Information Security Policy and Guidelines

Ver. 2.00

PHILKOEI INTERNATIONAL, INC.
CONSULTANTS • PLANNERS • ENGINEERS

2024-July-01

Contents

Version Control

Version	Date	Details	Author
1.00	2021-Jul-01	1st release	BRFuertes/ JACBeringuela
2.00	2024-Jul-01	Based on ISO/IEC 27001 (ISMS) and NK/ID&E's Departmental Compliance	BRFuertes

1. Introduction

1.1. Definition of Information Security

a. Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (src: https://csrc.nist.gov/glossary/term/information_security)

b. Information security, often referred to as “InfoSec”, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection. (src: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html)

1.2. Purpose

The intention of this document is to provide an overview of information security principles by introducing related concepts and the security controls that Philkoei International, Inc. (PKII) (or the “Company”), can leverage to securely manage the information assets and systems.

1.3. Intended audience

The target audience of this document is for those new to the information security principles and tenets needed to protect information assets and systems in a way that is commensurate with risk.

This document will provide a basic foundation of concepts and ideas to any PKII personnel tasked with or interested in understanding how to secure its information assets and systems.

PKII personnels may refer to the latest IT Policy of the Company for the other items that are not mentioned in this document.

2. Basic Policy on Information Security

PKII makes it its basic policy on information security that it will take all possible measures to ensure the safety and reliability of the information assets widely used in the execution of our business and to ensure information security, thereby meeting the confidence placed in us by society, our clients and our business partners.

PKII declares that it will without fail observe the following:

1. The Company shall take appropriate measures for the management of information security with respect to each and every information asset handled in the course of its business;
2. All personnel handling information assets in the execution of the business of the Company shall recognize the importance of information security, abide by this basic policy on information security and act in accordance with regulations, such as management standards and procedures, determined on the basis of this policy;

3. The Company shall endeavor to ensure that information assets entrusted to the Company in the course of business are used appropriately and protected from exposure, while giving special recognition to the importance of such information assets;
4. The Company shall comply with the laws and standards relating to the management of information security; and
5. The Company shall develop a structure for the management of information security and shall carry out continuous improvement activities to combat new threats to information assets.

3. Principles of Information Security

There are three (3) principles of InfoSec namely:

Confidentiality, Integrity, and Availability (CIA).

It is a model within Information Security that is designed to guide policies within an organization and is used to introduce controls and remediation strategies along with the primary security infrastructure of the organization.

Confidentiality (C)	Characteristics that make information unusable or private to unauthorized individuals, entities (e.g., groups), or processes. -or- Information security efforts should endeavor to keep information private, ensuring that only those with permission can access a given data set.
Integrity (I)	refers to the property that protects the accuracy and completeness of an asset. -or- The information should have integrity, meaning that users can be confident that it has not been modified or selectively deleted by accident or malicious act.
Availability (A)	The characteristic of being available for access and use when requested by an authorized entity (e.g., organization). -or- Information should be available to users to the greatest extent possible, ideally 100% of the time.

4. Information Management Regulations

4.1. Objectives

The Information Management Regulations' Objective is to determine the necessary matters relating to the management of information held by the company, and by so doing to manage the information appropriately and prevent it from being leaked.

4.2. Information Assets

Definition

We define "information assets" as information held by the company that must be protected. "Information assets" include insider information, personal information of employees, and confidential information of contract work.

Classification of Information Assets

Secret	Extremely sensitive and of the highest value to the organization.
	Unauthorized access or disclosure would be critically damaging to the organization.
	Access should be limited to a very limited small number of names and authorized individuals.
Confidential	Sensitive and confidential within the organization.
	Unauthorized access or disclosure would be critically damaging to the organization.
	Access should be limited to those with a legitimate business need.
Internal	Non-sensitive and used for day to day operations within the organization.
	Unauthorized access or disclosure would be inconvenience but not critical.
	Access should be limited to workers within the company.
Public	Non-sensitive information and can be made publicly available.
	Unauthorized access or disclosure would not be an issue.
	Access does not need to be limited to anyone.

Types of Information Assets

Types of Information Assets			
		InfoSec	CyberSec
digital	data stored electronically	✓	✓
material form	paper-based	✓	
knowledge	know-how from employees, clients, business partners	✓	

4.3. Confidential Information

Definition

Confidential information is defined as any data or know-how that a disclosing party offers a receiving party, orally or in writing, that is meant to be private. The receiving party reasonably understands its confidential nature and any circumstances that would call for disclosure of said information.

