

TIP-Quezon City
College of Information Technology Education
Bachelor of Science in Information Technology

Meraki Co. Start-Up Security Proposal

In Partial Fulfillment
of the Requirement of the Course
IT 001-IT32S1 - Information Assurance and Security 1

Presented by:

Astudillo, Zeejay

Baniqued, Jocelle

Lorenzana, Jasmine

Soriano, Nygie Mae

Tacadino, Arrianne

Section:

IT32S2

Presented to:

Engr. Jerry E. Borromeo

Adviser

March, 2021

I. Introduction

Company Background

Meraki simply means creativity and love which is the foundation of our company. With the teamwork that we have, we are capable to serve thousands of customers every day. The Meraki Co. has a goal to guarantee customer health safety. The built e-commerce website ensures your trust and integrity. The Meraki Co. has the vision to provide the best quality of products and services for the best customers. Being the best means exceeding the customer's expectations because a healthy vision is for a brighter future. Our company provides different anti-radiation products and services.

Meraki Co. also is a start-up company. A start-up is a company that wants to produce or develop a product and services which the founders think there are high demands. They are also a company that is looking for venture capitalists or investors. Some examples of successful businesses we have today that started as simple start-up companies were Microsoft, Facebook, and Apple.

Overview

Meraki Co. is committed to protecting everyone's data and information. Security Policy explains how your personal information is collected, used, and disclosed by Meraki. The proposed security policies would also demonstrate how loyal the business is to its customers by protecting all the data we have. We take care to protect the safety of your records. We provide human, electronic, and managerial protocols to help protect, avoid unwanted access, preserve data protection, and use the information appropriately. The policy lays out internal security procedures that mitigate the risk of cybersecurity breaches.

Objectives

The proposed policy has a purpose to achieve the following:

- To provide a security policy that will fall to the following criteria: integrity, availability, authentication, confidentiality, and nonrepudiation.
- To keep the Meraki's reputation by strengthen or somehow repair the image of the company.
- To protect the company's network, management, data, employees, and its users from possible cybercrimes.

Scope

The security policy document defines common security requirements for all customers and personnel. We are also committed to secure the systems that create, maintain, store, access, process or transmit information. In the event of a conflict, the more restrictive measures apply. This policy extends its protection to a network practice infrastructure consisting of different hardware, software, networking facilities, and other instruments intended to assist the practice in the production, reception, storage, retrieval, and transmitting of information.

II. Security Policy

Integrity

Access Control

- Implementing the RBAC or the Role-Based Access Control in the company.
- Employees are only allowed to access the information necessary to effectively perform their job duties.
- Access control is a technique of ensuring that users and employees are who they claim they are and that they have adequate access to company information.
- Permission must be received from department heads prior to access to confidential data.

Error Detection

- To make sure our data will keep its integrity, the company needs to detect its error and fix it.
- Using different software like Screaming Frog, W3C Validator, Pingdom, and Web Page Test to make sure our system and website will not easily experience error.

Backup and recovery procedures

- Requiring the use of cloud services and database servers.
- Critical systems and services disaster recovery plans will be established and revised annually.
- File and data recovery plans will be maintained and followed with all devices and facilities. Backup media would be kept off-site to reduce damage. All media shall be rotated and destroyed on a routine basis.

Availability

Proper monitoring

- To make sure our contents and our website is available, our company need to focus on monitoring the running programs.
- To enhance the efficiency of our e-commerce site, we would need to introduce monitoring procedures that give us insight to take effective action.
- Some employees are required to constantly monitor the company's data and information.

Off-site backups

- Implementing off-site backups to make sure our data will still be available even after some crash and errors.
- The company must maintain an off-site secure storage facility where sensitive data is stored.
- A suitable off-site backup facility might be another entity, a company, etc. Some preferred storage medium types are tape and hard disk cartridges.

Server Clustering

- Server clustering refers to a group of servers working together on one system to provide users with higher availability.
- Implement this practice to our company to offer clients a higher level of availability, reliability, and scalability.

Authentication

Password

- To make sure the user's information will be secure, they need to provide a password that is exclusive for them.
- The users or customers were required to put at least 6 characters for password.

- At least 13 characters with numbers and special symbol were required for the employee's workstations.
- All system passwords are updated on an annual basis. Safe authentication guidelines will be always implemented.

Two-factor authentication

- Any users and customer can use two-factor authentication to make sure their account was totally secured. Google authenticator is suggested.
- Employees were required to have two-factor authentication.

