INFORMATION TECHNOLOGY POLICY

Approved by the Management Team
2018 November 23

PHILKOEI INTERNATIONAL, INC.
CONSULTANTS • PLANNERS • ENGINEERS

TABLE OF CONTENTS

TABLE OF CONTENTS.....i
1 Intent..... 1
2 Purpose.....1
3 The Policy.....1
3.1 Network Architecture..... 2
3.2 The Servers.....3
3.2.1 Shared folders on each department.....4
3.2.2 Data redundancy and backup.....5
3.3 PKII Intranet..... 6
3.3.1 IT Support Request..... 7
3.3.2 Users' Activity Log.....9
3.4 IT EQUIPMENT and Software use..... 9
3.5 Internet access use..... 11
3.5.1 The world-wide-web..... 11
3.6 Email Etiquette.....13
3.7 SECURITY AWARENESS.....15
3.7.1 Incident Management..... 15
3.7.2 Door Access..... 16
3.7.3 Computer Encryption..... 16
3.8 IT Violations with corresponding disciplinary action.....16
3.8.1 Oral Warning.....16
3.8.2 Written Warning..... 17
3.8.3 Suspension.....17
3.8.4 Dismissal..... 17

List of Figures

Figure 3. 1 Current Network Diagram of Philkoei International Inc.....3

Figure 3.2 Example of shared folders.....4

Figure 3.3 Screenshot of user's folder.....5

Figure 3.4 Servers' Data Backup and Redundancy Program.....6

Figure 3.5 Intranet Home Page.....7

Figure 3.6 IT Support Request Module.....8

List of Tables

Table No. 1 - Category A Offenses.....17

Table No. 2 - Category B Offenses.....18

Revision History

Date	Version	Details	Author
2008-Dec-15	V1.00	First released version	IT-brfuertes
2012-Dec-03	V2.00	2nd release – additional 3rd office (Design Center) and updates to the networking equipments and virtual firewall using Open DNS	IT-brfuertes
2016-May	V3.00	3rd release – new office location in Orient Square Bldg, Ortigas and updates to the networking diagrams	IT-brfuertes
2018-Oct	V4.00	4th release – new web-based system called Intranet as a paperless system for office transactions; IT Violations with corresponding disciplinary action; Door access and computer encryption and incident management	IT-msgutierrez

INFORMATION TECHNOLOGY POLICY

1 INTENT

The intent of this policy is to establish guidelines for all employees of "Philkoei International, Inc." (or here in after referred as the "Company"), using the Company's computing facilities including computer software, hardware, printers, internet, e-mail and intranet (if any) access, collectively called "Information Technology" or "IT".

2 PURPOSE

All employees share and use the Information Technology facilities at Philkoei International Inc. located at Unit 1701 Orient Square Bldg., F. Ortigas Jr. Ave. (formerly Emerald Ave.), Ortigas Center, Pasig City, Metro Manila, Philippines.

These facilities are provided to employees for the purpose of conducting the Company's business and operations.

All employees are expected to exercise responsible and ethical behavior when using the Company's Information Technology facilities.

Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

3 THE POLICY

The use of the Company's information technology facilities in connection with company business and limited personal use is a privilege but not a right, extended to various company employees. Users of Philkoei International Inc.'s computing facilities are required to comply with all policies referred to in this document.

The management of Philkoei International Inc. reserves the right to amend these policies and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable laws.

To protect the integrity of the Company's computing facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation of Company rules and regulations, the management of Philkoei International Inc. reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of Company rules or policies.

The management through its IT department also reserves the right periodically to examine any system, data, internet access, e-mail communications and other usage and authorization history as necessary to protect its computing facilities.

The Company disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

This policy covers seven (7) parts namely:

- ✓ Network Architecture
- ✓ Servers
- ✓ Intranet
- ✓ Computer and Software Use
- ✓ Internet Access Use
- ✓ Email
- ✓ List of Violations and Disciplinary Actions

3.1 NETWORK ARCHITECTURE

All computers are connected to the internal network or local-area-network (LAN) via cascading network switches with speeds of 10/100/1000mbps.

Network routers with WiFi features are in place in the whole office. The routers act as the network-address-translator (NAT), firewall, WiFi access points and port forwarder from the LAN to the public IP/WAN.

Internet access policy is controlled by the routers using Net Gear’s Live Parental Control thru open DNS (Domain Name System).

The PKII LAN uses the Transmission Control Protocol over Internet Protocol (TCP/IP) and the Windows Networking Protocol.

All computer desktop workstations connected to the LAN are currently on static-IP mode and most laptops and smart phones use the DHCP (Dynamic Host Control Protocol) connection for automatic IP address assignment from the server's domain controller.

Printers may be accessed by different computers thru the network with their designated IP addresses. Other printers use the printer-sharing configuration by physical connection to some workstations.

