Information Security Regulations

(or Data Privacy Manual)

V1.00

PHILKOEI INTERNATIONAL, INC.
CONSULTANTS • PLANNERS • ENGINEERS

Version control

Version No.	Date	Details	Author
1.00	2021-Jul-01	1st release	BRFuertes/JACBeringuela

Table of Contents

Introduction

This **Information Security Regulations** or **Data Privacy Manual** is hereby adopted in compliance with **Republic Act No. 10173** or the **Data Privacy Act (DPA) of 2012**, its Implementing Rules and Regulations, and other relevant policies, including issuances of the **National Privacy Commission**.

Philkoei International Inc. (PKII) respects and values your data privacy rights, and makes sure that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

Definition of Terms

"Data Subject" – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization. It may refer to officers, employees, consultants, and clients of this organization.

"Personal Information" – refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

"Processing" - refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

"The Company" or "The Organization" - refers to Philkoei International Inc. (PKII)

Scope and Limitations

All personnel of PKII, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Data Privacy Manual.

Processing of Personal Data

1. **Collection**

PKII collects the basic contact information of its personnel, clients and customers, including their full name, address, email address, contact number, and other Personal Information, together with the other information in relation to the project and/or the services they are involved.

The Human Resources Department (HRD) together with the Business Development Department (BDD), and as well as the Accounting and Finance (ACT/FIN) Department will collect such information from the Data Subject.

2. Use

Personal data collected shall be used by PKII for documentation purposes, for the duration of the Data Subject's project involvement, and for other purposes needed within the PKII organization.

3. **Storage, Retention and Destruction**

PKII will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. PKII will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

All information gathered shall not be retained for a period longer than **ten (10) years**.

After ten (10) years, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

4. **Access**

Due to the sensitive and confidential nature of the personal data under the custody of the company, only the Data Subject and the Authorized Representative of PKII shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

5. **Disclosure and Sharing**

All employees and personnel of PKII shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations.

Personal data under the custody of PKII shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

Security Measures

A. **Organization Security Measures**

1. Data Protection Officer (DPO), or Compliance Officer for Privacy (COP)

   The designated DPO or COP is **Mr. Jose Adones Beringuela**, who is concurrently serving as the Vice President for Domestic Consulting Group (DCG) of PKII.

2. Assistant to the Data Protection Officer (Asst. DPO)

   The designated Asst. DPO is **Mr. Brian Jose Fuertes**, who is concurrently serving as the IT Manager of PKII.

3. Personal Information Controller (PIC), or Personal Information Processor (PIP)

   The designated PIC or PIP is **Ms. Mary Ann Castañares**, who is currently assigned to the Human Resources Department (HRD) as HR Supervisor.

4. Assistant to the Personal Information Controller (Asst. PIC)

   The designated Asst. PIC shall be any IT staff from the IT Department.

5. Functions of the DPO, COP and/or any other responsible personnel with similar functions

   The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

6. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security

   PKII shall sponsor a mandatory training on data privacy and security at least once a year for personnel directly involved in the processing of personal data.

   The Human Resources Department (HRD) shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

7. Conduct of Privacy Impact Assessment (PIA)

   PKII shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct of a PIA to a third party.

   In the absence of a third party to conduct the PIA, the DPO/COP shall create a team to conduct the Privacy Impact Assessment internally, to be assisted by the IT Department.

8. Duty of Confidentiality

   All PKII personnel including its employees and consultants have signed a Non-Disclosure Agreement (NDA) during their employment.

   All PKII personnel with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

9. Review of Privacy Manual

   This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

B. **Physical Security Measures**

1. Format of data to be collected

Personal data in the custody of PKII may be in digital/electronic format and paper-based/physical format.

2. Storage type and location

   All personal data being processed by the organization shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computer servers in PKII's Main Office - IT Room.

3. Access procedure of agency personnel

   Only authorized PKII personnel shall be allowed inside the data room.

   Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

4. Monitoring and limitation of access to room or facility

   All personnel authorized to enter and access the data room or facility must log and fill out the logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.

5. Design of office space/work station

   The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

6. Persons involved in processing, and their duties and responsibilities

   Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.

7. Modes of transfer of personal data within the organization, or to third parties

   Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments.

   Facsimile (Fax) technology shall not be used for transmitting documents containing personal data.

8. Retention and disposal procedure

   The organization shall retain the personal data for at least ten (10) years from the date of entry. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

C. **Technical Security Measures**

1. Monitoring for security breaches

   PKII shall use a Data Leak/Loss Prevention (DLP) solution to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

2. Security features of the software/s and application/s used

   PKII shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

3. Process for regularly testing, assessment and evaluation of effectiveness of security measures

   PKII shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the appropriate department or unit.

