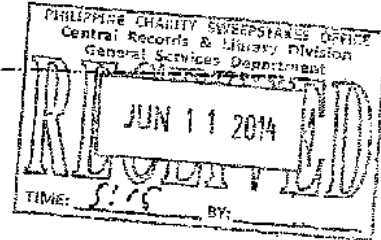


PHILIPPINE CHARITY SWEEPSTAKES OFFICE

Sun Plaza Building, 1507 Shaw Boulevard, Mandaluyong City



SECRETARY'S CERTIFICATE

I, **RAMON RODRIGO**, of legal age, Filipino, married and with business and postal address at the Philippine Charity Sweepstakes Office, 4th Floor, Sun Plaza Building, Shaw Blvd., corner Princeton Street, Mandaluyong City after being duly sworn according to Law, hereby certify:

1. That I am the Board Secretary of the Philippine Charity Sweepstakes Office (hereinafter referred to as "PCSO"), an agency of the national government engaged in the operation of sweepstakes and lotto;
2. That as such, I have custody of all records pertaining to the Board of Directors of the PCSO including all Board Resolutions;
3. Per the records of the Office of the Corporate Secretary of the PCSO, the Board of Directors thereof, during its **20th Regular Board Meeting held on June 11, 2014** held at 4th Floor, Sun Plaza Building, Shaw Blvd., corner Princeton St., Mandaluyong City passed the following Resolution:

**RESOLUTION NO. 207**  
Series 2014

**"WHEREAS**, the Assistant General Manager for the Management Services Sector recommended the Information and Communication Technology (ICT) Usage and Security Policy covering the appropriate, secure and legal use of ICT equipment, facilities, data, software and services;

**"WHEREFORE**, per recommendation of the Management Services Sector, the Board **RESOLVED AS IT HEREBY RESOLVES** to approve the Information and Communication Technology (ICT) Usage and Security Policy hereto attached as Annex "A" covering the appropriate, secure and legal use of ICT equipment, facilities, data, software and services, subject to compliance with applicable laws, rules and regulations."

4. Per the records of the Office of the Board Secretary, the foregoing Board Resolution has not been replaced, amended or repealed.
5. This Secretary's Certificate is issued for whatever legal purpose it may serve.

IN WITNESS WHEREOF, I have affixed my signature on this \_\_\_ of June 2014, at Pasay City.

**ATTY. RAMON RODRIGO**  
Board Secretary

SUBSCRIBED AND SWORN to before me on this \_\_\_ day of June 2014, affiant exhibiting to me his SSS No. 03-27523102-4.

**Certified True | Xerox Copy**

**OFFICE OF THE BOARD SECRETARY**

**NOTARY PUBLIC**

\_\_\_\_\_  
6-11-14  
DATE

**ROSALYN D. CAMPANANO-CORTES**  
NOTARY PUBLIC  
VALID UNTIL DECEMBER 31, 2014  
IBP OR No. 913632 PASIG CITY 01-02-2013  
PTR OR No. 1201278 PASAY CITY 01-02-2013  
MCLE No. 19501112

Doc. No. 324  
Page No. 66  
Book No. 107

**Information Technology Services Department (ITSD) Information and Communication Technology (ICT) Usage and Security Policy**

**I. POLICY STATEMENT**

- A. All the Information and Communication Technology (ICT) equipment like computers, printers, switches and the likes and all Information Technology resources are property of Philippine Charity Sweepstakes Office (PCSO) and not of particular individuals and therefore must be used in work related tasks which then will be beneficial to the Agency as a whole.
- B. Furthermore, all ICT facilities, equipment, devices and information should be used within legal boundaries, effectively, in good faith to others and most especially without undermining PCSO.
- C. This policy relates to all ICT facilities, equipment, resources, services and information provided by PCSO. All employees either permanent, casual, confidential agents, consultants or every category of employees as long as they are connected with the agency and the agency's branch offices are expected to adhere to it.
- D. Failure to abide by this policy shall be dealt with accordingly pursuant to Civil Service Commission (CSC) rules and regulations and more importantly by laws governing the Republic of the Philippines.

**II. SCOPE OF THE POLICY**

This policy covers the appropriate, secure and legal use of ICT equipment, facilities, data, software and services and will apply to all PCSO employees or personnel attached to the agency and branch offices.

### III. DEFINITION OF TERMS

#### **Antivirus**

a protective software designed to defend your computer against malicious software. Malicious software, or "malware" includes: viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals your computer contents.

#### **Application Delivery Controller (ADC)**

a computer network device in a Data Centre, often part of an application delivery network (ADN), that helps perform common tasks such as those done by web sites to remove load from the web servers themselves. Many also provide load balancing. ADCs are often placed in the DMZ, between the firewall or router and a web farm.

#### **Bandwidth**

a measurement of bit-rate of available or consumed data communication resources expressed in bits per second or multiples of it.

#### **Computer**

An electronic device for storing and processing data, typically in binary form, according to instructions given to it in a variable form.

#### **Data Centre**

a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

#### **Disk Space**

an amount of computer storage space on random-access memory devices, such as on a hard drive, floppy or USB flash drive.

**Email**

a system for sending and receiving messages electronically over a computer network, as between personal computers

**End User**

The person who actually uses a particular product.

**External hard drive**

a portable storage device that can be attached to a computer through a USB or FireWire connection, or wirelessly. External hard drives typically have high storage capacities and are often used to back up computers or serve as a network drive.

**Hardware**

The machines, wiring, and other physical components of a computer or other electronic system.

**Hub**

a device for connecting multiple Ethernet devices together and making them act as a single network segment.