Account Management

- The users were required to disclose all their information if they wanted to deactivate their accounts.
- To make sure the account still existing and secured, users were required to change their password twice a year.
- All accounts shall be checked at least periodically by the data owner to ensure that access and account rights are commensurate with the job function, the need to know, and the employment status.

Confidentiality

The following measures were designed for employees to ensure all the data were kept secure and confidential:

- Employees were requested to sign a non-compete or non-disclosure agreements (NDAs) for the protection of all records.
- Employees are prohibited in disseminating data that came from users.
- Employees are required to encrypt different electronic information and secure databases.
- If employees want to access some confidential information, they need to get a permission to the administrator or senior management.
- Employees must understand the consequence in breaching information.
- Employees who do not comply with our company policies will undergo punitive and, potentially, legal action.

III. Other Security Policies and Services

Monitored Security Systems

- The monitored security system is a system that are actively monitored by a professional home security. When the system detects a break-in, fire, or other emergency, it notifies the security team and, in some cases, emergency responders.
- Establish standard protocols for the design, implementation, training and management of intrusion and alarm systems within the company.
- Encourage the involvement of everyone in the self-policing of protected environments, protected doors and restricted areas.

Residential IT Support

- People whose expert in removing viruses, resolving errors, reinstalling or upgrading operating systems, and other fixes.
- Employees who get the appropriate backup system in order, with inexpensive, painless, automated cloud backup systems with reliable reporting.
- They can be also an on-call employees who can get rid of horrible spyware and viruses. Hold them out of place with powerful defense.

Privacy Policy

- This Privacy Policy explains how your personal information is collected, used, and disclosed by Meraki.
- Privacy Policy applies to our website named Meraki, and its associated subdomains. By accessing or using our Service, you signify that you have read, understood, and agree to our collection, storage, use, and disclosure of your personal information as described in this Privacy Policy and our Terms of Service.
- We may engage trusted third-party service providers to perform functions and provide services to us, such as hosting and maintaining our servers and our service, database storage and management, e-mail management, storage marketing, credit card processing, customer service and fulfilling orders for products and services you may purchase through our platform.

- We may share portions of our log file data, including IP addresses, for analytics purposes with third parties such as web analytics partners, application developers, and ad networks.
- In respect to any credit card or other payment processing details you have provided us, we commit that this confidential information will be stored in the most secure manner possible.

Security and Virus Protection

The security and virus protection policy were designed to maintain the integrity, confidentiality, and availability of our company. Our company divided the policy in to two different areas. These are the network and device.

Network

- If an attack is probable or inevitable, IT security could isolate the company's network from the rest of the Internet if no other defense is available.
- Employees will respond to any observed, probable, or imminent intrusion on the business network as they see fit under the Information Security Policies.

Device

- A workstation or other system that has been corrupted by the virus will be isolated from the company's network.
- The device that is infected with the virus will be required to be sent to IT maintenance and senior management for review before reconnection to the company network is authorized.
- The compromised device would need to be repaired and cleared of any threat to the company's network.