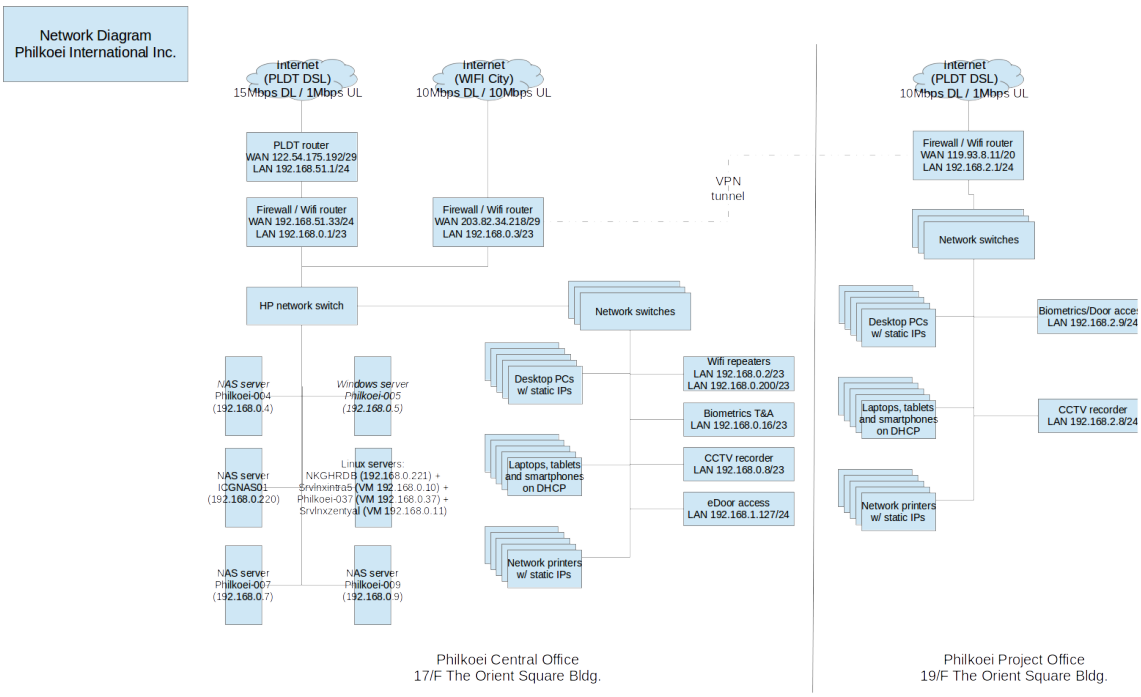


Figure 3. 1 Current Network Diagram of Philkoei International Inc.

3.2 THE SERVERS

- The company is equipped with several servers as follows:
- Departmental File Server for BDD/Admin/HR/IT/Management (Philkoei-004)
- Departmental File Server for MRT 7 (Philkoei-006)
- Departmental File Server for Engineering/Design Center (Philkoei-007 – Read only)
- Departmental File Server for Engineering/Design Center (Philkoei-009 – Read and Write Access)
- Departmental File Server for Finance/Accounting (Philkoei-037)
- Departmental File Server for ICG (ICG-NAS01)
- Backup server and VM host (NKHRDB1)
- Intranet Server (192.168.0.10)
- Active Directory Domain Controller, DNS and DHCP server using Zentyal (192.168.0.11)

It is mandatory for all employees to save all their data files to their respective folders on the designated servers.

Any data files or folders saved on the local computer workstations shall have no guarantee of any backup and/or data retrieval in case of a software or hardware failure. It is mandatory to save all data files to the file server.

Any data files or folders that were accidentally deleted in the file server may be retrieved considering the user must report first to their respective manager and to the IT Department within one (1) week from the date of deletion. Please note that accidental deletion of files has no guaranty of successful retrieval.

3.2.1 SHARED FOLDERS ON EACH DEPARTMENT

Since servers have confidential data/files per department, access should be requested thru intranet that will be approved by the immediate supervisor/manager. Please consult with your IT representative to allow user permissions and restrictions on the available shared folders.

A representative in every department may be assigned to handle the files and folders for file management in organizing the files within their respective shared folders on the file servers.

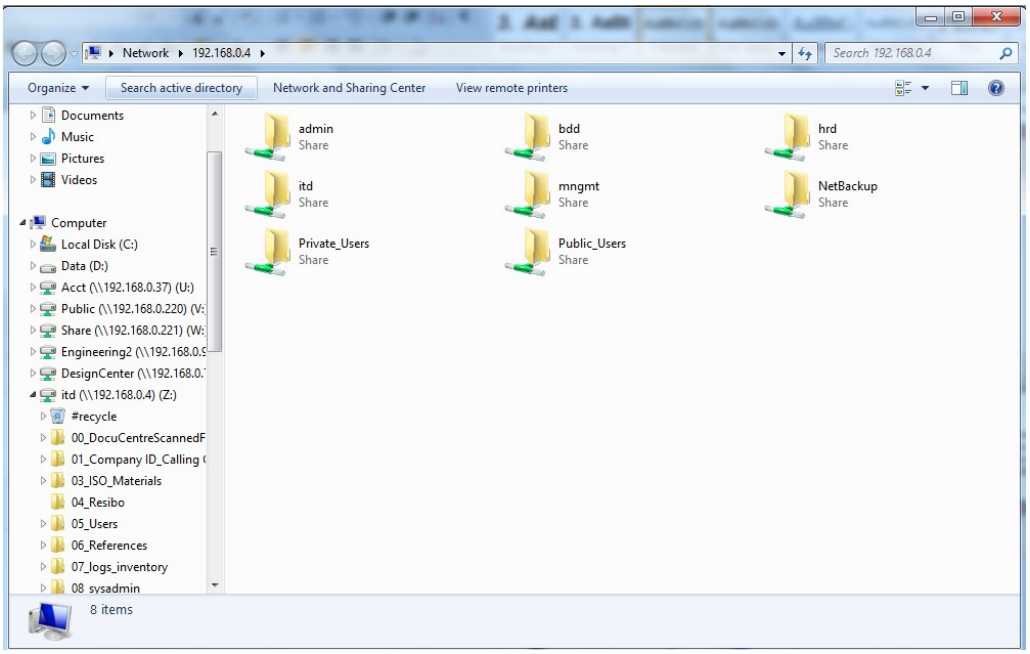


Figure 3.2 Example of shared folders

A 'users' folder in \\philkoei-004\Public_Users is available to all users with different folders on each usernames, with their respective access permissions. All users are advised to save regularly their office-related files from their desktops or laptops to their assigned folders in order to have a copy of their files for data recovery, just in case one's hard drive fails.