For example, confidential information may include financial projections, business forecasts, customer lists, employee information, sales, patents, and trade secrets.

Confidential information plays an essential role in companies as it helps protect the company from losing any vital information necessary for the business's success. (src: https://study.com/academy/lesson/confidential-information-legal-definition-types.html)

Types of Confidential Information

1. Personal data	Information concerning specified individuals that has been made into a database
2. Customer secrets	Information concerning receipt of orders, joint research, etc., designated as confidential information
3. Business secrets	Non-public information concerning business, technology, manufacturing methods, etc. that is useful for business and designated as confidential information
4. Management secrets	Confidential information concerning personnel management, planning and finance, etc. and designated as confidential information

5. Information Security Management System (ISMS)

Information Security Management System (ISMS) is an ISO/IEC 27001 international standard, and refers to a process cycle (PDCA mechanism) to manage organizational, human, physical, and technical measures and their operation to ensure and maintain information security

ISMS Processes

Plan	As the establishment of ISMS, specific plans and goals for ensuring information security are formulated. (Scope of application, organization, risk assessment, risk response, etc. are formulated.)
Do	Implement and operate countermeasures based on the plan as a risk response.
Check	Monitors and reviews ISMS.
Action	Improvements and actions are taken based on the review.

5.1. Risks in ISMS

Risks in ISMS refers to the impact of "loss of Confidentiality, Integrity and Availability (CIA) of information assets" due to vulnerabilities that may allow threats to slip through existing countermeasures against the "information assets".

5.2. Risk Assessment

Identifying, analyzing, and evaluating risks is called risk assessment, the results of which determine subsequent actions.

With respect to the assessment of risk, risk management is

“Risk assessment = magnitude of loss (impact) x probability of occurrence (frequency)”.

However, in ISMS, it is necessary to make it a little more concrete and consider it as "value of information assets," "threat level (probability and frequency of occurrence) and its magnitude," and "vulnerability level (degree and extent)," as shown below.

"Risk assessment = asset value x threat level (probability and magnitude of occurrence) x vulnerability level (degree or extent)".

5.3. Risk Response

After the risk assessment, a response is required for risks that exceed the acceptance criteria. Since this response has been in accordance with ISO 31000 since 2013, the following seven (7) risk responses are required:

1. Avoid risk by not initiating or continuing risk-generating activities
2. Taking or increasing the risk of an opportunity in order to pursue it
3. Eliminate sources of risk
4. Change the likelihood of this happening.
5. Change the outcome (outcomes are the consequences of risk events: impact, damage, profit gain, etc.)
6. Share its risks with one or more other companies (including contracts and risk financing)
7. Own that risk by making informed decisions

5.4. Risk Measures

ISMS requires the implementation of various measures (called control measures in ISMS) to deal with undesirable outcomes as a risk response. As outlined below, there are 14 major categories of measures (A.5 to A.18)

Reference control objectives and controls (Annex A)
ISO/IEC 27001:2013

1	A.5	Policy Groups for Information Security
2	A.6	Organization for Information Security
3	A.7	Security of Human Resources
4	A.8	Asset Management
5	A.9	Access Control
6	A.10	Cryptography
7	A.11	Physical and Environmental Security
8	A.12	Supplier Management
9	A.13	Communication Security
10	A.14	Acquisition, development and maintenance of systems
11	A.15	Supplier Management

12	A.16	Information Security Incident Management
13	A.17	Information Security Aspects of Business Continuity Management
14	A.18	Compliance

PKII IT Department shall soon revise this document and implement the above list of reference control objectives as risk measures.

For the meantime, please refer to the next chapter on PKII's current measures and compliance on Information Security.

6. Current Measures and Compliance

6.1. Compliance with Basic Policy

Code of Conduct

This Code of Conduct is taken from the ID&E Group Code of Conduct that states:

"ID&E Group strictly protects and controls all information obtained in the course of business and prevents abuse and leaking of such information. ID&E Group also maintains the systems of compliance to prevent insider trading."

