Office IT Policy
(DRAFT)

Philkoei International Inc.
4/F Pacific Star Bldg.
Makati City

2008-12-15

Table of Contents

1. Intent

The intent of this policy is to establish guidelines for all employees of "**Philkoei International, Inc.**" (or hereinafter 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 4/F Pacific Star Bldg., Makati Ave. cor. Sen. Gil Puyat Ave., Makati City.
- 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 also reserves the right periodically to examine any system, data, internet access, e-mail transactions 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.

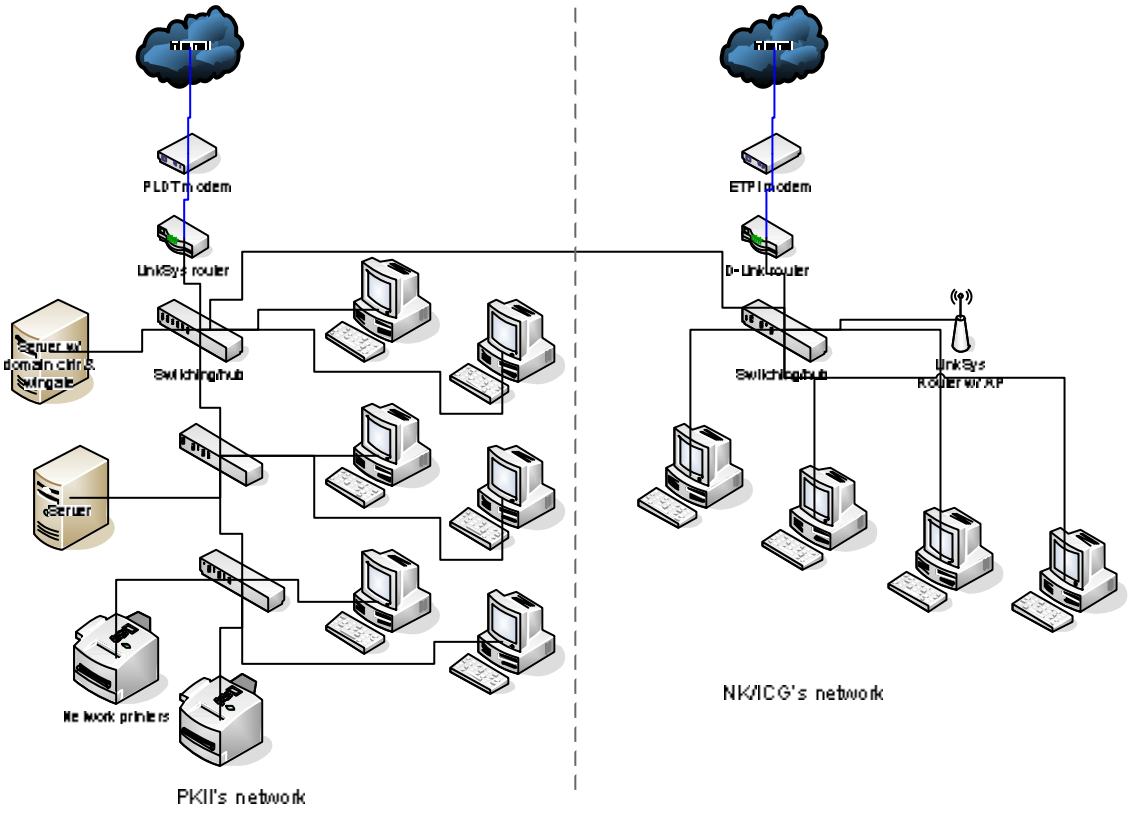
This policy covers four (4) parts namely:

1. Network Architecture
2. File Servers

3. Computer and Software Use
4. Internet Access Use
5. Security and Best Practices

3.1. Network Architecture

- All computers are connected to the internal network or local-area-network (LAN) via cascading switching hubs with a maximum of 100mbps network connection speed.
- An ADSL router is placed on the network and acts as the network-address-translator (NAT), firewall and (DHCP) from the LAN to the PLDT DSL's WAN.
- The PKII LAN use the Transmission Control Protocol over Internet Protocol (TCP/IP) and the Windows Internet Naming Service (WINS) Protocol.
- All computer workstations connected to the LAN are currently on static-IP mode and most mobile PC's or laptops use the DHCP 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.
- Another network from NK/ICG is also connected using Ethernet RJ-45 cable linked to both network switches
- NK/ICG also has its own internet WAN connection thru Eastern Telecoms
- Some users especially the managers and officers using their laptop computers may be allowed to connect automatically on both WAN networks by choosing the DHCP configuration.