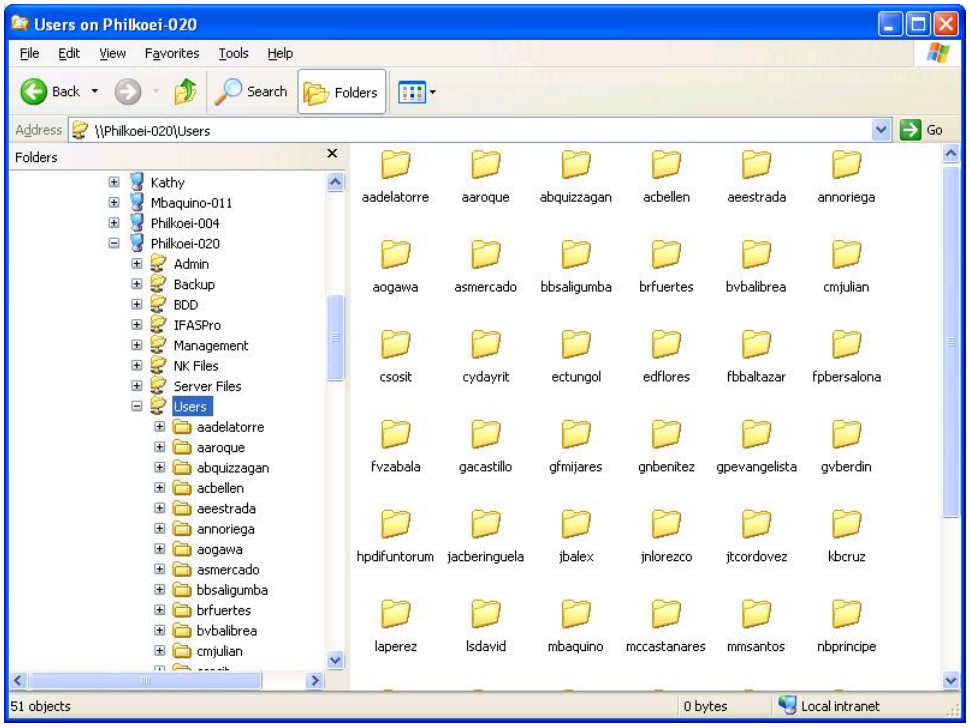


Figure 3.3 Screenshot of user's folder

3.2.2 DATA REDUNDANCY AND BACKUP

Currently, the office use the configured hard disk mirroring (RAID-1) and block-level striping with distributed parity (RAID-5) on its file servers for data redundancy.

A backup of all the file servers are manually done by the IT Department, by using two (2) sets of external hard drives. These two (2) sets of external hard drives are placed off-site, and to be brought in the office for updating the backups. These off-site backups shall also be used for Disaster Recovery (DR) and/or Business Continuity planning.

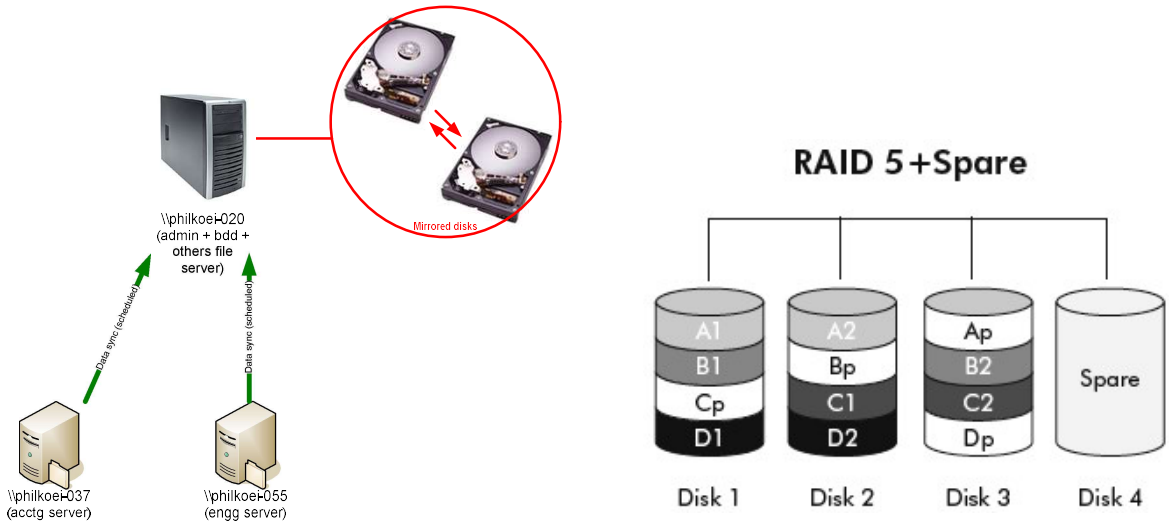


Figure 3.4 Servers' Data Backup and Redundancy Program

3.3 PKII INTRANET

The PKII Intranet System is a web-based application that runs on a Linux server with a Relational Database Management System (RDBMS). It is an Enterprise Resource Planning (ERP) system used by the different departments of Philkoei International Inc. as their back-office system. Intranet is developed for automated processes. This cloud-based system is used for sorting of data/information in a digital format. The main purpose of intranet is to share company information and computing resources among employees. Intranet is divided into two (2) main functions; one is for individual/personal access of employee (non-admin page). The non-admin page serves as the employees' main access to office and his/her personal information. The other one is the admin page. The admin page is the primary system used in office transactions. Several modules were developed to be used by the different departments of the organization. The admin page is also limited to those personnel who need access to automated processes of the company. This is a digital form to eliminate or greatly reduce the use of paper. In addition, all information is stored in a database for security purposes.