Specific standards of conduct for employees are as follows:

1. Build and maintain an information infrastructure in accordance with the Information Security Policy.
2. Recognize the importance of all information, including client and personal information, and collect, record, control, use, and dispose of confidential information as appropriate.
3. Place priority on fulfilling the responsibility to protect the confidentiality of the contract. All formal and informal confidential information on customers and clients, business partners, and corporate management, technologies, and sales and marketing is strictly controlled during your tenure of office or even after retirement. Do not disclose information to third parties without prior permission, in order not to cause damage to the concerned parties or use it for your own or any third party's benefit.

Basic Policy on Information Security (Information Security Initiatives)

1. PKII shall take appropriate measures for the management of information security with respect to each and every information asset handled in the course of its business.
2. All personnel who handle information assets in the execution of the business of PKII shall recognize the importance of information security, abide by this basic policy on information security and act in accordance with regulations, such as management standards and procedures, determined on the basis of this policy.
3. PKII shall endeavor to ensure that information assets entrusted to our Group in the course of business are used appropriately and protected from exposure, while giving special recognition to the importance of such information assets.

4. PKII shall comply with the laws and standards and contractual obligations relating to the management of information security.
5. PKII shall develop a structure for the management of information security and shall carry out continuous improvement activities to combat new threats to information assets.

6.2. On (the use of) Information Devices and Software

DO NOT USE information devices and software that are NOT company assets, including personally owned devices, for business purposes.

Business use of information devices and software that are not personally owned or the property of the company ("non-company") increases the possibility of license violations and the company's inability to control security, so the following must be observed:

- Do not install company software on non-company information devices.
- Do not install non-company software on company-issued information devices.
- Use company information devices to create, edit, save, and view business information by using services provided or permitted by the company.

However, the use of non-company information devices as authentication devices for services provided by the company (the Authenticator application for smartphones can be used with personal smartphones), and the use of non-company information devices owned by individuals for outsourced or quasi-subcontracted work under a non-disclosure agreement are permitted provided that appropriate information security measures are in place.

6.3. Disposal of Information Assets

On paper-based documents

- All paper-based documents especially those categorized as Confidential shall be destroyed through the use of paper shredder prior to disposal.

On digital media devices

- The IT Department shall initiate the assessment of devices subject for disposal and shall detach the hard disk drives on the device.
- The use of an electric drill to penetrate the hard disk drives will be utilized in order for its datafiles to be no longer recoverable.
- In the case of re-using the hard disk drives, the IT Department shall re-format the drive and install a new Operating System.

6.4. Measures to Prevent Loss or Theft of Information Devices

On paper-based documents

- Avoid unnecessary taking out of confidential and business information from the office premises.
- Archived Information assets such as confidential and business documents are located in the storage room equipped with e-door lock and surveillance (CCTV) camera.

On digital devices (IT/Technical equipment)

- Encryption with the use of BitLocker to company-owned laptops.
- Servers are located in the server room equipped with e-door lock and surveillance (CCTV) camera.
- Servers are equipped and configured with the Redundant Array of Independent Disks (RAID) technology.
- Desktop PCs are set with a password screen lock.
- Regular incremental backups of company-owned laptops to the cloud.
- Weekly incremental backups of all file servers to the cloud.

6.5. Measures to Prevent Data Leakage and Loss due to Viruses and Other Malware

Data leakage or loss due to malware is one of the most common causes of electronic information incident, and this section describes countermeasures against such leakage or loss.

- Do not open links (URLs) or attachments in the body of the e-mail that you do not recognize.
- Make sure that the virus definition files of anti-virus software such as eScan or Windows Defender are up-to-date.
- Please apply security patches to Operating System (OS) and applications on a regular basis. (Prohibit the use of end-of-support products, apply Windows Update, etc.)
- In principle, the transfer of data via USB memory devices to/from persons outside the company is prohibited.
- Please use Microsoft Edge as your browser and enable security settings such as [Settings] -> [Privacy, Search, Services] -> [Windows Defender SmartScreen].
- Do not use software in company-owned devices that is not work-related.
- Please refrain from using the Internet and Social Networking Sites (SNS) for non-business purposes.
- In File Explorer, set Show extensions in folder options.
- Do not share folders on your computer (use server or Cloud Services).

- If you suspect infection, immediately disconnect the network (unplug the LAN cable or disconnect Wi-Fi) and contact the IT Department for appropriate action.
- Automatic forwarding of e-mails is prohibited.

6.6. Software License Compliance

- Software, including operating systems (OS), must be used in compliance with the license.
- The use of pirated software is PROHIBITED.
- Microsoft, Adobe, Autodesk, Bentley and other Architectural, Engineering and Construction (AEC) software products should be purchased from its Authorized Distributor through the Admin-Purchasing Department with technical recommendations from the IT Department.

