# University of the Philippines

## Proposed University ICT Security Policy

*Version 0.03*
*25 April 2014*

## Table of Contents

## I. Policy Statement and Summary

A. The University of the Philippines is committed to keeping the availability and security of its Information Technology resources.

B. The security of Information Technology services, data, and equipment as shared resources is the responsibility of all network users in the University. It has therefore adapted a policy enforcing security measures for services, users, devices, and information within the network.

C. IT Offices or Computer Centers (CC) of each Constituent University (CU) is the primary implementer of the Security Policies, and personnel of such offices must subscribe to strict ethical and service standards.

D. Towards this end, the University ICT Security Policy has:

1. Designated the proper authority to carry out investigation on misuse and policy violations;
2. Outlined the responsibilities of network users;
3. Provided best practices recommendations to guide administrators to protect the network; and
4. Put forward sanctions for noncompliance, such as network disconnection.

## II. Scope

A. General Coverage

1. This policy shall apply to all faculty, staff, and students of the University and all other users authorized by the University.
2. This policy shall likewise cover the use of University owned, leased, rented, or on-loan facilities; private systems, whether they are owned, leased, rented, or on-loan when connected to the University network directly or indirectly; to all University-owned/licensed data/programs, be they on University or on private systems; and to all data or programs provided to the University by sponsors or external agencies.
3. All users must be aware of the regulations and understand that they are bound by this Policy when performing actions that meet the stipulations outlined herein.

B. Local Use

1. Units within the University may provide for additional terms of use, guidelines, restrictions, enforcement mechanisms, and any other such conditions for devices, data, program, equipment, or any other devices under their jurisdiction.
2. When adopting additional regulations, units will be responsible for publishing such conditions regarding the appropriate and/or authorized use of the facilities for which they are responsible within fifteen (15) calendar days.
3. Such additional regulations, however, must be consistent with the overall Policy.

## III. Purpose of the Policy

This Policy aims to:

A. Prescribe mechanisms that help identify and prevent the compromise of the University network and the misuse of University data, applications, and computer systems;

B. Ensure that all users understand their specific responsibilities for protecting the availability, confidentiality, and integrity of the data and the network they utilize and also realize the importance of applying appropriate security standards in all University related activities;

C. Ensure the automation, technical support, and implementation of proper guidelines needed to keep the Policy effective;

D. Define mechanisms that protect the reputation of the University with respect to its network connectivity to worldwide networks;

E. Implement best practices in addressing the following network issues, which include, but are not limited to:

   1. System, Desktop, and Network Vulnerability Scanning, Logging, Auditing and Intrusion Detection;
   2. Online Services Authentication;
   3. University Internet Access;
   4. Connection to External Networks;
   5. Incident Handling;
   6. Remote Access to the University Network; and
   7. Back-up Policy

## IV. Policies

A. General Security Policy

The following are the general security standards for all devices upon connection to the University network.

1. Device Access

   Only devices authorized by the Constituent University's respective Computer Center shall be allowed access to the CU's networks.

2. Installation of Licensed Software and Software Patch Updates

   When installing software, make sure to install the latest version of the licensed software needed, including all recommended and security patches that are available at the time of installation. After installation, all computers should be routinely maintained and updated. Only the authorized system administrator(s) will have installation privileges. All unnecessary services and software must be disabled or uninstalled.

3. Licensed Anti-Malware and Firewall Software

   Anti-malware and firewall software must be properly installed, running, and updated regularly.

4. Network Authentication

   Proper authentication should be implemented before access to the network is granted. All devices must utilize the University Network Registration System for authorized network access.

5. Physical Security

   Devices must be secured against theft and unauthorized access.

6. Logging
   Operating system and application software logging processes must be enabled on all host and server systems, and configured to lock and re-authenticate when left unattended. Where possible, alarm and alert functions, as well as logging and monitoring systems, must likewise be enabled.

7. Password Strength Recommendation
   University IT equipment should have passwords of at least 10 alphanumeric characters, where applicable.

B. Server Management
The following are the policies for management of servers connected to the University Network:

1. Approved Equipment
   Only equipment of a type that has been approved by the CU CC may be connected to the University network. Wireless equipment is subject to further constraints stated in section C of this document.

2. Server Administrator
   Each server will have a corresponding server administrator whose responsibilities are the following:
   a. Properly register the server at the CU CC.
   b. Keep the server(s) updated and patched appropriately; and configure the server to check for new updates regularly.
   c. Ensure that physical access to the server is limited to authorized personnel only.
   d. The login banner, which informs users accessing the server about its functions, should contain the system's function, ownership, and the consequence of unauthorized access.
   e. Log-in passwords should:
      i. Be at least ten (10) alphanumeric characters including symbols and/or special characters.
      ii. Aging at most three months.
      iii. Have two-step authentication enabled, when possible.
   f. Disable automatic logins and root logins to the server and limit remote access to SSH.
   g. Aside from Systems Administrators' access, there should be a Supervisor account for creating system administrator accounts only.
   h. Set-up a screensaver that is password protected for GUI installations.
   i. Install and regularly update anti-malware software.
   j. Install a firewall and configure it accordingly.
   k. Ensure that only secure file transfer protocols such as scp and sftp, is used for file sharing.

3. IP Address Setting
   All servers must have a static IP address registered with the CU CC. These servers can be mapped to a public address, i.e., through a NAT or similar gateway. Only servers for special cases will be allocated public addresses and have direct access to the Internet.

