Security Plan

Section I. OBJECTIVE:

Our objective, in the development and implementation of this security plan, is to create effective administrative, technical, and physical safeguards in order to protect our customer’s private personal information. The plan will evaluate our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our customers’ private personal information.

Section II. PURPOSES:

a) Ensure the security and confidentiality of our customer’s information;

b) Protect against any anticipated threats or hazards to the security or integrity of our customers’ information;

c) Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any of our customers.

Section III. ACTION PLANS:

a) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems;

b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;

c) Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

Section IV. ACTION STEPS:

a) Appoint a specific person or persons within the company to be responsible for: 1) initial implementation of the plan; 2) training of employees; 3) regular testing of the controls and safeguards established by the plan; 4) evaluating the ability of prospective service providers to maintain appropriate information security practices, ensuring that such providers are required to comply with this information security plan, and monitoring such providers for compliance herewith; and 5) periodically evaluating and adjusting the plan, as necessary, in light of relevant changes in technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to our own business (such as mergers or acquisitions or outsourcing), and/or changes to customer information systems.

b) Conduct an annual training session for all owners, managers, employees and independent contractors—and periodic training for new employees—working for the company on the elements of this information security plan, the contents of the company’s “Privacy Policy,” and any other requirements of federal or state privacy laws. All persons in attendance should be required to certify their attendance at the training, their receipt of the company’s privacy policy, and their familiarity with the company’s requirements for ensuring the protection of customers’ private personal information.

Section V. RISK ASSESSMENT:

a) E-commerce businesses are in constant danger of hackers, credit card fraud, extortionists, and other types of cybercriminal activity. System failures such as server crashes and errors on the payment site are also possible events. To prevent and mitigate these events, a risk assessment is created.

b) Types of Threats: Internal and External attacks

|  |  |
| --- | --- |
| Identified Internal Risk | Risk Level (low, medium, high) |
| Network Threats | High |
| Technological Risk | Medium |
| Weak Passwords | Medium |
| Human-Factor Risk | High |

|  |  |
| --- | --- |
| Identified External Risk | Risk Level (low, medium, high) |
| Active Threats | High |
| Virus Attacks | Medium |
| SQL Injections | High |
| Ransomware | High |

c) Current Control Measures:

We have created complex passwords to control access to our network. We keep software up to date to prevent falling behind to new potential threats. We have put together trained management to provide good leadership. We have put in place a firewall, an antivirus, and OSSIM. These policies we have put into place should help prevent different types of attacks to our network and keep it safe.

Section VI. TOOLS and STRATEGIES:

1. Our company has adopted the following strategies for information security on our systems: 1) “Deny by Default” firewall policy; 2) Complex Passwords consisting of at least one capital letter, one symbol and one number with a minimum length of 15 characters; 3) Close unnecessary ports on network equipment; 4) Policy of Least Privilege for all accounts.
2. Our company has adopted the following tools for information security on our systems: 1) RedHat Firewall to protect the server; 2) Avast as an antivirus; 3) OSSIM to collect and aggregate logs; 4) Tripwire to provide alerts; 5) Fail2Ban to stop login attempts after 3 failed attempts.