Moreover, the IT Department includes e-mail as a mode of communication in submitting request especially those requests needed by the management and needed urgent attention.

Features and Modules:

- Directory of projects
- Directory of personnel
- Directory of businesses and contact persons
- Accounting/finance's voucher system

- Accounting/finance's custom payroll system
- Accounting/finance's employees' payslip email notifier
- Accounting/finance's special pay notifier
- Accounting/finance reports
- HR's time and attendance
- HR's office time logs
- HR's project deployment
- HR's list of expiring contracts
- HR reports
- Documents archiving
- User's activity log
- Separate login portal for non-admin
- Separate login portal for administrative users
- View logs
- User management and access control
- Categories management
- Modules management

3.3.1 IT Support Request

The IT Support Request is one of the modules of the Intranet with support ticketing system wherein users may request for technical support to the IT Department. Once a user has submitted a request, his/her Superior/Manager shall approve the said request and a support ticket will be created by the IT Support Group from the IT Department. The module has a chat-style feature for clarifications and further communications between the requestor, the approver and the IT Support Group.

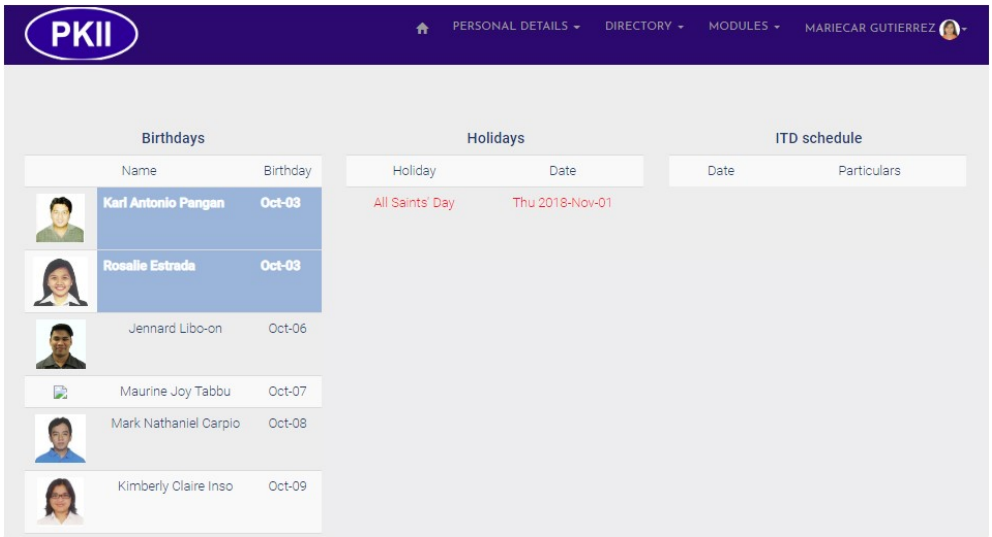


Figure 3.5 Intranet Home Page

The figure above shows the home page of individual employee in accessing the Intranet. Non-admin page is composed of 3 modules which include personal details for personal information, time log, activity log and pay slip summary of each employee. Directory module includes company information and important documents that each employee needs to know about the company. In addition, the modules tab includes different kind of request for inventory, IT and HR.