4. Firewalls
   The server must have a firewall running automatically. Appropriate firewall settings must be configured which include, but are not limited to, the prescribed standards set by the CU CC.

5. Logging
   The server must be configured such that minimum services like connections and authentication information will be logged. The server administrator should be assigned the responsibility to review and follow up on possible security violations identified in the system logs. Audited log reports must be submitted monthly to the CU CC.

6. Back-ups
   Server data back-ups must be regularly run and periodically stored off-site. The restore capability must also be tested periodically.

C. Network Infrastructure and Management
The following are additional requirements for Wireless Access Points connected to Constituent University's network. All other standard usage policies for the Constituent University network likewise apply to its wireless network.

1. Wireless Hotspots
   The Constituent University's wireless network allows mobile users access without having to connect using cables. Users will need to log-in with their CU NET username and password to be able to access the Internet.

   Units who wish to connect to the wireless network maintained by the Constituent University's respective Computer Center must have their access point configured by authorized personnel from the same. All recommendations regarding access point use and security must be agreed upon by both parties.

2. Wireless Consultation and Registration
   It is important to consult with the Constituent University's respective Computer Center if a unit wishes to deploy their own wireless network. The former can help in the planning, specification, and deployment of the wireless network.

   All access points, whether for wireless network access to the Constituent University network or otherwise, have to be registered with the Constituent University's respective Computer Center and must comply with the minimum security standards for access points as discussed in this document. All rogue access points detected by the Constituent University's respective Computer Center will be disconnected from the network and corresponding penalties for non-compliance will be implemented. This would prevent unauthorized wireless access to the local network.

3. Security Settings
    a. All access points should be configured for authentication using 802.1x.
    b. Wireless access points should not be configured as DHCP servers, and the firmware should be configured so as the default settings are not DHCP servers, unless a valid reason for this has been given to the Constituent University's respective Computer Center.
    c. Network Address Translation in the access point is not permitted unless a valid reason for this has been given to the Constituent University's respective Computer Center.

4. Channel Settings
   The Constituent University's respective Computer Center has the discretion for assigning channels for use of wireless internet access within the University.

5. Network Sniffing
   Running any unauthorized data packet collection programs on the wireless network is prohibited. Such practices are a violation of privacy and constitute the theft of user data. Only the Constituent University's respective Computer Center has the authority to monitor the network.

6. Unencrypted Authentication
   All authentications going to and coming from the networked device must use the prescribed encryption method (e.g., SSH, HTTPS).

7. Email Relays
   All communication going to and coming from the networked device must use the prescribed encryption method (e.g., SSH, HTTPS).

8. Proxy Services
   Only properly configured and authenticated proxy servers maintained by the Constituent University's respective Computer Center may be used.

D. Edge Computing Equipment and Management

1. Online Services Authentication
   The following actions shall also be done to ensure authentication is performed when accessing online services:
    a. Configure the system to use available authentication capabilities.
    b. Remove unneeded default accounts and groups.
    c. Change default passwords.
    d. Ensure users follow an industry-approved password policy.

e. Configure computers to require re-authentication after idle periods.
f. Configure computers to deny login after three (3) failed attempts.

2. University Internet Access
    a. Connection to the Internet will only be allowed through gateways and proxies properly configured by the Constituent University's respective Computer Center.
    b. All UP faculty, staff, and students are allowed Internet access through computers assigned for this use in each unit.
    c. All computers connected to the Constituent University's network automatically have access to the Internet. The UP Acceptable Use Policy specifies the appropriate behavior while using this network service.
    d. Internet services will be provided by the Constituent University's respective Computer Center to all units whenever possible in terms of infrastructure. Network infrastructure concerns may be consulted also with this office. Units in turn cannot offer this service using dial-in servers.

The CU CC reserves the right to restrict web access to sites that are appropriate for the University's needs and purposes as discussed in the Acceptable Use Policy of the University. Requests may be made for special cases and submitted to the Constituent University's respective Computer Center for approval.

E. Network Issues

The following are guidelines for the effective intrusion detection within the University network:

1. Device Vulnerability Scanning, Logging, Auditing, and Intrusion Detection
    a. Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
    b. Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
    c. Audit logging of any firewalls and other network perimeter access control system must be enabled.
    d. Audit logs from the perimeter access control systems must be monitored and reviewed regularly by the system administrator.
    e. System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
    f. Audit logs for servers and hosts on the internal protected network must be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the Constituent University's respective Computer Center.
    g. Host-based intrusion tools should be checked on a routine basis.
    h. All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
    i. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported accordingly to the Security team.

Users shall be encouraged to report anomalies in system performance and signs of wrongdoing to the Constituent University's respective Computer Center.

2. External Network Connections
   Connection to external networks is discouraged. If a unit subscribes to a separate network, the external network should be disconnected from the University network, or require network-based firewall, where the following guidelines must be met:
   a. Alerts should be raised if important services/processes crash.
   b. The firewall policy and configuration must be accurately documented and consulted with the CU CC.
   c. The firewall equipment must be subject to regular monitoring and monthly audits by the CU CC and a unit representative.
   d. Remote Access to the University Network shall only be via Virtual Private Network (VPN) connection

## V. Abbreviations

A. DHCP – Dynamic Host Configuration Protocol
B. HTTPS – Hypertext Transfer Protocol Secure
C. scp – secure copy
D. sftp – secure file transfer protocol
E. SSH – Secure Shell
F. VPN – Virtual Private Network