



ISO 9001:2015 Certified  
Level I Institutionally Accredited

Republic of the Philippines  
Laguna State Polytechnic University  
Province of Laguna

## **INFORMATION SECURITY ASSURANCE PLAN FOR DATA ELECTRICITY NEST INNOVATION**

### **Submitted by:**

Alaro, Rick Allen C.  
Carillaga, Vince Ashley M.  
De Leon, Melvin R.  
Samia, Antonio C. Jr.  
Sotto, Jerwin A.

BSIT 4B-SMP

### **Submitted to:**

**Ms. Micah Joy P. Formaran**  
Instructor

January 2024

## TABLE OF CONTENTS

TITLE PAGE .....	I
ACKNOWLEDGEMENT .....	III
CHAPTER I.....	1
SANPIT Municipal Financial Office .....	1
CHAPTER II.....	5
List of Resources .....	5
CHAPTER III .....	10
System Administrator.....	10
Security Training/System Users:.....	12
CHAPTER IV .....	13
IMPORTANCE OF SECURITY CONTROLS .....	13
Risk Management:.....	13
Confidentiality, Integrity, and Availability (CIA): .....	13
Compliance with Regulations: .....	13
Prevention of Unauthorized Access: .....	13
Protection Against Cyber Threats: .....	13
Trust and Reputation: .....	14
Financial Protection:.....	14
Prevention of Data Loss: .....	14
SECURITY CONTROLS – Back-up Recovery .....	14
SECURITY CONTROLS – Restore Process .....	15
SECURITY CONTROLS – Disaster Recovery .....	15
CHAPTER V .....	16

## **ACKNOWLEDGEMENT**

We are honored to use this opportunity to show our sincere gratitude to Ms. Micah Joy Formaran, a person of outstanding ability. Her efforts not just produced a big influence on our group, but they also made an eternal mark on the projects we worked on together. Her passion, professionalism, and consistent dedication to our shared objectives are highlighted by this acknowledgement.

One of the most important factors in our accomplishments is Ms. Formaran's extraordinary willingness to face down on challenging scenarios immediately and consistently produce outstanding results. Her remarkable skills at problem-solving and careful consideration to detail have elevated our standards for success in all of our tasks. We are managed to achieve the great milestones we have because of her persistent efforts and unique perspectives.

Besides her achievements within her area of expertise, Ms. Formaran has also contributed to a calm workplace which promotes creativity and cooperation. Her dedication to working together and preparedness to guide and assist one another not just making our tasks easier, but also developed our potential to improve together individuals. She is an inspiration for us all because of her interpersonal abilities and moral integrity.

We truly look forward to the opportunity to collaborate together Ms. Formaran in the decades that come. She proves to be an invaluable resource to our team, and we are really grateful to have the chance to work with someone that truly dedicated and proficient. We are motivated to discover what opportunities we may accomplish as a group.

This acknowledgement stands as a humble way to express our deep appreciation for Ms. Micah Joy Formaran. Our team will forever cherish her persistent dedication, outstanding remarks, and favorable impact, and we look forward to many in the future of accomplishment

## CHAPTER I

### INTRODUCTION

#### **SANPIT Municipal Financial Office**

Particularly, the accounting operation in the Municipality of Sanpit is managed by this office, the SANPIT Financial Office. The development of digital technology has made it an efficient tool for improving the effectiveness and productivity of accounting procedures in municipality departments. Data security and privacy are essential since confidential money-related data is managed. The collection of revenue could be simplified by using digital payment methods for taxes, fees, and other municipal services. This research will focus on how these systems are utilized and how that affects financial status production. This gives access to financial management, business licensing, municipal scholarships, and handling revenue. It guarantees that the local financial department is important in maintaining the privacy, security, and accessibility of the financial information. It will have access to databases or information that list the beneficiaries of scholarships and applicants as well as the amount of money granted. This Office would require access to the municipality's IT infrastructure in order to carry out its responsibilities properly. It includes servers, networks, and software systems that secure accessibility to financial information and databases for auditing purposes in order to ensure openness and adherence with regulations and laws.

