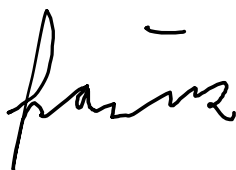


<b>Student Name/ID Number:</b>	Francis Roel L. Abarca – BDSE-0922-118
<b>Assignment Title:</b>	Project Report 2
<b>Module Name:</b>	BDSE-ISE-IT Security

### Learner declaration

I certify that the work submitted for this assignment is my own and research sources are fully acknowledged.

Student signature:



Date: June 13, 2024

## Summary

This security policy proposal outlines a plan to create a strong defense for our organization's valuable data and IT systems. Our main goals are to pinpoint and reduce security vulnerabilities, meet data protection rules, and cultivate a security-conscious culture across the board. To achieve this, we propose implementing strict access controls, conducting regular risk evaluations, and keeping a watchful eye on our IT environment to quickly identify and address potential security breaches.

## Introduction

In today's digital age, the organization faces increasing threats to its data and IT systems. Cyber-attacks, data breaches, and other security incidents can have severe consequences, including financial loss, reputational damage, and legal penalties. Therefore, a robust security policy is essential to safeguard the organization's assets and maintain trust with customers and partners.

The primary goal of this security policy is to provide a structured approach to managing and mitigating IT security risks. By outlining clear procedures and responsibilities, the policy aims to protect sensitive information, ensure compliance with relevant regulations, and promote a secure working environment. This policy will serve as a guide for all employees and stakeholders in maintaining and enhancing the organization's security posture.

## Security Risks

### **Types of Risks:**

- **Malware:** Any software that can cause harm to the servers and computer networks. Include viruses, trojans, and spywares
- **Phishing:** A type of attack where attackers deceive individuals into providing sensitive information. This can come in the form of emails, text messages, or voice call
- **Insider threats:** Risks posed by individuals who misuse their authorization or inadvertently cause security breaches due to careless actions
- **Data breaches:** Occurs when protected information is accessed without authorization.

## ISO Standards

### ISO 31000

ISO 31000 is a framework for risk management in all kinds of organizations. The intention is to assist companies in developing a culture of risk awareness and integration into all aspects of their operations.

#### Principles of ISO 31000

1. Make Risk Management a Part of Everything
  - Include risk analysis in all operational and decision-making processes within the company.
2. Be Thorough and Consistent
  - To guarantee consistent and similar outcomes, choose a methodical and thorough risk management procedure.
3. Customize the Approach
  - Modify the procedures and framework to the unique internal and external environment of the company.
4. Involve Everyone
  - Involve stakeholders at the appropriate moment to guarantee that their viewpoints are taken into account for improved risk management.
5. Remain Adaptable
  - Be prepared to modify risk management procedures when needed.
6. Utilize the Best Information
  - Base your choices on the most accurate and current information accessible.
7. Take Human Factor into Account
  - Recognize the capacities, attitudes, and goals of internal and external stakeholders.
8. Never Stop Improving
  - As you gain expertise, keep refining your risk management techniques.

#### Benefits of Implementing ISO 31000

- Sharpened Risk Awareness
  - Boost the organization's capacity to recognize, evaluate, and successfully manage risks.
- Wiser Decision-Making
  - To assess risk and make knowledgeable choices, apply an organized method.
- Enhanced Resilience
  - Create an organization that is more able to withstand unforeseen circumstances and adjust to change.
- Increased Stakeholder Trust

- Show a resolute dedication to risk management to inspire trust among stakeholders.
- Fulfilling Regulatory Requirements
  - Adherence to risk management-related laws and standards is easier.

## IT Security Audit Impact

### Benefits of Conducting an IT Security Audit:

1. **Vulnerability Detection:** Audits function as security inspections, identifying vulnerabilities in our IT systems that cybercriminals can take advantage of. We are able to address vulnerabilities before they become issues because to our proactive strategy.
2. **Stronger Security Generally:** Consistent audits guarantee that our security protocols are current and efficient, fortifying our general defenses against online attacks.
3. **Remaining Compliant:** Audits assist us in adhering to industry norms and laws such as GDPR and HIPAA. This keeps us out of trouble and preserves our good name.
4. **Wiser Risk Management:** Audits help us manage and lower risks more efficiently by seeing possible hazards and comprehending their implications.
5. **Better Processes and Policies:** Audits offer insightful criticism on our security protocols, pointing out areas in need of development.
6. **Establishing Trust:** Consistent audits show our dedication to security and foster trust among our stakeholders, partners, and customers.
7. **Incident Preparedness:** Audits assess our incident response strategy to ensure our ability to respond to security incidents promptly and effectively.