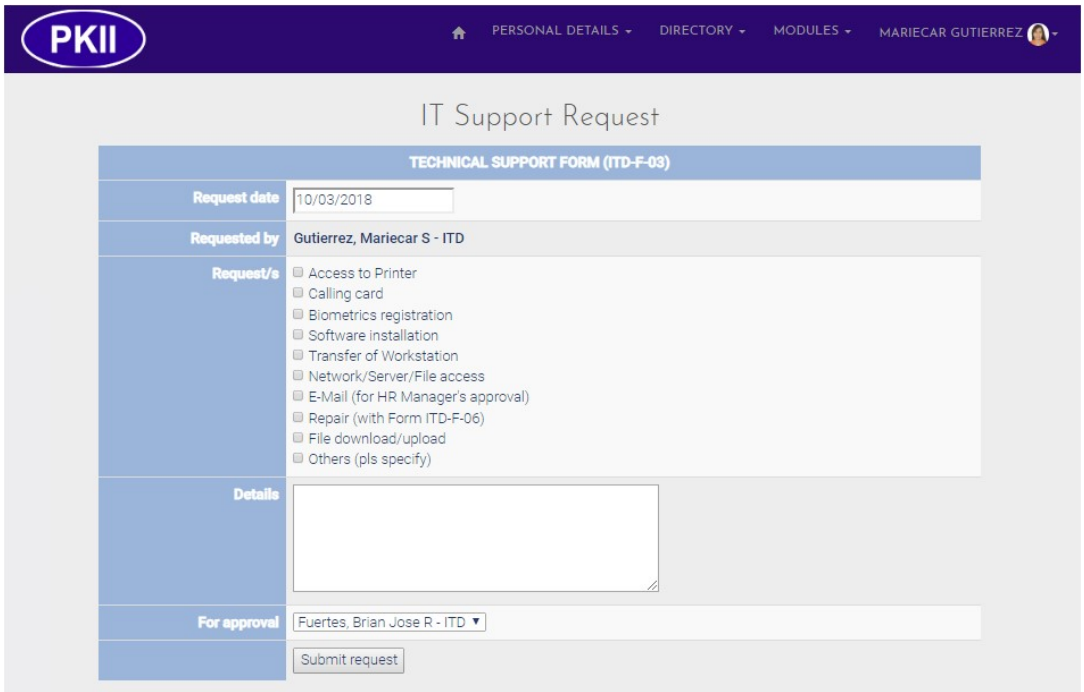
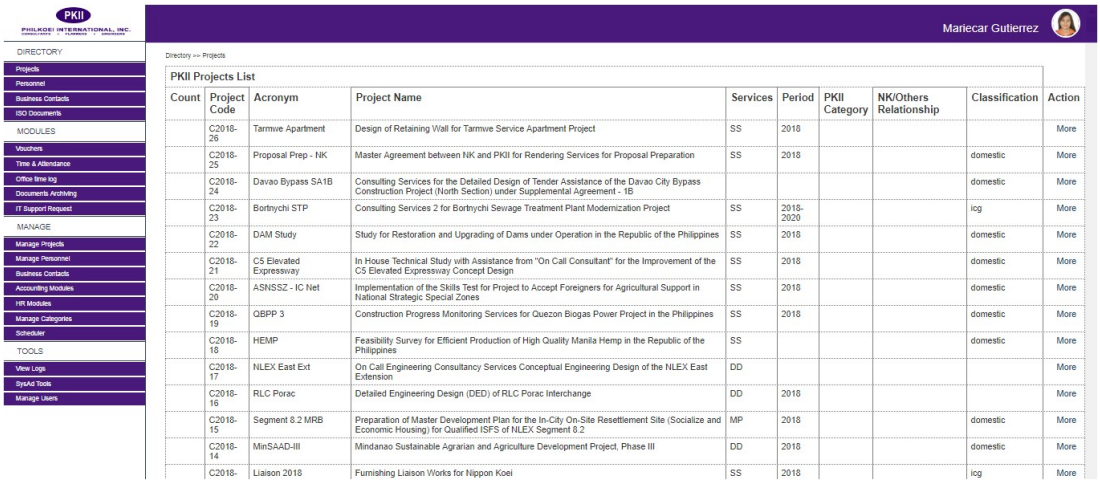


Figure 3.6 IT Support Request Module

Figure 3.6 shows the kind of request that can be done by the IT Department, which needs to be approved by the immediate supervisor/manager before ITD take necessary actions.



Count	Project Code	Acronym	Project Name	Services	Period	PKII Category	NK/Others Relationship	Classification	Action
	C2018-26	Tarmwe Apartment	Design of Retaining Wall for Tarmwe Service Apartment Project	SS	2018				More
	C2018-25	Proposal Prep - NK	Master Agreement between NK and PKII for Rendering Services for Proposal Preparation	SS	2018			domestic	More
	C2018-24	Davao Bypass SA1B	Consulting Services for the Detailed Design of Tender Assistance of the Davao City Bypass Construction Project (North Section) under Supplemental Agreement - 1B					domestic	More
	C2018-23	Bortnychi STP	Consulting Services 2 for Bortnychi Sewage Treatment Plant Modernization Project	SS	2018-2020			icg	More
	C2018-22	DAM Study	Study for Restoration and Upgrading of Dams under Operation in the Republic of the Philippines	SS	2018			domestic	More
	C2018-21	C5 Elevated Expressway	In House Technical Study with Assistance from "On Call Consultant" for the Improvement of the C5 Elevated Expressway Concept Design	SS	2018			domestic	More
	C2018-20	ASNSSZ - IC Net	Implementation of the Skills Test for Project to Accept Foreigners for Agricultural Support in National Strategic Special Zones	SS	2018			domestic	More
	C2018-19	QBPP 3	Construction Progress Monitoring Services for Quezon Biogas Power Project in the Philippines	SS	2018			domestic	More
	C2018-18	HEMP	Feasibility Survey for Efficient Production of High Quality Manila Hemp in the Republic of the Philippines	SS				domestic	More
	C2018-17	NLEX East Ext	On Call Engineering Consultancy Services Conceptual Engineering Design of the NLEX East Extension	DD					More
	C2018-16	RLC Porac	Detailed Engineering Design (DED) of RLC Porac Interchange	DD	2018				More
	C2018-15	Segment 8.2 MRB	Preparation of Master Development Plan for the In-City On-Site Resettlement Site (Socialize and Economic Housing) for Qualified ISFS of NLEX Segment 8.2	MP	2018			domestic	More
	C2018-14	MinSAAD-III	Mindanao Sustainable Agrarian and Agriculture Development Project, Phase III	DD	2018			domestic	More
	C2018-	Liaison 2018	Furnishing Liaison Works for Nippon Koei	SS	2018			icg	More

Figure 3.7 Admin Home Page

Figure 3.7 displays the admin page with different modules that are used in day to day transaction per department to eliminate the cost of shredding services for paperwork with sensitive information.

3.3.2 USERS' ACTIVITY LOG

The Users' Activity Log is a module to provide documentations to their daily activities. It also shows their time and attendance logs from the biometrics device. It can be viewed either monthly or bi-monthly. It is recommended that each user shall regularly use and fill-up their Activity Log.