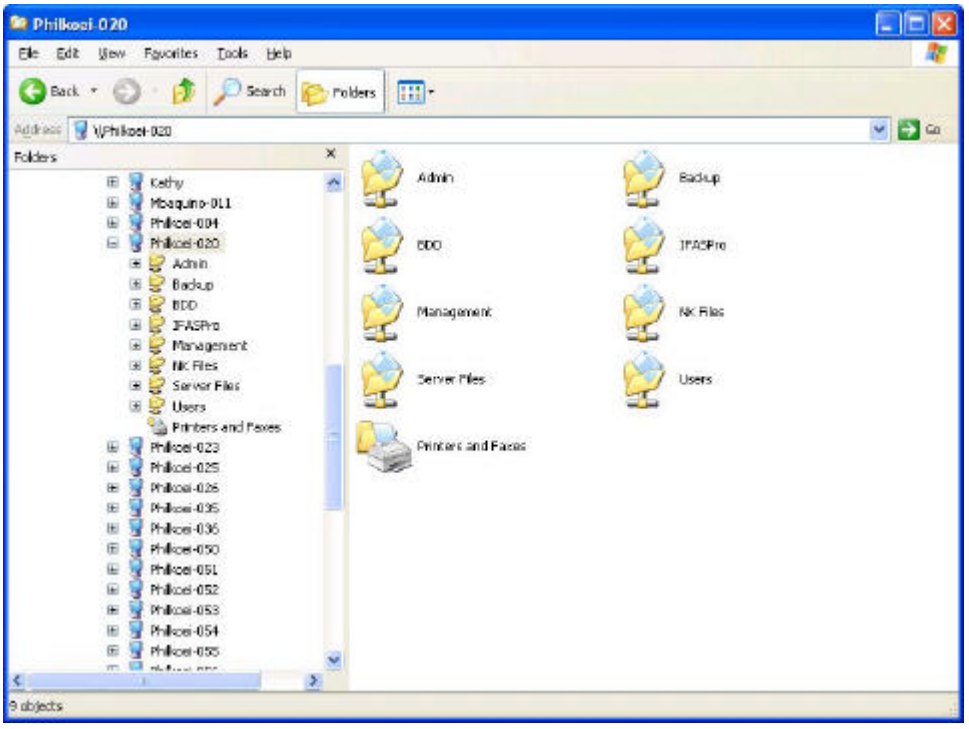
The existing network diagram for Philkoei International Inc.

3.2. The Servers

- The company is equipped with at least three (3) departmental file servers for:
  - Engineering (\\philkoei-055\)
  - Accounting/Finance (\\philkoei-037\), and for
  - Business_Dev't./Admin/Management (\\philkoei-020\).
- The company also has a domain controller server which also acts as the DHCP and internet access policy controller using the WinGate software.
- Two (2) SATA hard drives with the capacity of 320GB (each), mirrored for data redundancy are installed on the file server: \\philkoei-020.
- It is mandatory for all employees to save all their data files to their respective folders in the file server.
- 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 to the management or IT representative within one (1) week from the date of deletion.
- A representative in every department may be assigned to handle the files and folders management in order to organize the files within their respective shared folders on the file servers.

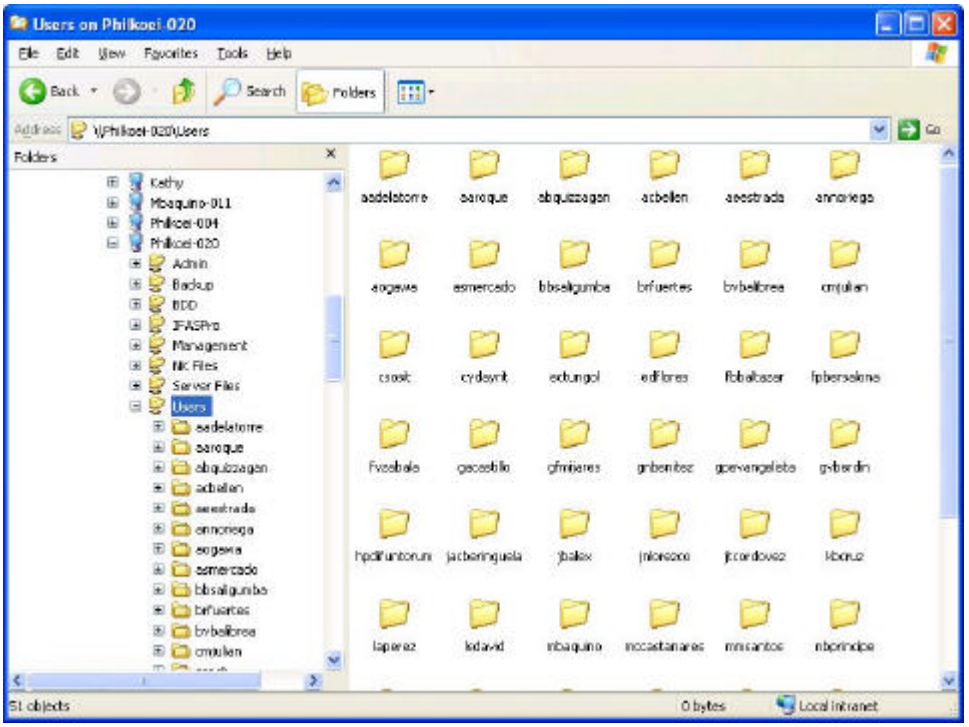
3.4.1. Shared folders on each department