4. Encryption, authentication process, and other technical security measures that control and limit access to personal data

   Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and if possible, a multi-level authentication.

   PKII has its own intranet system where personnel can check his/her personal data encoded by the PIC/PIP or its authorized personnel.

Breach and Security Incidents

1. Creation of a Data Breach Response Team

   A Data Breach Response Team comprising of at least three (3) to five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. Measures to prevent and minimize occurrence of breach and security incidents

   PKII shall regularly conduct a Privacy Impact Assessment (PIA) to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and

seminars for capacity building. A periodic review of policies and procedures being implemented shall be conducted within the organization.

3. Procedure for recovery and restoration of personal data

   PKII shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

   PKII also provide an offsite (cloud) backup server as its disaster recovery and business continuity planning preparations. Weekly incremental backups of all datafiles are copied to the offsite backup server.

4. Notification protocol

   The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. PKII Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

5. Documentation and reporting procedure of security incidents or a personal data breach

   The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

Inquiries and Complaints

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the PKII organization, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization at **hrd@philkoei.com.ph** and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be sent to **mails@philkoei.com.ph**. The concerned department or unit shall confirm with the complainant its receipt of the complaint.

Effectivity

The provisions of this Data Privacy Manual or Information Security Regulations are effective this 1st day of August, 2021, until revoked or amended by Philkoei International Inc. (PKII), through a Board Resolution.

Annexes

1. Consent Clause
2. E-mail Disclaimer

Annex 1

The clause below shall be included to any PKII personal data form before the signature input field.

> "All personal data acquired by Philkoei International Inc. (PKII) shall only be used for the purposes of this document and shall not be disclosed to any third-party without the consent of the data subject."

Annex 2

The clause below shall be used by PKII personnel when sending personal or sensitive data through e-mail.

> "CONFIDENTIALITY NOTICE
>
> The information contained in this e-mail, including those in its attachments, may contain personal and sensitive personal information, and will be subject to the Data Privacy Act of 2012, its implementing rules, regulations and issuances of the National Privacy Commission of the Philippines ("Privacy Laws"). By viewing, using, storing, sharing and disposing (collectively "Processing") this Email, you agree to comply with the Privacy Laws. If you are not an intended recipient, you must not read, copy, store, disclose, distribute this message, or act in reliance upon the information contained in it. If you received this e-mail in error, please contact the sender and delete the material from any computer."

Data Loss/Leak Prevention (DLP)

Policy and Guidelines

V1.00

PHILKOEI INTERNATIONAL, INC.
CONSULTANTS • PLANNERS • ENGINEERS

Revision history

Version No.	Date	Details	Author
1.00	2021-Jul-01	1st release	BRFuertes/JACBeringuela

Table of Contents

Purpose

Philkoei International Inc. (PKII) must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting its operations. The protection of in-scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical. This policy supports a range of general regulations by restricting access to data hosted in PKII's servers located in PKII's Central Office.

PKII is bound to protect certain information that is transmitted using the office's IT systems, hardware, and networks. Pursuant to these objectives, PKII has the duty to actively prevent the loss of Protected Information. It is the policy of PKII to engage in sustained and substantial efforts to provide for the confidentiality and integrity of Protected Information; to promptly discover and remedy any Security Breach or misuse of Information Technology Resources; and to expeditiously take those measures needed to reduce the probability of a Security Breach or a misuse of Information Technology Resources. This Policy is intended to further and not replace, in whole or in part, approved Office Policies dealing with the collection, storage, maintenance, transmission and use of Data.

Definitions

"Data" - means electronic information whether stored digitally or in text, voice, code

or visual representation or in any other electronic medium.

"Data-At- Rest" - means stored or archived Data and includes, but is not limited to, Data stored on Information Technology Resources.

"Data-In-Motion" - means Data that is traversing the PKII Network or otherwise being transferred electronically and includes, but is not limited to, email, instant messages, ftp, and web traffic utilizing Information Technology Resources.

"Data-in-Use" - means Data that is being manipulated by a user, and includes, but is not limited to, transferring Data to a USB drive or copying, altering and/or pasting Data.

"DLP" - means Data Loss Prevention or Data Leak Prevention.

"Information Technology Resources" – PKII's IT system and network including its computers and components, electronic storage devices, wiring, and electronic transmission devices owned and operated by PKII, and all licensed softwares.

"Protected Information" - Protected Information is a single term that includes all of the following: Confidential Information, Departmental Records, Personal Information, and Proprietary Data of PKII, including all of its Project-related Data.

