*Republic of the Philippines*

DON HONORIO VENTURA STATE UNIVERSITY

Cabambangan, Bacolor, Pampanga

🕿 (6345) 458 0021 Local 211 **COLLEGE OF COMPUTING STUDIES**

🖳 [**http://dhvsu.edu.ph**](http://dhvsu.edu.ph) 🖰 *Email: ccs@dhvsu.edu.ph*

**FINAL TERM – ACTIVITY # 1**

*IAS-313 – Information Assurance and Security I*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Noelle Adrian M. Martin** | | | **Score** |  |
| **Year & Section** | **BSIT-3G** | **Date** | **11/21/23** |

**Objective:** The purpose of this assignment is to develop a comprehensive Information Security Plan for a fictional organization. Students will apply their knowledge of information security principles, risk assessment, and planning to create a plan that safeguards the organization's sensitive data and ensures the confidentiality, integrity, and availability of information.

**CactusShield-Pro Security. IT Secruity Plan**

CactusShield-Pro Security is a Cyber-Security company that goals to protect and prevent the risks of malware, hackers or any cyber-threats that can cause cybercrime. It is our main goal to protect and prevent any threats and risk of your system. Here our Objective of our Rules n Regulations that strictly followed by our Employee`s.

**Whats is in a Company Policy?**

The main purpose of a company policy must consistently included in IT Security Policies, either in any documents. The most Important policies apply to every user information systems within the firm. The availability, Confidentiality and the Integrity of systems and data are protected by these policies.

**Risk and Threats**

* **Cybersecurity Attacks –** You may need an IT Security Expert assistance to help and fight the cyber attacks that you having.
* **Insider Threats –** These may cause by the Employee that wants to sell the security or the system of the company.
* **Phishing Attacks –** Be careful of what you are clicking on any sites on the internet that may cause the leakage of your data.
* **Financial Fraud –** Employee`s may attempt to manipulate the financial systems or transactions.
* **Denial of Service (DoS) Attack –** Overwhelming a system or network to disrupt services.
* **Data Breach –** Unauthorized access or disclosure of sensitive information.
* **Regulatory Compliance –** Failure to comply with Industry regulations.

**Rules n Regulations**

* **Acceptable Use Policy (AUP) –** The acceptable use of computer equipment. It is used only for business purposes serving the company.
* **Security Awareness and Training Policy –** Security awareness and training must be conducted for each one of the employee, they must know the proper awareness of security and have a proper training for their positions.
* **Change Management Policy –** It must minimize the negative impacts to service of the company as for the customer have the proper service they must receive.
* **Incident Response Policy –** It must have a proper Preparation, Identification, Containment and Eradication
* **Remote Access Policy –** It must have a remote device that have easy access to the company`s network

The Rules n Regulations , Risk n Threats that provided below helps security personnel in dealing with day-to-day process it helps us to grow and improve more for any future cases.

**REFERENCE**

<https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/>

https://www.essentialtech.com.au/blog/9-policies-to-reduce-it-security-and-compliance-risks