- There are several shared folders on each departmental servers available and accessible with different users permissions and restrictions. Please consult with your IT representative the allowed user permissions and restrictions on the available shared folders.



Example of shared folders on \\philkoei-020

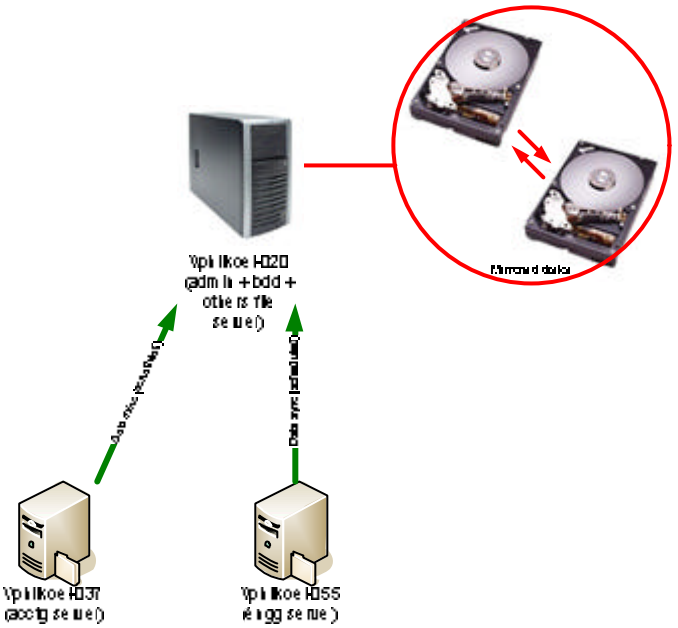
- A 'users' folder in \\philkoei-020\users\ is available to all users with different folders on each usernames, with their respective access permissions. All users are advised to save regularly their office-related files from their desktops or laptops to their assigned folders in order to have a copy of their files for data recovery if ever one's hard drive fails.



Screenshot of the \\philkoei-020\users\ folder

3.4.2. Data backup

- Currently, the office use the configured hard disk mirroring (RAID-1) on \\philkoei-020\ server for data redundancy and backup.
- For the \\philkoei-055\ and \\philkoei-037\ servers for engineering and finance, a scheduled incremental backup to \\philkoei-020\ were configured automatically.
- Plans for a scheduled monthly or quarterly full backup are in the process until the proposed backup device are installed and configured.
- Offsite backup are also planned and may be implemented soon for disaster recovery (DR) purposes.



Servers' data backup and redundancy diagram

3.3. Computer and software use

- All employees with IT access have their individual logins on their respective or assigned computers.
- All computer workstations may be configured to assign several network drives for easy access to their data files on the file servers. These assigned network drives should 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.
- Productivity softwares (such as spreadsheets, document editor and reader, presentation and other productivity tools), anti-virus, internet browser and e-mail clients are installed on each computer.
- Anti-virus software are installed on each computer. Virus definition files are updated automatically when one's computer is connected to the internet or local-area-network.
- All employees are advised not to install any software or programs by themselves. All software installations must be handled by the IT staff/representative and may be pre-approved by the management prior to installation.
- Pirated softwares are prohibited on any computers inside the office premises. Any computer found to have pirated softwares 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 disturb the Company's office operations. It may only be allowed, upon management's approval, if it is work-related.

3.4. Internet access use

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

3.4.3. 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 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 may be accessed by using an internet browser like MS Internet Explorer, Mozilla Firefox, Netscape Navigator, etc.
- Internet access may be available only during office hours. A designated common user_login per department may be assigned for those employees who wish to access the internet after office hours.
- Internet access activities may be monitored by the management anytime.