The Financial Municipal Office's data center is in responsible for handling and storing all computerized information collected by and utilized inside. This involves tax information, financial records, budget data, and other private financial documents. It is the responsibility of the data center to make sure that information is organized efficiently, maintained securely, and easily accessible when needed. The data centers of Financial Municipal Office serve as the protectors of financial systems' smooth functioning, privacy of information, and transparency.

Here are the following people who can **access the database**:

- **Security Personnel** - Security personnel will keep track of who entered the data center, when, and for what reason. They'll also keep an eye on what's happening there and nearby. In order to conduct an investigation into the

occurrence, it may also be possible to obtain CCTV footage of the incident, incident reports, and employee activities.

- **Data Center Operators** – Data center operators have control over the daily administration and operation of the data center in addition to establishing and implementing disaster recovery plans. They are also in charge of maintaining the sensitive data, such as student information, related to the municipality's scholars.
- **Financial Accountant** – Financial accountants frequently use financial statements like income statements, balance sheets, and cash flow statements to analyze and report on the financial data of the municipality. They can also access budget data to track expenses and revenues and ensure that the municipality is adhering to its financial restrictions.
- **IT Personnel** – Responsible for maintaining strong safety protocols that protect sensitive financial data from intrusions, breaches, and cyberattacks. This includes measures including access restrictions, firewalls, and encryption as well as routine security assessments. IT personnel makes sure that crucial financial data can be recovered in the event of a hardware malfunction, human error, or other unanticipated catastrophes.

<u>SANPIT Municipal Scholar List</u>						
Name	Barangay	School	Year Level	GWA	Joined	Financial
<u>Alaro,</u> Rick Allen C.	San Francisco	San Francisco University	2 <sup>nd</sup> Year	91.1	2020	10,000
<u>Carillaga,</u> Vince	San Diego	San Diego University	4 <sup>th</sup> Year	90.4	2021	50,000
De Leon, Melvin	Chicago	Kentucky University	1 <sup>st</sup> Year	78	2022	77,000
<u>Sotto,</u> <u>Jerwin</u>	<u>Ele-Ele</u>	<u>Ele-Ele</u> University	3 <sup>rd</sup> Year	77.7	2023	25,000
<u>Samia,</u> Antonio C. Jr.	<u>Sampalukan</u>	<u>Sampalukan</u> School	Grade 11	75	2018	500
<b>Total:</b>	<b>5</b>					

The table above shows the list of Municipal Scholars. This is one of the responsibilities of the Municipal Financial Office Data Center. The Data Center Operators handle this list and pass it on to the Financial Accountant to record important information. Data Center Operators are also responsible for managing Scholar Applicants to avoid errors to Financial Accountants. Moreover, computerized systems enhance the security of scholar information. This is particularly important in safeguarding the personal and academic information of students, ensuring their privacy is respected and reducing the risk of data breaches.

## CHAPTER II ARCHITECTURE



A. Physical Layout (one pager layout)

### B. List of Resources Needed

#### - Security Infrastructure

- Firewall: 11 units
- Security cameras: 4 cameras, 1 camera each room
- Antivirus software: it is installed in every computer
- VPN: install in every computer

#### - Network Infrastructure (router, modem, etc.)



- Router: 3
- Switch: 3
- Wireless Access Point: Aircon, cctv cameras, motion detector

- Network Cable: each room has one network cable
- Network Security: antivirus,VPN




#### Server Infrastructure (hardware requirement of the server)



- Smart phone: 1 smartphone for security camera
- Smart TV: 1 for conference room
- Server Hardware: 1
- Telephone: 11, 8 for data center, 1for it personel, 1 for financial accountant and 1 for conference room
- Printer : 3, 1 each room
- Cooling System: 4 Aircon, 1 each room
- Back-up and Recovery System: all the units and flashdrive
- Uninterruptible Power Supply: Generator

#### List of Resources


Equipment + Picture	Unit Price	Quantity	Subtotals
<b>PC</b> 	15,000	11	165,000
<b>Server</b> 	13,000	1	13,000



<div>Router</div> <div></div>	4,000	3	12,000
<div>Mobile Phone</div> <div></div>	8,000	1	8,000
<div>Motion Detector</div> <div></div>	5,000	1	5,000