IV. Company Visualization

- Website

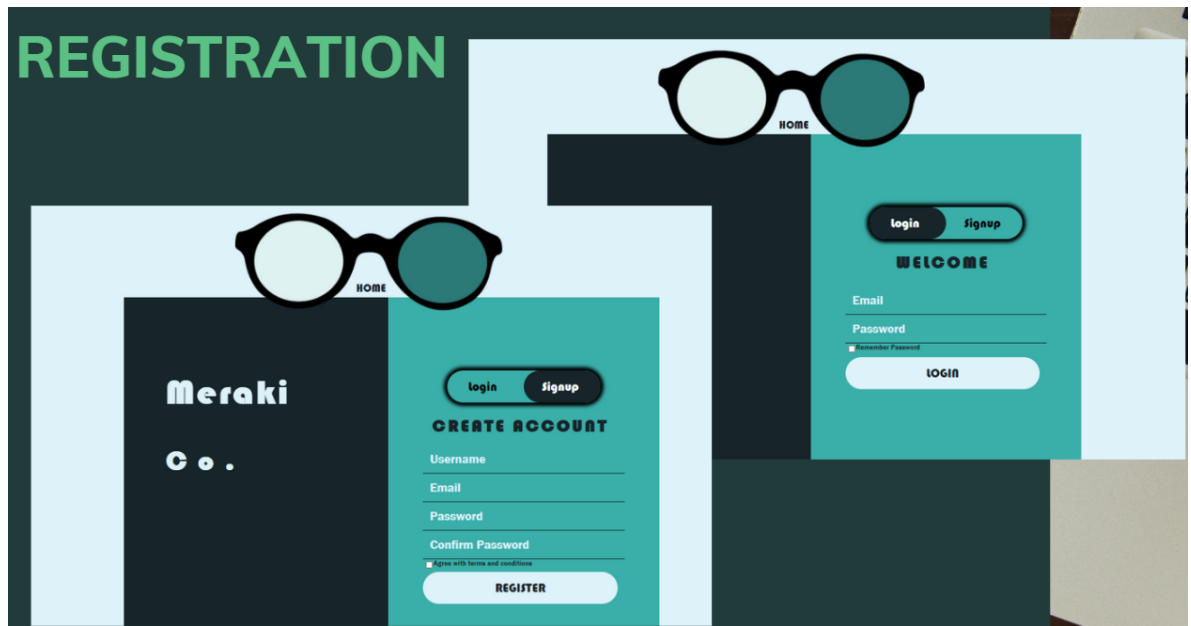


Figure 1. For the registration we wanted to implement the method of encryption to give security for the sensitive information to be saved to the database. We wanted to implement the hashing techniques for the password, so that it will not be easily read.

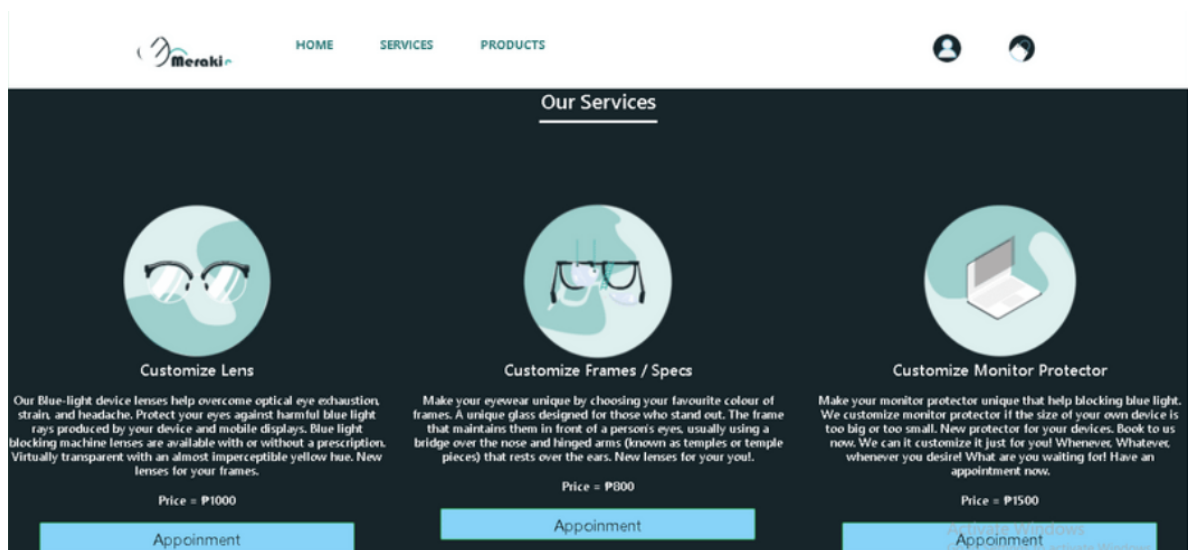


Figure 2. Our company provides customizing lens or anti-radiation and also offers services like pickup, for delivery and door-to-door customer service.

Services and Order Form

[HOME](#)
[SERVICES](#)
[PRODUCTS](#)
[LOGOUT](#)

[Appointment Cart /](#)
[Fill up for the Appointment Information /](#)
[Appointment Summary /](#)

First Name *
Last Name *
Email Address *
Phone *
Home Address *
City in Metro Manila *
Time*
Date*
Lens specifications*

Home Address *
City in Metro Manila *
Time*
Date*
Lens specifications*
Lens Type*
Lens Shape *

42945084

Book Now

Figure 3.. For the order form of our company we wanted to make sure that this sensitive information that we will gather will be safe and secure. As our company gathers information like bank accounts we wanted to implement the two-factor authentication so that whenever they have to pay, there would be a security after the payment being confirmed and processed.










