropriate corrective actions, notify affected parties when required, and cooperate with applicable authorities.

---

3. Customer Account Safety

Customers are responsible for maintaining the confidentiality of their account credentials.

3.1 Customer Responsibilities

Customers should:

- Use strong and unique passwords.
- Avoid sharing login credentials with others.
- Immediately report unauthorized account activity.
- Ensure billing and shipping information remains accurate.

The company is not responsible for losses caused by customer negligence, including compromised passwords or unauthorized account sharing.

---

4. Fraud Prevention

The company maintains a zero-tolerance policy toward fraud, theft, chargeback abuse, identity theft, and unauthorized transactions.

4.1 Fraudulent Orders

The company reserves the right to:

- Cancel suspicious orders.
- Request additional verification for high-risk transactions.
- Refuse service to individuals suspected of fraudulent activity.
- Report fraudulent activities to law enforcement or financial institutions when necessary.

---

5. Product Safety & Compliance

All products sold through the company's e-commerce platforms should comply with applicable safety standards, regulations, and legal requirements.

5.1 Product Information

- Product descriptions should accurately represent the product being sold.
- Safety warnings and usage instructions must be included when appropriate.
- Restricted or prohibited items may not be sold through the platform.

---

6. Employee Responsibilities

Employees handling e-commerce operations are expected to follow all security procedures and confidentiality requirements.

6.1 Internal Conduct

Employees must:

- Protect customer and company information.
- Follow password and account security guidelines.
- Report suspicious activity or potential vulnerabilities.
- Avoid unauthorized access to company systems.

Failure to comply with this policy may result in disciplinary action, including termination.

---

7. Third-Party Services

The company may utilize third-party providers for payment processing, shipping, analytics, hosting, or other operational services.

7.1 Vendor Security

Third-party vendors are expected to maintain reasonable security standards and comply with applicable data protection regulations.

The company is not responsible for independent security failures or service interruptions caused by third-party providers beyond its reasonable control.

---

8. Limitation of Liability

While the company takes reasonable measures to maintain a secure e-commerce environment, no online platform can guarantee absolute security.

The company shall not be held liable for:

- Unauthorized access caused by customer negligence.
- Service interruptions beyond reasonable control.
- Cyberattacks or technical failures that could not reasonably be prevented.
- Indirect or consequential damages resulting from use of the platform.

---

9. Policy Updates

The company reserves the right to modify or update this E-Commerce Safety Policy at any time to reflect operational, legal, or technological changes.

Updated versions of this policy may be published on the company website or distributed through official communication channels.

---

10. Acceptance of Policy

By accessing, using, or purchasing products from the company's e-commerce platforms, customers acknowledge and agree to the terms outlined in this E-Commerce Safety Policy.

Company Information

PARENT COMPANY - RDWY GLOBAL HOLDINGS LLC

Website - http://www.rdwyglobal.com

Effective Date - 05/23/2026

This policy extends to all RDWY Global Holding owned platforms & brands. RDWY Global has the right to change or update this policy at any time with or without notice. For more information, please contact us at support@rdwyglobalholdings.com or call us at 1(800) 210-9756.