3.4 IT EQUIPMENT AND SOFTWARE USE

- All employees with network access have their individual logins on their respective or assigned computers.
- Passwords should be changed (at least) every six months for security purposes.
- All computer workstations may be configured to assign several shared network folders from the file servers for easy access to their data files. These assigned and shared network folders shall be used in saving all the data files.
- It is not recommended to save any data files to your desktop or local hard drives unless temporary only because the present network setup cannot automatically backup any data files from a local hard drive of a computer unit. Users must back up their work files on a regular basis.

- Productivity software (such as spreadsheets, document editor and reader, presentation and other productivity tools), anti-virus, internet browser and e-mail clients are installed and configured on each computer.
- Anti-virus software is installed on each computer. Virus definition files are updated automatically when one's computer is connected to the internet or local-area-network. The IT Department shall check randomly and any time if such computer has the current update.
- The IT Department will assist employees in installing anti-virus software according to standards on personally owned computers that will be used for business purposes. The IT Department will not provide anti-virus software in these cases.
- Administrator login is prohibited to any employee unless allowed and approved by the management and the IT Department.
- Please notify the assigned IT staff or the management if a security problem is found on his/her computer workstation. Ex.: viruses, worms, Trojans, spywares, network attacks, etc. Such workstation should be disconnected to the network immediately.
- All employees are advised not to install any software or programs by themselves. All software installations must be handled by the IT Department and may be pre-approved by the management prior to installation.
- Pirated software or unlicensed software is prohibited on any computers inside the office premises. Any computer found to have pirated software installed will be removed/uninstalled by the IT department.
- Software games whether online or offline are prohibited. All (pre)-installed games found on the company's computer workstations may be uninstalled or deleted anytime by the management.
- Playing of media files (such as mp3/wma audios and videos) are also discouraged and may not be allowed especially if it hampers or disturbs the Company's office operations. It may only be allowed, upon management's approval, if it is work-related.
- All sites and downloads may be monitored and/or blocked by the company if they are deemed to be harmful and/or not productive to business
- Always log-off when you leave the computer. Or use desktop locking like screen saver with password.
- Individual employee is responsible to their respective workstation. Please make sure to turn-off assigned computers individually after working hours.
- Please do not install file-sharing programs like limewire, kazaa, etc. on the Company's computers. The (pre)configured shared folder of your hard

drive from these programs and the files within can be accessible from anyone on the internet.

- Please do not remove any installed software in individual computers assigned in each employee. If such application is not required, please call the attention of any IT Personnel.
- Borrowing of laptops or any IT equipments to be used outside office premises should be requested at least 2 days before the date needed for the availability of IT equipments and must be approved by the manager/supervisor thru Intranet. In addition, requestor should sign a memorandum receipt prepared by the Administrative Department for the monitoring of outgoing/ incoming office equipments.
- Bringing of personal computers, devices (BYOD) is strictly prohibited unless approved by the management.
- The IT Department reserves the right to audit any laptop/ devices whether it is personal or company owned used for business to ensure that it continues to conform to policy. The IT Department will also deny network access to any laptop/devices, which has not been properly configured and certified.
- Devices connected to the company network will be reviewed on a regular basis for the latest operating system and application security patches applicable to that device as well as the latest anti-virus software. Devices not compliant with IT Security Office standards may be disconnected from the network.
- If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not "trained" in how to fix the problem, please do not try. Instead, report the problem to IT or ask a trained co-worker for help. Report any malfunction of any printing device to the IT Department as soon as possible.
- Suspected problems with computers, networks and any IT equipment should be reported to the IT Department.
- Misuse of computer devices and/or any IT equipments and network resources will be given appropriate disciplinary action. (See Section 7. IT Violations with corresponding disciplinary actions)

3.5 INTERNET ACCESS USE

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers.

3.5.1 THE WORLD-WIDE-WEB

- Employees of the company have the privilege to have access to different information, news and e-mails.
- The Company has its own web presence in the internet: www.philkoei.com.ph
- It is encouraged to use the internet for office-related purposes in order to increase productivity, improve one's technical knowledge and be updated on the current situations. It is the responsibility of each employee to use this resource responsibly and respectfully. All of these resources can be accessed by using an internet browser like Mozilla Firefox, Google Chrome, etc.
- Internet access may be available anytime with scheduled site restrictions.
- The management anytime may monitor internet access activities.
- Instant messengers such as Viber, Skype, Yahoo Messenger, MSN Messenger, Chikka, etc. are restricted on the company's computers unless such use are approved and allowed by the management on a case-to-case basis and should only be for official business transactions with the company.
- The use of network-file-sharing and peer-to-peer (P2P) programs like bittorrent, utorrent, etc. are not allowed. These programs can and may bypass the firewall settings and makes the entire network vulnerable from attacks and may slow the internet bandwidth.
- Please be careful in entering or providing sensitive information whether personal or business. You might be a victim of a phishing scam. Example is when someone is trying to send an email asking for a verification of your credit card, username and password, personal information, etc. Please check and verify first if the sender or the website is legitimate.
- Viewing and access to social networking sites such as facebook, twitter, instagram, hi5, MySpace, tagged, etc. are not allowed or will only be allowed on a limited time and should never be accessed especially during office hours.
- Viewing and watching of online video sites such as YouTube and other online streaming sites are not allowed due to the large bandwidth it consumes. It may slow down the internet performance within the office's network.
- Adult-related or porn sites, underground, abusive and hate sites are also prohibited inside the Company's computer network premises. These sites normally provide viruses, network attacks, etc. and may infect one's computer system anytime.
- Access to these prohibited resources may be controlled and barred anytime upon management's discretion.
- All Internet data that is composed, transmitted and/or received by PKII's computer systems is considered to belong to company and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties. (See Section 5. Security and Best Practices)

- Do not be abusive in communications to others.
- Do not swear or use vulgarities or any other inappropriate language.
- Do not reveal personal addresses, phone numbers, Social Security numbers, or other identifying personal information.
- Do not use the network in such a way that would disrupt the use of the network by other users.