+ Options								
				id	username	email	password	access
<input type="checkbox"/>				26	jasi1@gmail	jas@gmail.com	\$2y\$10\$IVsq7IOM8i8ac/0dVzPAermZU/h40a5.z5GKbCluhG...	admin
<input type="checkbox"/>				27	admin	admin@gmail.com	\$2y\$10\$feBCW0YXk6wtylzggC.CyukDO7AJVJIDcHn4GKANmDh...	admin
<input type="checkbox"/>				28	mi1o2	mi1o2@gmail.com	\$2y\$10\$nXc6j16jKEvp7IjUaXGI.YccvQxlvZLUbS9h6qFqrP...	admin

Figure 4. For this one is the hashing technique that we can implement for the security of our website, so that the passwords are hidden; also it has the account management to better handle who are the only authorized users that can use and access specific websites.

- Company Office

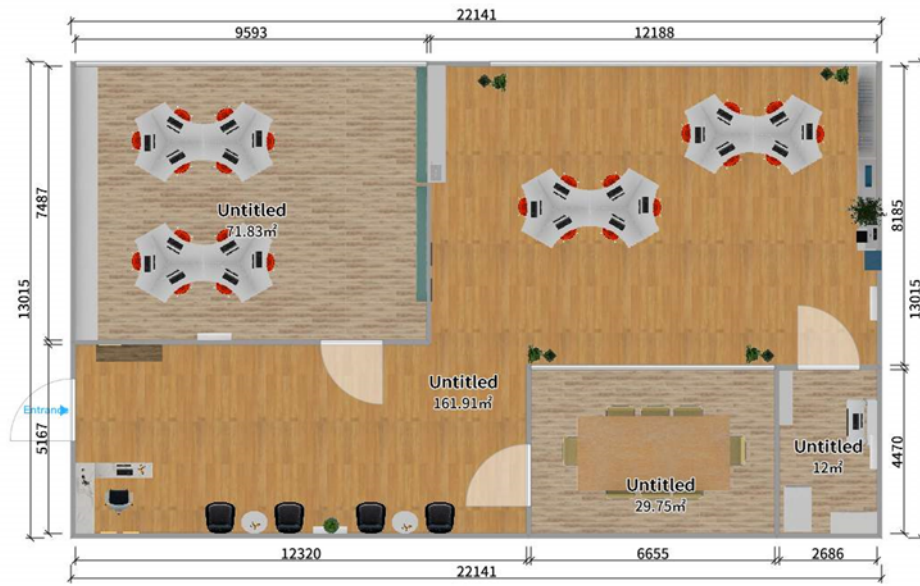


Figure 5. Floor plan for proposal for the company environment.



Figure 6. Proposal room for the IT department.



Figure 7. Proposal room for the IT department.



Figure 8.. Proposal for the meeting room and the server rooms.

V. Common Tools

The cybersecurity risks faced by companies differ widely. On the other hand, e-commerce companies face all the problems that regular firms face, and all the threats associated with ransomware, social engineering, and other similar attacks that everyone on the Internet might face. It is important for companies looking to retain a competitive edge to strengthen their cyber defenses. To ensure the safety of our company we used the following common tools:

Firewalls

- The Firewall will protect our business against malicious code. Any efficient firewalls will inspect the traffic coming in and out of your network. They search and block malware, worms, email, and other unnecessary internet traffic. They would also log attack attempts and other breaches of company policy. This helps us to investigate illegal login attempts and any unusual activities. Many of these efficient firewalls would also allow you to maintain a list of known malicious applications and known successful applications. They're going to ban malicious programs, thus allowing the successful ones.

W3C Validator

- W3C Validator validator tests the validation of Web documents in HTML, XHTML, SMIL, MathML, etc. If you want to validate particular information, such as RSS/Atom feeds or CSS stylesheets, MobileOK content, or find broken ties, other validators and tools are available.

Pingdom

- Pingdom lets our company gain instant visibility into the availability and efficiency of your website so that you can market for an exceptional end-user experience. Comprehensive tracking incorporates synthetic and end-user control with ultimate insight and improved troubleshooting.
- Simulate the contact of the user with the website to know whether and when important pages or services stop functioning correctly. Gain visibility about how individual end-users communicate with and experience the website with flexible and easy-to-use Real User Monitoring.

VI. References

[1] Confidentiality, integrity, & availability: Basics of information security. (2020, October 09). Retrieved March 15, 2021, from <https://smartebytechnology.com/confidentiality-integrity-availability-basics-of-information-security/>

[2] Canner, B. (2021, February 18). 7 access management best practices for enterprises. Retrieved March 15, 2021, from <https://solutionsreview.com/identity-management/7-access-management-best-practices-for-enterprises/>