<p><b>Flashdrive</b></p> 	800	1	800
<p><b>Printer</b></p> 	5,000	3	15,000

<div>Switch</div> <div></div>	3,000	1	3,000
<div>CCTV</div> <div></div>	5,000	4	20,000
<div>Smart TV</div> <div></div>	18,000	1	18,000
<div>Generator</div> <div></div>	9,000	1	9,000
<div>Aircon</div> <div></div>	5,000	4	20,000

<div data-bbox="196 322 464 573"></div> <div data-bbox="295 584 440 622"><b>Telephone</b></div>	<div data-bbox="699 271 772 309">3,200</div>	<div data-bbox="1005 271 1037 309">11</div>	<div data-bbox="1273 271 1347 309">6,400</div>
--	--	---	--

# CHAPTER III

## USER ACCESS CONTROLS AND POLICIES

### System Administrator

Security Personnel	<p>Physical Security:</p> <ul style="list-style-type: none"><li>- Implement strict access controls to data centers.</li><li>- Monitor and log physical access.</li></ul> <p>Surveillance:</p> <ul style="list-style-type: none"><li>- Utilize surveillance systems to monitor sensitive areas.</li><li>- Establish protocols for reviewing and responding to security footage.</li></ul> <p>Emergency Response:</p> <ul style="list-style-type: none"><li>- Develop and communicate emergency response plans.</li><li>- Conduct regular drills for security personnel.</li></ul> <p>Communication Protocols:</p> <ul style="list-style-type: none"><li>- Establish secure communication channels for sensitive information.</li><li>- Regularly update encryption protocols.</li></ul>
Data Center Operators	<p>Environmental Controls:</p> <ul style="list-style-type: none"><li>-Maintain optimal temperature and humidity levels.</li><li>-Implement fire suppression systems.</li></ul> <p>Equipment Handling:</p> <ul style="list-style-type: none"><li>-Define guidelines for handling and installing equipment.</li><li>-Regularly inspect and maintain hardware.</li></ul> <p>Inventory Management:</p> <ul style="list-style-type: none"><li>-Keep an up-to-date inventory of all hardware.</li></ul>

	<ul style="list-style-type: none"> <li>-Implement a secure disposal process for retired equipment.</li> </ul>
Financial Accountant	<p>Access Controls:</p> <ul style="list-style-type: none"> <li>-Restrict access to financial systems to authorized personnel only.</li> <li>-Implement segregation of duties to prevent fraud.</li> </ul> <p>Data Encryption:</p> <ul style="list-style-type: none"> <li>-Encrypt sensitive financial data during transmission and storage.</li> <li>-Regularly update encryption protocols.</li> </ul> <p>Audit Trails:</p> <ul style="list-style-type: none"> <li>-Maintain detailed audit trails for financial transactions.</li> <li>-Regularly review and reconcile financial records.</li> </ul>
IT Personnel	<p>Software Development Guidelines:</p> <ul style="list-style-type: none"> <li>- Follow secure coding practices.</li> <li>- Regularly update and patch software.</li> </ul> <p>Network Security:</p> <ul style="list-style-type: none"> <li>- Implement firewalls and intrusion detection/prevention systems.</li> <li>- Regularly conduct vulnerability assessments.</li> </ul> <p>User Training:</p> <ul style="list-style-type: none"> <li>- Provide ongoing cybersecurity training to all employees.</li> <li>- Educate users on the importance of security practices.</li> </ul> <p>Device Management:</p> <ul style="list-style-type: none"> <li>- Enforce policies for securing mobile devices and laptops.</li> <li>- Implement remote wipe capabilities for lost</li> </ul>

	or stolen devices.
--	--------------------

### **Security Training/System Users:**

Security Personnel	Security personnel play a critical role in maintaining the safety of our facilities by diligently monitoring surveillance systems and enforcing access control policies
Data Center Operators	Data center operator helps ensuring the physical and digital security of our servers is paramount, requiring strict access controls and vigilant monitoring of environmental conditions.
Financial Accountant	In the realm of finance, accountants must stay vigilant against phishing attempts and adhere to strict password management practices to safeguard sensitive financial information.
IT Personnel	IT personnel are at the frontline of cyber security, responsible for implementing robust network security measures, conducting regular software updates, and educating users on best practices to mitigate evolving threats.

