

Introduction

The Management Information System (MIS) office was created in 2003 by the Office of the Campus Director to meet and manage the growing Information and Communication Technology (ICT) requirements of the PSHS – Main Campus. The MIS directly reports to and works with the Campus Director to support PSHS's core mission.

The MIS office will assist the campus community (faculty, staff and student) to apply and help them apply ICT in the execution of their tasks and to the achievement of their goals.

The MIS envisions being the PSHS ICT services partner of choice, delivering quality products, support, and services that focus on customers and add value to the work of the PSHS people -- faculty, students and staff.

Furthermore, the MIS has the following goals:

- Consistently deliver ICT products, support, and services
- Improve, maintain and operate PSHS ICT environment
- Engage in ICT literacy program for faculty, staff and students to realize value of information and communication technology in their line of work and interests.
- Establish a system to continually improve knowledge and skills of the MIS organization.

Overview of MIS Services

The following are the services that the MIS has created and maintained to help the community to properly utilize the ICT resources of the campus:

- Network Infrastructure that are used for:
 - Centralized File Systems for faculty, staff and students
 - File and Print Sharing
 - Wi-Fi Access
 - Internet Access
- Hardware and Software Installation
- Community user accounts
- Response to Repair and/or Service Request
- Web Server Maintenance for PSHS Web Site and Moodle (Course Management Application)
- User orientation and training
- Technical Consultant for the campus
- Enforcement of ICT Policies
- Other services that relates to the use of ICT resources in the campus

The MIS has created several policies, procedures and guidelines to help the community to responsibly enjoy its services listed above. These policies, procedures and guidelines are presented in the next section.

Lastly, the MIS has included in this handbook, several basic safety tips on how to properly use the agency's ICT resources.

PSHS – Main Campus Policies User Account

PSHS Domain User Account and Network Access Policy

A. Username and Password usage and security requirements

1. Every PSHS Network User (student/faculty/staff) is given a username and password and are given a network account with access to their respective server folders, Internet and other network services deemed necessary to his/her position.
2. Username is **first letter of each given name + middle initial + lastname**. Username collision will be resolved by appending a unique number to the more recently created account.
3. Password should be at least eight (8) characters long and a combination of letters, numbers and special characters. Initially all passwords are the same.
4. Students' initial passwords will be announced by the CST teacher one (1) week after the first CS meeting.
5. All users will be required to change their password every 90 days. New password must not be the same with previous passwords. Users will be automatically notified by the system when they will have to change their password.
6. User accounts idle for 3 months (90 days) will be deactivated and will only be made available upon written approved request of the user.
7. User is not allowed to lock the computer.
8. User should refrain from logging-in to more than one computer.
9. User should Log-out from their account when leaving the workstation or room for long period of time.
10. In case of not remembering password, each user is allowed only three (3) password resets per school year

B. User/Unit/Department Server Folder Maintenance

11. All users are given the same limited amount of server disk space (TBA), unless requested otherwise individually. Request should be justified and approved by the department / unit head.
12. All faculty / students user accounts are refreshed (i.e. no network access, individual server folders erased) every start of summer vacation (end of April). Exemption subject to approval.
13. Individual user folder (**My Documents**) content is the responsibility of the user. MIS will not do an individual user data backup.
14. Shared Unit/Department folders' will be backed up by the MIS periodically.

C. Personal Computers/Laptop

15. Personal computers and laptops that will be connected to PSHS network are therefore required to be registered in the MIS department for security and tracking purposes.

D. How to maintain your own user account?

Your username and password is your account passport, and this will entitle you to gain access to the campus network services. The type of services that you can enjoy depends on a profile associated with your account. Therefore you are requested to keep and remember your account information; under no circumstances that you are allowed to share or show your account information with anybody.

Once you gain access to the network, you may be able to work on your documents and access shared information anywhere in the campus, provided that the computer you are using is attached to and recognized by the network and the documents you are accessing was properly saved in the network file servers.

Always properly log-off from the computer after use. Logging-off provides the user with the following benefits:

- Protection from information thefts.

- Protection from identity thefts.
- Network servers will get updated with your profile and your documents, which will allow you to work with the same set of documents anywhere in the campus once you log-in again.

Using My Documents...

Documents that are saved in the My Documents are files that are not to be shared with anybody else but can be accessed by you anywhere in the campus. It is your responsibility that the contents of the My Documents will not go beyond the allotted server space. It is also your responsibility to back-up the files saved in the My Documents. Lost or damaged files in the My Documents are not the responsibility of the MIS office.