3.6 EMAIL ETIQUETTE

Regularly check your inbox

- Employees will have their own official e-mail address (Ex. email@philkoei.com.ph) as primary means of communication.
- Personal use of e-mails like yahoo mail, hotmail, Gmail, etc. will only be allowed on a limited time and never a priority over work matters.
- Currently, the e-mail server is using POP3 for incoming mail server in which there is a limited amount of storage quota per user. It is advisable to regularly check and download or save their e-mails with attachment/s in order to free-up space on the server. If a user needed additional storage space, he/she shall access the IT Support Request module in the PKII Intranet, fill-up the form, and ask for approval to his/her superiors so the technical support personnel can temporarily adjust the disk storage quota.
- Official e-mails is accessible using an e-mail client such as Microsoft Outlook or Mozilla Thunderbird on their assigned computers. It can also be accessed thru a web browser by logging in to: https://www.philkoei.com.ph:2096/
- Employees are advised to change their password every month for security purposes. E-mail password may be changed anytime by accessing the web-based e-mail https://www.philkoei.com.ph:2096/ login with you complete e-mail address and your current password. Once logged-in, an icon link to change password is now visible together with the other icons to select an online e-mail client interface.
- Proper e-mail etiquette dictates that you respond to all e-mail in a timely fashion. Generally, you should respond to all professional or official e-mail within a business day, even if it has just to say you have received the message and will look into the matter.
- E-mail clients such as Outlook or Thunderbird can be set to automatically retrieve messages every hour or shorter periods.
- Avoid phishing attacks, virus outbreaks and spam
- Phishing frauds are to steal personal information. They often use doctored and fraudulent e-mail messages to trick recipients into divulging private information, such as credit card numbers, account usernames and passwords.

- Phishing messages often boast real logos and appear to have come from the actual organization, but those messages are designed to capture your personal information.
- If you suspect a message possesses any credibility, you are much safer calling the company directly—preferably at a telephone number printed on a paper statement or invoice—and talking to an authorized representative.
- Avoid opening e-mail file attachment if you do not know the sender.
- If you are sure that an e-mail attachment came from a known sender, please save first the file attachment and scan for viruses before opening.
- Do not open unsolicited e-mail, most of these are spam.
- Never click a hyperlink from an e-mail message if you suspect the e-mail is a spam.

Manage your inbox

- On your e-mail client such as Outlook or Thunderbird, you can sort messages by priority, subject, date, sender and other options to help find important e-mail that you need.
- You can also create sub-folders for categories such as senders, projects or archived by months or years.

Secure and compress file attachment

- Please compress file attachment(s) especially if such file(s) reach more than 1 megabyte.
- Please also provide security to the file(s) by assigning a password during file compression.
- A compression utility tool such as Winzip, Winrar, 7-zip or IZArc is installed on your assigned workstation.

Utilize cloud servers for large file attachment

- Please ask assistance from the IT Support Group if you wish to send large sized file attachment, so they can assist and guide you in uploading to a cloud server and provide you the hyperlink for download.

E-mail best practices guidelines

Signatures and disclaimers may be added to the end of all emails as they may be forwarded to external parties.

- Use discretion when:
- Forwarding or copying emails to one or more recipients.
- Including the original content when replying to a message

- Seeking automatic confirmation of the reading of a message by the addressees
- Sending electronic messages if a telephone call would be a more appropriate alternative
- Use the subject field appropriately. If there is a deadline for an action or response, include it after the subject.
- Remember to treat email communication like any other business document. Speak in the third person and do not include subjective or personal comments.
- Be sparing in use of the red exclamation mark and only use this for genuinely URGENT communications. When you write in all **capital letters**, most recipients assume you are shouting at them.
- Provide clear instructions about dissemination of email content and any relevant consideration such as privacy.
- Indicate confidentiality required in the email (e.g., „this matter should remain confidential among Managers until such time as ...").
- If the email needs to be sent to multiple recipient, the extent of distribution should be indicated (e.g., „Please distribute this information to all project members.").
- Be cautious about using Bcc (Blind copies) that may be considered as breach of confidentiality to send an email to a third party of whom the other recipients are not aware.
- Use "Out of Office" auto-reply to alert those contacting you via email of your availability, expected return date or best person to contact in your absence. An auto-responder tool is available when you use the webmail login (using a web browser). Webmail link: https://www.philkoei.com.ph:2096

3.7 SECURITY AWARENESS

3.7.1 INCIDENT MANAGEMENT

As PKII prioritized the security, CCTV cameras are configured inside PKII premises. This is to monitor and protect all the property owned by the company. Information obtained via CCTV monitoring will be used exclusively for security and law enforcement purposes. Information obtained by CCTV monitoring will only be released when authorized by both the manager and Safety department. Department of Information Technology is authorized to oversee and coordinate the use of CCTV monitoring equipment while Safety and Security has the primary responsibility for disseminating and implementing policy and procedures.

As part of the security, IT department encourage everyone to use IT Support Request thru Intranet to submit a request for CCTV footage review indicating the reason and time of the incident which must be approved by the manager/supervisor. An Incident Report Form will be fill-out by the person involved to be kept by the Safety

Department. Please take note that recording of CCTV is first in, first out basis with 6 weeks retention. In addition, ITD is not responsible in investigating a particular incident.

