**IT 4983 Capstone in Cybersecurity Information Security Policy**

**[**W02-12777 Project 11 Cybersecurity Group 2**]**

# Purpose

The purpose for creating an information security policy (ISP) is to create a framework that outlines the overall approach to information security. The policy is to allow the company to think ahead and pinpoint vulnerabilities that may lead to security breaches and stop them before they become an issue. It also gives all employees a clear guideline of what is allowed when dealing with company servers, even limiting some access based on classifications and roles. It is our duty to respect customers’ rights and uphold ethical and legal responsibilities.

# Audience

The audience that the ISP focuses on is all workers at Akwaaba, from the restaurants to the corporate office, contractors, vendors, and even the owner. We need to ensure that security is of the utmost priority and that does not just stop with management and IT. One of the most vulnerable aspects of security is people/users.

# Information Security Objective

The security objective protects the privacy of Akwaaba’s information content that prevents unauthorized individuals from accessing business information and systems. It restrains the employees’ and customers’ errors or malicious entries in the data that can compromise their confidentiality. To maintain the accuracy of the business information and the business' system, restriction permission is delegated to the staff member for editing or modifying them without disrupting the data integrity. As a result, an authorized person can access the information, back up the data, and ensure that they are always available for business operation.

# Data Classification

All corporate databases that process, stores, and transmit customers’ and employees’ PII (personal identifiable information) are considered “High Security Systems” and should be clearly marked as such. The data stored on these systems is considered confidential.

# Authority and Access Control Policy

This policy applies to Akwaaba staff, contractors, and vendors that connect to servers, applications, or network devices belonging to the company. Access to these devices is role-based therefore, access will be granted based on the role of each employee. IT (Information Technology) administrators and members of the security consulting firm hired by the company will have remote access to all servers and databases. The company web developer will only have access to WordPress with permission to access and make changes to the eCommerce website. “High Security Systems” must only be accessed for security and/or maintenance purposes. All other employees not mentioned above will not have access to any of the company’s servers or databases. Server rooms storing network devices will require badge access, which will be accessible to the network administrators only. Access logs will be kept and maintained for these server rooms as well.

# Data support and operation

This policy applies to all Akwaaba systems that contain sensitive information. These systems must be protected according to the organization's standards, best practices, industry compliance standards and regulation. Data should be encrypted and protected by a firewall and anti-malware protection. Backup media should be safely and securely stored if physical or moved to cloud. Any data movement should only be transferred via secure protocols. All data copied to portable devices or transmitted on a public network should be encrypted.

# Security awareness and behavior

Akwaaba’s employees could access the company IT security policy online and they also have the option to have a paper copy of the policy in the IT security office. Every new employee would have training and a quiz about security policy. Every six months every single employee should finish a 30-minute security policy course. Employees are responsible for noticing, preventing, and reporting any social engineering attacks (for example phishing emails). The company needs to practice a clear desk policy- all laptops need to be secure with cable locks. Shred all documents that are no longer needed. Internet usage should be restricted, especially YouTube and other social media websites (Facebook, Instagram etc.) and these actions would be determined by IT security team. All unwanted websites should be blocked using a proxy system.

**Responsibilities, rights, and duties of personnel.**

Responsibilities are divided between the regular team members, the IT team, and members of the management team. All rights and duties of personnel are more specified in their rights and duties book for each department and the implementation of these activities should be monitored by the special management team. IT security team is responsible for periodically updating ISP and informing other parts of the Akwaaba’s company about these updates.