Using Shared Resources (Folder, printer, etc.).....

Documents that are used by and shared with the entire department / unit should be saved in **drive Z:**. Files saved in drive Z: could also be accessed anywhere in the campus once you log-in. It is the responsibility of the department / unit to keep the contents of their drive Z: lean. Please remove unnecessary files.

MIS perform periodic back-up procedures on drive Z:. Files in drive Z: and in the back-up disks are not kept indefinitely. Since our network servers have limited space and are used by the entire community, the MIS perform server refresh once a year usually during summer, where everything is erased. Please inform the MIS if you want a CD copy of your documents, and please provide the CDs. **Do not wait until summer to do this.**

To promote cost cutting and to fully utilize our network infrastructure, laser or Inkjet printers are encouraged to be shared within each department / unit. Please contact the MIS for shared printer setup and user orientation on how to use shared printers.

How to request user account creation/updates/password reset?

Staff (Admin) Accounts are created already. Faculty and student user accounts are created / reset every start of the S.Y. Please use the MIS User Account Maintenance Form in case of one of the following:

- Account Creations for
 - new employee (faculty/staff) – by HR / unit head
 - late entry students. –by registrars or CS faculty
- Account cancellation for
 - resigned, terminated or retired employee – by HR
 - or graduated or kick-out students – by registrar
- Reset Account Password
- Account Setup/Reassignment
 - Special request for employee – by HR or by Academic Unit Head
 - Students requirements that does not follow the standard Network User Account Policy.- by any Faculty

Submit the MIS User Account Maintenance Form in the MIS office ASTB RM 101a. Usually, every request is processed on a first-come, first-serve basis. In case when the MIS could not attend to the request immediately, you will be notified of the status thru phone or in case of students thru their Computer Science teachers. The MIS User Account Maintenance Form is available with this user handbook or could be requested from the MIS office.

For immediate processing of request on creating/maintaining user account, please drop by the MIS office and fill-up the MIS User Account Maintenance Logbook and the available technician will attend to you immediately.

Service Request

General Policy

New ICT equipment is tested and setup by the MIS technician and together with the property office personnel place them in the appropriate location.

Each service request that the MIS received is normally processed on a first-come first-serve basis. Priority is given if the request will come from the Office of the Campus Director (OCD) or from the Office of the Executive Director (OED).

OCD and OED requests could be superseded with requests of the utmost importance especially if it will affect delivery of instructions or employee status and compensations.

For each request, please phone the MIS office at 9291603 and supply the needed information for the request. The MIS technician or Systems Administrator will attend to your request the soonest possible time. Please confirm every service made by the MIS technician by signing the service request form or the MIS technician logbook.

Wi-Fi Policy

Through the generosity of Batch '85, the MIS has installed and is currently maintaining three (3) Wi-Fi 802.11b/g "hot spots". These hotspots are located around the vicinity of the ASTB front lobby, cafeteria, and girl's dormitory annex.

All faculty, staff and students could enjoy the use of these hotspots provided that their mobile devices are registered with the MIS office for tracking and security purposes. The use of these facility is limited only for internet surfing.

Wi-Fi Registration and Access

Mobile devices that are to be used for internet surfing must be registered every school year in the MIS office. Fill-up and sign the MIS Wi-Fi Registration Form, the technician or systems administrator will copy the MAC Address and computer name of the mobile device. An access-point domain name and WEP pass key will be configured in the mobile device for security purposes. Once registered, you can enjoy the use of the hotspots until the end of the school year.

Use of the "hotspots" during summer break should have a written approval by the CISD Chief or by the Campus Director.

Service and Support for Teacher/Staff Equipment/Laptops

The MIS will assist teachers/Staff with hardware and software problems provided they are directly related to their duties and assignments. Whenever there is a software problem that can not be fixed in a reasonable amount of time, re-imaging of the machine will be encouraged. This will return the machine to its original working condition. All effort will be made to recover official data on the laptop. The MIS will answer specific questions about software use if possible.

Service and Support for Students'/Parents' Equipment/Laptops

Due to limited number of MIS personnel, we are not accepting service requests or give technical support to Students' Equipment/Laptops, unless it is for W-Fi registration

Limitations on Support for Personal Equipment

The MIS does not offer service on personal equipment or personal use of equipment during school hours. If a student or teacher requests help for a personal use of their machine, the request must be cleared by the MIS Coordinator.