6.7. Protection on Usernames and Passwords

Since fraudulent acts such as identity theft may be considered as information leakage, please take the following measures.

- Do not use passwords that are easily guessed (name, date of birth, etc.).
- Access to PKII Intranet requires users to have passwords with at least:
  - not less than 7 characters
  - should be alphanumeric (with numbers and letters)
  - should have both UPPERCASE and lowercase letters
  - password expiry is 30-days for Accounting/Finance Department, while 90-days for the other Departments
- Please use one ID per person and do not share your password with others. And also, do not use the same ID and password as for services outside the company.
- Please enable multi-factor authentication for cloud service accounts contracted by each company and office, such as Microsoft 365.
- Ensure that employee IDs are managed (issuance/deletion) using an employee management system or other means.

6.8. Secure Server Location and Appropriate Access Rights

- Servers are located and installed in the server room in PKII central office.
- The server room is equipped with electronic door lock and surveillance (CCTV) camera.
- Only IT Department personnel are allowed to access the Server Room.
- When storing information that is subject to confidentiality obligations, such as contracts, or

personal information or important secrets on the server, please ask the IT Department to set appropriate access rights.

6.9. Preservation of Data

- Please save your business files to PKII's file servers or cloud storage such as SharePoint. This is because file servers have data redundancy and SharePoint backs up data.
- If the above is not available, back up to an encrypted external storage device, disconnect the encrypted external storage device after the backup is complete to prevent ransomware infection, and connect it only when necessary.
- Please back up important business data in progress to the designated PKII file server.
- For remote workers, the use of VPN to connect to the PKII file servers for downloading and uploading of datafiles is encouraged. The use of web-based access to the PKII file servers such as quickconnect.to is only used with the appropriate access rights and allowed by the IT Department.

6.10. Measures for Sending and Receiving Business Information

- When receiving an email, be sure to check the sender's e-mail address if correct, and do not rely only on given names.
- When sending an email outside the company, be sure to check the recipient and include the relevant persons in the CC.
- When attaching files such as Important Confidential Information, it is advisable to password-protect the file/s, and send the password to a separate e-mail, or other means of communications such as through text messaging or messaging app.
- For sending large files, please ask the assistance from the IT Department to create a cloud (download) link from the PKII file server, then send that link to your recipient.

6.11. Use of Other Services

- When using information and communication services, whether within or outside the company, in principle, please use the services provided and allowed by the IT Department. When using Internet services such as provider contracts, cloud services, file storage, web construction, mailing lists, schedule sharing, and VPN services, please consult with the IT Department in advance.
- Please avoid using free online services because the provider is granted the right to use, edit, reproduce, display, and distribute the data stored in the free service.
- Please consult with the IT Department regarding the network devices you wish to be connected to the in-house LAN or WiFi. Currently, no personal devices are allowed to connect, unless special

arrangements were carried-out by the requesting Department and assessed by the IT Department to be free of malware and no unlicensed softwares installed.

- In principle, the use of software and hardware that may cause problems for others is prohibited, including remote access and file exchange with outside the company, as well as software and hardware that may place a heavy load on the network.
- Posting business information on social networking sites (SNS) or Internet bulletin boards is prohibited. Furthermore, please be aware that unintentional remarks or slanderous remarks may be reprehensible.
- Please avoid in-house use of personal devices other than Windows OS including Linux. If you have a business reason, please contact the IT Department. If security measures are not appropriate, there is a possibility that malware may be distributed or used as a jumping attack.

6.12. Recognize Logging

- Logs are obtained for information systems and networks in case of audits or information security incidents/accidents. The IT Department shall regularly monitor the logs for suspicious activities and shall initiate archiving for future retrieval, if investigation is required.
- Other Departments shall provide their own paper-based logs for their business processes.

6.13. Service Level Agreement (SLA)

- When contracting with subcontractors, the concerned Department shall obtain a written pledge regarding the maintenance of confidential information, and ensure that antivirus or security software is installed on the PCs and other devices used by the subcontractors.
- Service Level Agreements (SLA) shall be prepared and signed by both parties.

6.14. Immediate Contact for Any Issues on Information Security

- If something happens about information security to prevent the spread of damage, please contact the IT Department immediately through support@philkoei.com.ph