3.4.4. E-mails

- Employees are assigned with their own official e-mail address (Ex. *loginname*@philkoei.com.ph).
- Official e-mails may be accessed by using an e-mail client such as Microsoft Outlook, Outlook Express or Mozilla Thunderbird on their assigned computers. It can also be accessed thru the web by logging in to: http://www.philkoei.com.ph/webmail
- When sending high-security or very sensitive information thru email, please consult with your IT representative on how to secure your email while sending.
- All e-mail transactions may be monitored by the management anytime.
- Personal use of e-mails like yahoomail, hotmail, gmail, etc. will only be allowed on a limited time and never a priority over work matters.

3.4.5. Instant messengers and prohibited sites

- Instant messengers such as Yahoo Messenger, MSN Messenger, AOL, Chikka, etc. are also not allowed 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 programs like limewire, kazaa, etc. are not allowed in the Company's computer workstations. These programs can and may bypass the firewall settings and makes the entire network vulnerable from attacks and may slow the internet bandwidth.
- Viewing and access to social networking sites such as friendster, facebook, hi5, myspace, tagged, etc. are not allowed in the Company's premises.
- Viewing and watching of online video sites such as youtube, yahoovideo, googlevideo, etc. 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.

3.4.6. Netiquette

A general accepted rules of network etiquette is included on this policy in order for the employees to observe and follow. These include, but are not limited to the following:

- Be polite. Your messages should not be abusive to others.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- Do not reveal any sensitive personal information such as your personal address, phone number or personal pictures to anyone on the internet.
- Illegal activities are strictly forbidden.
- Do not use the network in such a way that you would disrupt the use of the network by other users.
- Note that electronic mail (e-mail) is not guaranteed to be private. Messages relating to or in support of illegal activities may be scanned by the authorities.
- Remove all forwarding message from previous emails. If the email is important enough for you to send it to someone else, it's important enough for you to take the few seconds to remove all the junk and only send the message. Just highlight the section you want to omit and hit the delete key.
- For certain, NEVER post anyone's email address to any web page unless you have their explicit permission. Most of these sites are just gathering email addresses to sell to Spammers.
- Don't forward hoax emails. If there is an unknown virus, you should probably tell the anti-virus software companies so they can update their information to protect everybody.
- Don't send or forward threatening chain emails. People wouldn't want to receive threatening chain emails. Example: "Send this to 10 people or you will get bad luck." Try to send inspiring and encouraging emails.
- Reply within 24 hours. If a reply is needed, try to reply within 24 hours, less if possible. In fact, get in the habit of replying immediately -- the recipient will appreciate a prompt reply and it will make you look efficient.

3.5. Security and Best Practices

3.4.7. Security awareness

Security on any computer system is a high priority, especially when the system involves many users.

- Administrator login is prohibited to any employee unless allowed and approved by the management.
- Please notify the assigned IT technical representative or the management if a security problem is found. Ex.: viruses, worms, Trojans, spywares, network attacks, etc.
- When using a diskette or thumb/usb drives, please scan the drive first using the anti-virus scanner before opening any files within that drive.
- Please be careful of opening any file attachments from your emails (or don't open at all) especially if you don't know the sender. Viruses, worms, Trojans,

etc. are embedded on those attached files and may infect your computer and the network.
- Do not reply to e-mails which you think are spam or junk emails.
- 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. Please check and verify first if the sender or the website is legitimate.
- Always log-off when you leave the computer. Or use desktop locking like screen saver with password.
- 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.

3.4.8. File Management

All employees are advised to establish proper file management in saving their data files on the server. Every department may initiate or provide certain policy on file management for easy access and retrieval of data files.

3.4.9. Version Control

Version Control may also be implemented and mandatory on every employee when creating and saving data files. Additional order or memo may be provided on the proper format on version control of different data files.

3.4.10. Templates

Templates are also encouraged to be created and readily available for better office operations and faster productivity. Every department may provide their own templates based on their needs or requirements.

3.4.11. Support requests

- Requests for IT support may be coursed thru voice, email or other means of communications available.
- Response to these requests may be acted on the soonest possible time. However, IT representatives may need to assess the importance of such requests and the time availability of the representative.
- IT representatives may also validate such requests to their respective managers and officers of each department before any actions are done.

3.6. Additional access policies

Additional access policy or rules such as scheduling of internet access, access to folders on departmental file servers, etc. should be followed based on group or individual policies enforced by the management.

A separate order or memo may be released by the management from time to time to update said additional access policies.