MIS User Form Templates

Basic Survival Tips

Creating a Strong Password and Don'ts in Password Protection

(Source: Colorado State College)

A. General Password Construction Guidelines

Passwords are used for various purposes in PSHS-Main Campus. It is used to access your domain accounts, to access your e-based accounts and your email accounts. It is very easy to guess or crack certain types of passwords, everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "PSHS-Main Campus" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:;';<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for PSHS accounts as for other non-PSHS access. **Where possible, don't use the same password for various PSHS access needs. For example, select one password for the network/computer logon and a separate password for ebased systems.**

Do not share PSHS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential PSHS information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to a friend
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")

- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- For employees, don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to the MIS office.

Avoid using the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger), where possible.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to the MIS and change all passwords.

Internet Access Guidelines

The entire PSHS Community unlike other institution is given the privilege of the use of the network infrastructure for internet access. This privilege must be used responsibly in order not to compromise the entire PSHS network.

The following are guidelines on safe internet access:

- Do not go to sites that are prohibited in the DOST ICT Network Usage and Security Policy.
 - No game sites
 - No pornographic sites
 - No video streaming sites
 - No proxy sites or anonymizers
- Surf with caution. If you are exploring sites that are not in your usual lists, do not click links indiscriminately.
- Avoid excessive downloads during office hours.
- Any sites that requires you to log-in, please refrain from clicking save this password button.
- When joining an on-line discussion, please observe proper etiquette. (i.e. avoid typing in all caps, avoid foul languages, avoid bashing people online)
- Avoid clicking on pop-up advertisements, this could direct you to illegal sites or this could infect your computer with malwares (virus, worm, etc.)
- Avoid discussing sensitive cases over an online discussion group. (i.e. discipline cases)

Guidelines for using Emails

Public Email services are allowed by PSHS – Main Campus. The following are guidelines for proper email account use:

- According to our e-commerce law, emails are considered legal documents and it could be used for or against you in any legal proceedings.
- Avoid capital letters when creating your emails.
- Do not open emails from the following:
 - Unknown sources
 - Nonsense subject lines (i.e. randomized passages, software offers, freebies, etc.)
 - Known source but nonsense subject lines
- Treat any attachments with caution.
- Do not attach large documents in your emails, unless after office hours.
- When emailing or forwarding emails to group of people, refrain from displaying their individual email addresses, unless necessary. Use BCC instead of CC.
- Avoid email for sensitive subjects. (i.e. discussing discipline cases)

Before reporting any problems....

Before contacting MIS personnel, it would be helpful if you tried out a few simple troubleshooting tricks. Trying these out will aid the personnel later on in resolving your computer issues.

Is there power?

Everything works better with power, and when they are connected properly. Make sure that any network devices, such as hubs and switches, are powered on at least 5 minutes before any computers can log in. If there are unconnected cables at the back of the unit you are working on, and you are unsure of where they go, you may contact the MIS personnel for assistance.

Is the problem local or with the entire system?

Have someone else try out what you're trying to do. If the printer doesn't print, for example, you could ask a colleague to try it out using his or her user account. If that doesn't work, try it out on another workstation.

Have you tried restarting the computer?

You may be surprised how many issues can be resolved by this.

What was the last thing you did?

"Everything was working fine, until..."

Read the messages carefully before clicking anything

Some programs may leave suggestions or clues to the problem with their error dialog boxes. Read them carefully for such clues, and try them out.

**Philippine Science High School – Main Campus
Agham Road, Diliman Q. C.**

**User Handbook
on
Management Information System
Policies and Procedures**

Prepared by

Aline Teresa L. Mendoza
alinemendoza@yahoo.com

Jason Alcaez
jalcarez@yahoo.com

As of April 2007

Table of Contents

Introduction	1
Overview of MIS Services	1
PSHS – Main Campus Policies	
User Account	
PSHS Domain User Account and Network Access Policy	2
How to maintain your own user account?	2
Using My Document..	3
Using Shared Resources (Folder, printer, etc.)....	3
How to request user account creation/updates/password reset?	3
Service Request	4
General Policy	4
Wi-Fi Policy	4
Wi-Fi Registration and Access	4
Service and Support for Teacher/Staff Laptops	4
Service and Support for Students Laptops	4
Limitations on Support for Personal Equipment	4
MIS User Form Templates	
User Account Form	5
Service Request Form	6
Basic Survival Tips	
Creating a Strong Password and Don'ts in Password Protection	7
Internet Access Guidelines	8
Guidelines for using Emails	8
Before reporting any problems....	9
Annex A: DOST ICT Usage and Network Policy	