If a computer fails via an accident, lost or stolen involved personnel should report it immediately to the IT Department provided that a personnel has fill-out an incident report to be filed by the Safety Department. The IT Department is responsible for repairing of all company equipment.

IT Department takes action to provide reasonable protection against environmental threats such as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power for central server and network facilities. IT Department maintains procedures for protecting critical data that reside on servers. While the company provides security for files stored on servers, IT Department is not responsible for protection against floods, fires, and catastrophic events. IT Department does not guarantee the availability of backups for the restoration of files deleted through user error.

3.7.2 DOOR ACCESS

Door access is part of the security. Biometric is installed so that only authorized employees can enter the office premises. IT department makes sure that each employee has door access according to their scheduled time. Please take note that door access is available until 8:30 PM. IT department encourage every employee who will work beyond mentioned time should submit an overtime request thru Intranet. This is to make sure that only authorized employees of their manager/supervisor is inside the office premises.

3.7.3 COMPUTER ENCRYPTION

Encryption software is used for data/files protection. This software will turn the files of each computer into unreadable one.

3.8 IT VIOLATIONS WITH CORRESPONDING DISCIPLINARY ACTION

Offenses are classified based on their gravity, ranging from category A for minor offenses up to category B for the most serious offenses. Highly considered in the classification are the offenses' effects on the mission of Information Technology Department.

Penalties

3.8.1 ORAL WARNING

An oral warning may be appropriate when informal counselling does not alter the employee's behaviour or the situation warrants moving immediately to formal discipline.

3.8.2 WRITTEN WARNING

A written warning is for seriousness of the misconduct. This is in writing the details of the complaint and the improvement required, with timescales. A copy of the written warning will be on file

3.8.3 SUSPENSION

Suspension is for those employees who commit serious violations that may affect the production. This will be automatically deducted in employee's salary depending on how many days the employee will be suspended.

C.1. Five (5) working days suspension

C.2. 10 to 31 working days suspension without pay

3.8.4 DISMISSAL

Employees who commit most severe violations that may cause shutdown of the operation and/or may put the safety and security of PKII's facilities unprotected and/or at risk, whether in physical form or digital in nature.

Table No. 1 - Category A Offenses

	LIST OF OFFENSES	**Frequency of Offense & Corresponding Penalty**				
		1st	2nd	3rd	4th	5th
1	Unable to turn off the computer after working schedule	A	B	C1	C2	
2	Using others employee assigned computer without permission from the admin and IT staff	A	B	C1	C2	D
3	Unauthorized use of other PKII personnel' User ID to access PKII's networks, e-mail and other IT facilities without its user's approval.	B	C1	C2	D	
4	Unauthorized access or copying or distribution and/or bringing of PKII data files within and outside of PKII's office premises whether virtual or physical.	B	C1	C2	D	
5	Using PKII's IT facilities while accessing internet sites categorized as prohibited sites, including access to time-based restricted sites during its restricted time.	A	B	C1	C2	D
6	Using PKII's IT facilities to make statements or comments against the PKII organization and its management whether through the internal network or through the internet.	A	B	C1	C2	D
7	Sending of unsolicited e-mails or junk/spam e-mails	A	B	C1	C2	D

	using PKII's IT facilities whether intentional or unintentional.					
8	Extensive use of PKII's IT facilities not related to his/her tasks, responsibilities or official business, which affects his/her, work performance and output.	A	B	C1	C2	D
9	Bringing any personal computer/devices used in office premises without any permission.	A	B	C1	C2	D
10	Playing local or online games inside office premises and using company devices.	A	B	C1	C2	D
11	Use of network-file-sharing and peer-to-peer (P2P) programs like bittorrent, utorrent	A	B	C1	C2	D
12	Using imaging equipment to duplicate, alter and subsequently reproduce official documents	B	C1	C2	D	
13	Unauthorized access of any social networking sites during office hours.	A	B	C1	C2	D

Table No. 2 - Category B Offenses

	LIST OF OFFENSES	**Frequency of Offense & Corresponding Penalty**				
		1st	2nd	3rd	4th	5th
1	Installation, distribution or use of any "unlicensed"/"pirated" software OR other proprietary software products not owned by PKII	B	C1	C2	D	
2	Introduction or propagation of malicious programs or scripts (i.e., malicious software/viruses or malware, trojans, worms or harmful e-mail attachments) within the PKII's networks and any of its devices whether intentional or unintentional.	C1	C2	D		
3	Using PKII's IT facilities while accessing internet sites and services using external proxy servers or proxy tools in order to bypass the network's restrictions and its firewall.	B	C1	C2	D	
4	Using PKII's IT facilities to open, display and/or actively engaging in sexually related materials.	C1	C2	D		
5	Any form of harassment to any individual or to its co-employees using any technical device whether owned by PKII or not.	C1	C2	D		

6	Damaging/ Destroying of PKII's IT and other technical facilities whether intentional or unintentional.	C1	C2	D		
7	Falsifying or tampering of daily time records	C2	D			
8	Removing of software without permission from the IT personnel	B	C1	C2	D	

INFORMATION TECHNOLOGY POLICY

Employees' Agreement

This is to confirm that I as personnel of Philkoei International Inc. (PKII) have read and fully understand the above IT Policy.

If I violate, I will submit myself to an investigation thru the IT committee, and if proven guilty may result to corresponding disciplinary actions.

Count	*Full name*	*Signature*	*Date signed*

Noted by:

_____

IT Manager / Supervisor