## **Strategies to Overcome Audit Challenges:**

1. Allocation of Resources (Time, Money, Expertise):
  - Recommendation: Incorporate audits into our routine IT planning and budget. If necessary, think about bringing in outside security professionals.
2. Opposition to Change:
  - Remedy: Clearly convey the value of security as well as the audit's conclusions. To make the process of adopting changes easier, offer support and training.
3. Scope Creep (Growing Outside of the Plan):
  - Remedy: Establish precise objectives and limitations for the audit right away. Check on progress frequently and make adjustments as needed.
4. Sensitivity of Data:
  - Remedy: Ascertain that every auditor executes confidentiality agreements and adheres to our data handling guidelines to the letter.
5. Adapting to Changing Dangers:
  - Recommendation: Perform routine audits and keep up with the most recent developments in security and emerging risks.

## Employee and Stakeholder Responsibilities

### **Employees:**

Our employees are essential for maintaining a strong security posture. Here's what we expect:

- Follow the Rules: Adhere Strictly to all security policies and procedures, such as creating strong, one-of-a-kind passwords and updating software with the most recent security updates. Take caution when handling sensitive data and adhere to established procedures.
- Stay Away from Unauthorized Tech: Avoid using unauthorized software or hardware on the business network as this may lead to security flaws.
- Report Security Concerns: Notify IT or the security team right once of any suspected security breaches or strange activity. This covers any security lapses, misplaced or pilfered gadgets, and any other anomalies. Participate completely in any security inquiry.
- Stay Informed: Take part in security awareness and training initiatives. Attend required sessions to get knowledge about current risks and information security best practices.

By fulfilling these responsibilities, employees help ensure our data remains accurate, private, and accessible while minimizing the impact of potential security events.

### **Stakeholders:**

Stakeholders are essential in supporting and directing our security activities, and they include management, board members, and important partners:

- **Provide Funds and Support:** Set aside the required funds and resources for personnel, training courses, and vital security equipment in order to keep strong security measures in place.
- **Form Security Policies:** Participate in the formulation, endorsement, and frequent evaluation of security policies. Ensure that these policies satisfy all legal and regulatory standards and are in line with the objectives of our firm.
- **Effectively Manage Risk:** Participate actively in the process of finding, evaluating, and reducing any dangers. Make sure that the foundation of our entire plan is risk management. By supporting these efforts, stakeholders help create a secure environment that safeguards our valuable assets and maintains the trust of our clients and partners.

Stakeholders contribute to the creation of a safe environment that protects our priceless assets and upholds the confidence of our partners and clients by supporting these initiatives.

## Security Policy Design

### **Access Control**

Access restrictions function similarly to digital gatekeepers, ensuring that only authorized individuals have access to our essential information. This involves:

- **Authentication and Authorization:** We will employ robust ways to verify user identities prior to giving access. Once validated, access permissions will be defined according to work roles, restricting what each individual may see and do.
- **Physical and Logical Controls:** We will protect both our physical locations (offices, equipment) and our digital environment (data, systems). Consider secured doors, passwords, biometric scanning, encryption, and secure connections.
- **Regular Audits and Monitoring:** We will conduct regular checks to ensure that our access restrictions are obeyed and to search for any unusual behavior. Continuous monitoring allows us to identify and respond swiftly to possible security problems.

### **Data Encryption:**

Data encryption converts information into unreadable code, prohibiting illegal access. It safeguards data both in transit and at rest. This way, even if someone does get their hands on our data, they will be unable to comprehend it. Encryption protects sensitive information such as money, personal details, and trade secrets. This not only keeps data confidential and correct, but it also allows us to comply with data protection regulations.

## **Incident Response Plans**

We have an incident response plan in place to handle security breaches. They assist us in minimizing harm and fast returning things to normal. This is how we get ready:

### **Incident Response Plan Components:**

- Preparation: We'll assemble a committed group and specify each person's tasks in detail. We'll also make sure that everyone is aware of what to do and set clear protocols for handling incidents.
- Identification and Analysis: We'll be keeping a careful eye on our systems for any clues that might point to a security problem. Any incidents will be thoroughly examined to determine their seriousness and any effects.
- Containment, Eradication, and Recovery: We'll move fast to remove any impacted systems and data, contain the issue, and eliminate its cause.
- Post-Incident Activities: We'll go over what happened in order to draw lessons from it, enhance our reaction, and make sure it doesn't happen again.