"Security Breach" - the unauthorized disclosure of Protected Information. PKII Management will classify such Breaches that will, in turn, specify the types of responses appropriate to the level of severity of the breach.

Data States and Implementation

All Data under PKII's Information Technology Resources whether At-Rest, In-Motion and In-Use shall be monitored by the use of hardware-based and software-based DLP solution.

1. A DLP software solution will be configured at the endpoints to identify data in motion to Browsers, IM Clients, E-mail clients and Mass storage devices.
2. A DLP hardware solution will be installed in the PKII Main Office - IT Room, connected to the Local Area Network (LAN) in order to monitor all Data states including PKII's system and file servers, and as well as its network.
3. All Data owners of each Department shall work closely with the IT Department to identify, assign and mark the Data to be included on the DLP solution scanning.
4. The DLP solution will scan for data in motion. DLP will identify specific content, i.e.:
    a) E-mail addresses, names, addresses and other combinations of personally identifiable information
    b) Documents that have been explicitly marked with the 'PKII Confidential' or 'PKII Use Only' string.
5. The DLP will be configured to alert in the event of a suspected transmission of sensitive data, and such data will be presented with a choice to authorize or reject the transfer. This allows the Data owner to make a sensible decision to protect the data, without interrupting business functions. Changes to the DLP product configuration will be handled through PKII's Information Technology Department's (ITD) change process and with the management approval, to identify requirements to adjust the information security policy.
6. The DLP will log incidents centrally for review. The IT Department, together with the Department involved, will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and if there is a concern of inappropriate use. These events will be escalated to the HR Department to be handled through the normal process and to protect the individual. A copy of such incident shall be provided to the PKII Management.
7. Where there is an active concern of data breach, the office's incident management process is to be used with specific notification provided to appropriate authority.
8. Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally, or

accidentally lost data but provides sufficient basis for investigation to ensure data has been appropriately protected.

Security Review

1. Scope

Based upon the determination made by the PKII Management in accordance with the provisions

of Section 2, PKII may:

a) access and examine PKII's office Computers (I.e., desktop PC, laptop, tablets and smartphones) and other Information Technology Resources and all Data (I.e., Data-In-Motion, Data-At-Rest, or Data-In-Use) utilizing Information Technology Resources in any manner whatsoever;

b) monitor the PKII Network activities of individual computer users of Information Technology Resources;

c) conduct a forensic analysis of Information Technology Resources, and the use and usage of such Resources.

2. Determination

PKII Management may exercise the rights to take one or more of the actions described in Section 1 if it deemed reasonably determines that such action is necessary or appropriate to –

a) protect the integrity or security of Protected Information or Information Technology Resources;

b) protect PKII from incurring liability;

c) reduce the risk of the deliberate or unwitting disclosure of Protected Information or security features of PKII's Network that are not publicly known;

d) investigate unusual or excessive activity typically associated with illegal activity or activity that may be in violation of acceptable use of PKII's Information Technology Resources or data;

e) investigate credible allegations of illegal activity or violations of PKII's policy; or

f) comply with law or compulsory legal process (such as a lawfully issued subpoena).

Probable Violations

In the event that a probable violation of a policy has been identified through the misuse of an Information Technology Resource, the incident shall be recorded in secure Information Security records system and a notification and description of the incident shall be sent to the PKII Management for further review and analysis.

If the PKII Management concurs that a probable violation has occurred or is likely to occur, it will then determine what disciplinary action will be given or shall refer to the existing IT Policy with its list of violations and corresponding disciplinary action, except that in all cases of suspected criminal activity PKII's Legal Representative shall be promptly notified and in all cases when a Security Breach is suspected.

Confidentiality and Privacy

All PKII personnel have signed a confidentiality agreement or Non-disclosure Agreement (NDA) during their employment. Any PKII personnel who haven't signed such confidentiality agreement shall coordinate with the Human Resources Department (HRD).

Any PKII personnel who use the Information Technology Resources for Data Storage, Data Transmission or Data Dissemination, or for the Processing of Data should not expect that:

- Such Data is Private and only accessible by them; or
- That such Data is exempt from retrieval, monitoring or analysis under this policy; and
- PKII may take actions authorized under this policy with or without prior notice.

Policy Compliance and Maintenance

PKII personnel are expected to cooperate with the IT Department with respect to the implementation of this Data Loss/Leak Prevention Policy and Guidelines. Any PKII personnel who knowingly attempts to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by PKII for the purpose of implementing this Policy shall be subject to appropriate disciplinary and remedial actions, up to and including termination of employment, and/or legal action.