INFORMATION SECURITY POLICY

Purpose

The purpose of this Information Security Policy is to define how Enjoy the Journey protects its information assets, including customer, employee, and business data. This policy establishes a framework for maintaining the confidentiality, integrity, and availability of information while ensuring compliance with applicable standards such as PCI DSS. It also provides clear guidance to personnel on their responsibilities in maintaining a secure environment.

Scope

This policy applies to all employees, contractors, and third parties who have access to Enjoy the Journey online store. It covers all devices, networks, and cloud-based platforms used in the operation of the website, including the payment processing through Authorize.net. All individuals are expected to comply with this policy regardless of their role or location.

Payment Processing

Enjoy the Journey does not store, process, or transmit credit card information directly on its website. All payment transactions are securely handled by a third-party payment gateway, Authorize.net, which is PCI-compliant. Customers enter their payment information directly into the secure environment provided by the payment processor, ensuring that sensitive cardholder data is not exposed to or handled by Enjoy the Journey systems.

Data Security

Enjoy the Journey is committed to protecting sensitive information by ensuring that it is not stored unnecessarily and that access is strictly controlled. Any data collected is limited to what is required for business operations, and appropriate safeguards are in place to prevent unauthorized access, disclosure, or misuse. Cloud-based services used by the company are selected based on their security standards and reliability.

System Security

All systems and devices used for business operations must maintain up-to-date security protections, including operating system updates, security patches, and built-in anti-malware protections. Employees are required to use secure devices when accessing the company website and must ensure that their devices are configured according to basic security best practices. Regular updates help mitigate vulnerabilities and reduce risk exposure.

Access Control

Access to systems and data is granted based on the principle of least privilege, meaning that individuals are only given access necessary to perform their job functions. User accounts must be unique and protected with strong authentication methods. Access rights are reviewed periodically and adjusted as necessary to ensure that only authorized personnel have access to sensitive systems and information.

Incident Response

In the event of a suspected or confirmed security incident, including potential data breaches, employees must immediately report the issue to management. Enjoy the Journey will assess the situation, take appropriate action to contain and mitigate the incident, and, if necessary, notify relevant stakeholders. Timely reporting and response are critical to minimizing potential damage and ensuring compliance with regulatory requirements.

Employee Responsibility

All employees are responsible for maintaining a secure working environment and adhering to this policy. This includes following best practices such as not sharing passwords, avoiding suspicious links or communications. Employees must remain vigilant and report any concerns related to security or data protection.

Policy Review

This Information Security Policy is reviewed at least annually and updated as necessary to reflect changes in technology, business operations, or regulatory requirements. Management is responsible for ensuring that the policy remains current and that all personnel are informed of any updates. Continuous improvement of security practices is essential to maintaining compliance and protecting the organization.