These components are essential to protecting our info. Robust access controls help to distinguish between legitimate users and possible intruders. By adding an additional degree of security, data encryption makes sure that only people with permission can access our information. Since incidents do occur, having a strong response strategy is essential to successfully managing any security issues.

# Tools and Technologies

## 1. Antivirus Software: The Frontline Defense Against Malware

- Examples:
  - Norton Antivirus: Offers real-time protection, virus removal, and robust online security features.
  - McAfee Total Protection: Combines antivirus, identity theft protection, and a secure VPN for comprehensive online defense.
  - Kaspersky Anti-Virus: Renowned for high malware detection rates with minimal impact on system performance.
- Benefits:
  - Real-Time Protection: Constantly scans for and neutralizes threats, preventing malware from infecting your systems.
  - Scheduled Scans: Provides the flexibility to run regular system checks for potential infections.
  - Automatic Updates: Ensures your antivirus software has the latest virus definitions to combat emerging threats.
  - Behavioral Analysis: Detects and blocks malware based on suspicious behavior, even if it's a new, unknown threat.

## 2. Network Monitoring Tools: Maintaining Network Health and Security

- Examples:
  - Wireshark: A powerful open-source tool for deep-dive analysis of network protocols, allowing you to capture and inspect network traffic.
  - Nagios: Offers comprehensive monitoring of systems, networks, and IT infrastructure, sending alerts for performance issues and recovery confirmations.
  - SolarWinds Network Performance Monitor: Provides in-depth network performance insights, including network path visualization and intelligent alerts.
- Benefits:
  - Clear Network Visibility: Provides real-time insights into network performance and traffic patterns, enabling rapid issue identification and resolution.



- Optimized Performance: Helps identify bottlenecks, abnormal traffic, and potential points of failure within the network, allowing for optimization.
- Security Monitoring: Aids in detecting suspicious network behavior that might indicate a security breach or malicious activity.
- Proactive Network Management: Enables proactive management by sending alerts about potential problems before they escalate into critical issues, minimizing downtime.

### 3. Security Information and Event Management (SIEM) Systems: Centralized Security Management & Threat Detection

- Examples:
  - Splunk Enterprise Security: Provides advanced threat detection, forensic capabilities, and tools for efficient incident management.
  - IBM QRadar: Combines security information and event management with network behavior analytics and log management for comprehensive security insights.
  - ArcSight ESM: Offers powerful security event correlation, analyzing security events in context to rapidly detect and respond to threats.
- Benefits:
  - Centralized Logging: Collects and aggregates log data from various sources into a central repository, streamlining security analysis and management.
  - Advanced Analytics: Leverages advanced analytics and machine learning to detect security threats and anomalies in real time.
  - Efficient Incident Response: Accelerates incident response by providing detailed insights and context surrounding security events and alerts.
  - Compliance Reporting: Helps organizations meet regulatory compliance requirements with robust reporting features and comprehensive audit trails.

## Conclusion

This security policy proposal outlined a strategy for securing our organization's data and IT systems from current threats. We utilize a mix of strict access restrictions, such as strong passwords and permissions, as well as physical and digital security features like encryption and biometrics. This guarantees that only the proper personnel have access to critical information, lowering the danger of data leaks.

The proposal involves encryption of sensitive data both during transmission and storage, allowing us to comply with standards such as GDPR and HIPAA. If a security event happens, we will have clear response strategies in place to promptly discover, contain, and resolve the breach, minimizing interruption and assuring the organization's ability to recover.

We will frequently examine our systems and monitor our IT environment to ensure that security regulations are followed and that 0-day attacks are prevented. Antivirus software, network monitoring, and SIEM solutions will help us discover and stop threats more quickly, therefore improving our overall security.

Finally, this policy strives to foster a security-conscious culture throughout the firm. We wish to earn trust and confidence by actively preserving our important assets and according to the regulations. By concentrating on prevention and timely reactions, we can stay ahead of the ever-changing cybersecurity scene, keep things operating smoothly, and safeguard our brand.