## **CHAPTER IV**

### **SECURITY CONTROLS**

- Security controls are guarantees or techniques implemented together by an organization to handle and mitigate threats to information security. Data and system availability, confidentiality, and integrity must all be maintained by these precautions. Security controls have a wide range of forms, and they may be separated into multiple categories according to the task they perform.

#### **IMPORTANCE OF SECURITY CONTROLS**

##### **Risk Management:**

- Security controls help identify, assess, and manage risks to an organization's information assets. By implementing controls, organizations can mitigate or reduce the impact of potential security threats.

##### **Confidentiality, Integrity, and Availability (CIA):**

- Security controls protect the confidentiality of sensitive information, ensuring that it is only accessible to authorized individuals. They also maintain the integrity of data, preventing unauthorized tampering or modification. Additionally, controls contribute to the availability of systems and data, ensuring that they are accessible when needed.

##### **Compliance with Regulations:**

- Many industries and jurisdictions have specific regulations and compliance requirements related to the protection of sensitive information. Security controls help organizations adhere to these regulations and avoid legal and financial consequences.

##### **Prevention of Unauthorized Access:**

- Access controls, encryption, and other security measures prevent unauthorized individuals from gaining access to systems and sensitive data. This is essential for protecting against data breaches and unauthorized use of information.

##### **Protection Against Cyber Threats:**

- In the face of evolving cyber threats such as malware, ransomware, and phishing attacks, security controls act as a frontline defense. They help detect, prevent, and respond to these threats, reducing the likelihood and impact of security incidents.



**Trust and Reputation:**

- Implementing robust security controls enhances the trustworthiness of an organization. Customers, partners, and stakeholders are more likely to trust an entity that demonstrates a commitment to protecting sensitive information and maintaining a secure environment.

**Financial Protection:**

- Security incidents, such as data breaches or system compromises, can have significant financial implications, including direct financial losses and costs associated with recovery and remediation. Security controls help minimize the financial impact of such incidents.

**Prevention of Data Loss:**

- Controls such as data encryption, backup, and data loss prevention mechanisms help prevent the loss of critical data. This is essential for protecting intellectual property, customer information, and other sensitive data.

**Explanation:** Security controls are essential for maintaining the overall health and resilience of an organization's information security posture. They provide a structured approach to risk management, help ensure compliance with regulations, and protect against a wide range of security threats, ultimately contributing to the organization's success and sustainability.

**SECURITY CONTROLS – Back-up Recovery**

Possible Threats	Recovery Plan	Resources Needed	Personnel In-charge
<ul style="list-style-type: none"> <li>- Hardware failure</li> <li>- Accidental data deletion</li> <li>- Ransomware attack</li> </ul>	<ul style="list-style-type: none"> <li>- Establish automated backup schedules and offsite storage.</li> <li>- Automated recovery scripts for quick restoration.</li> <li>- stored on secure,</li> </ul>	<ul style="list-style-type: none"> <li>- Network bandwidth.</li> <li>- Backup software</li> <li>- Secure storage using cloud or physical</li> </ul>	<ul style="list-style-type: none"> <li>- Security Personnel</li> <li>- IT Personnel</li> <li>- Data Center Operators</li> </ul>

	offsite location - Test backups regularly.		
--	---	--	--

### SECURITY CONTROLS – Restore Process

Possible Threats	Recovery Plan	Resources Needed	Personnel In-charge
- Incomplete or corrupt backups - Human error during restore.	- Document successful restores. - Test restore process regularly. - Defined restore procedures for different scenarios (individual files, entire systems)	- Trained personnel. - Dedicated test environment - Restore documentation	- Financial Accountant - IT Personnel - Data Center Operators

### SECURITY CONTROLS – Disaster Recovery

Possible Threats	Recovery Plan	Resources Needed	Personnel In-charge
- Natural disasters - fire - Cyberattacks causing widespread IT outage.	- Offsite DR facility or cloud environment with pre-configured systems and data replicas - Activate DR plan only for major incidents. - Train personnel on DR procedures.	- DR facility/cloud services - Communication channels - Training materials.	- Security Personnel - IT Personnel

## **CHAPTER V**

### **DOCUMENTATION**

#### **Format**

**Font Style:** Times New Roman

**Font Size:** 12

**Paragraph Spacing:** 1.5

**Margin:** Normal