**Information and Communication Technology**

refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions.

**Information Technology**

the branch of engineering that deals with the use of computers and telecommunications to retrieve and store transmit information.

**Internet**

the single worldwide computer network that interconnects other computer networks, on which end-user services, such as World Wide Web or data archives, are located, enabling data and other information to be exchanged.

**Intrusion Detection System (IDS)**

a network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

**Intrusion Prevention System (IPS)**

a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

**Laptop**

a portable microcomputer, suitable for use while travelling.

**Network**

a group of two or more computer system linked together.

**Network Connection**

a system of interconnected computer systems, terminals, and other equipment allowing information to be exchanged.

**Network Domain**

a group of users in a network who shares a common set of shared resources, such as server disk drives and printers.

An interconnected group or system.

**Network Firewall**

protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two.

**Operating System**

the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

**Precision Air Conditioning Unit (PACU)**

this system controls temperature, humidity and particle filtration within tight tolerances 24 hours a day and can be remotely monitored. It can have built-in automatic alerts when conditions within the server room move outside defined tolerances.

**Printer**

a machine for printing text or pictures onto paper, esp. one linked to a computer.

**Router**

a device that forwards data packets to parts of a computer network.

**Scanner**

a device that captures images from photographic prints, posters, magazines pages and similar sources for computing editing and display.

**Server**

a system (software and suitable computer hardware) that responds to requests across a computer network to provide, or help to provide, a network service.

**Social networking site**

a platform to build social networks or social relations among people who, for example

Share interests, activities, backgrounds, or real-life connections.

**Software**

the programs that can be used with a particular computer system.

**Specification**

a detailed description of the design and materials used to make something.

**Streaming media site**

A website where video or audio content are sent in compressed form over the Internet and played immediately, rather than being saved to the hard drive.

**Network Switch**

a computer networking device that links network segments or network devices.

**Uninterruptible Power Supply (UPS)**

an electrical apparatus that provides emergency power to a load when the input power source, typically mains power fails.

**Website**

a group of connected pages on the World Wide Web containing information on a particular subject.

#### **IV. GENERAL NETWORK ACCESS POLICY**

- A. The network connection in PCSO will be utilized by the agency's employees for work related functions only. Also, employees with permission from their respective department heads to access the network will be given user accounts by the Information Technology Services Department (ITSD). As such, all Network Access policy will apply to all users connected to the PCSO network.
- B. Internet websites such as social networking sites, websites with obscenity and pornography, websites that consume excessive Internet bandwidth and websites that pose risk to the network and IT resources will be prohibited for access.
- C. In the event that an employee must access certain blocked sites in the office for work related purposes, an employee must make a written request addressed to the Chairperson or General Manager and must be signed by his or her department head. Once the request is signed, that will be the time that the ITSD will unblock certain websites for that particular employee/s.

#### **V. COMPUTER ACQUISITION**

- A. ITSD shall be in charge in providing hardware specifications for desktop computers, laptops, printers, scanners and other computer peripherals.
- B. There shall be a standard specification for desktop computers and laptops. ITSD shall update this standard every six months, or as the need arises.
- C. End users requesting for desktop computers and laptops with additional peripherals shall inform ITSD of the particulars and the reason for such request. ITSD shall then evaluate the request and make the necessary recommendation.
- D. Desktop computers which are more than 5 years should be replaced, provided that the request is included in the Corporate Operating Budget (COB) and functional verifications by ITSD personnel have been made on the IT equipment which need replacement. Further, the request should be approved by their respective Department Manager, the Budget and Accounting Department Head and the General Manager.

## **VI. DESKTOP COMPUTER / LAPTOP Setup and Configuration**

- A. Newly acquired desktop computers and laptops shall be sent to the ITSD for proper setup and configuration.
- B. New desktop computers and laptops shall be installed with the following software packages:
  - a) Licensed Operating System (ex. Windows 7, etc.);
  - b) Corresponding device drivers;
  - c) Peripheral device drivers (for computers with printers, scanners, etc.);
  - d) Licensed Microsoft Office suite (Word, Excel, PowerPoint);
  - e) Licensed Endpoint protection software (Antivirus, Firewall, etc.);
  - f) Utility software such as Adobe Acrobat Reader;
  - g) Service packs, patches and other software updates;
  - h) PCSO Information Systems software used by the end user
- C. Only ITSD shall be authorized to install software in the computers. End users are not allowed to install any software on their desktop computers / laptops.
- D. End users needing additional software installed in their desktop computer / laptops shall inform ITSD of the particulars and the reason for the request. ITSD shall then evaluate the request and take the appropriate action.
- E. ITSD shall register the new desktop computer / laptop to the PCSO network domain before returning the workstation to the end user.

## **VII. IT HARDWARE AND SOFTWARE MANAGEMENT**

- A. Definition. IT Hardware are composed of, but not limited to the following:
  - Computers and its peripherals
  - Routers, hubs and switches or anything that controls data or flow in the network.
  - Network Security Devices such as Network Firewall and Intrusion Prevention System/Intrusion Detection system (IPS/IDS) and Application Delivery Controller (ADC).

- Data Centre equipment such as Uninterruptible Power Supply (UPS), Precision Air Conditioning Unit (PACU) and Temperature and Humidity Sensor.
  - All computer software and Operating System such as Windows XP, Windows 7, computer applications etc.
- B. Authority to install, upgrade, delete, configure and manage the IT hardware and Software are responsibilities of ITSD personnel or any person or group of persons who has written and signed authorization letter from the Head of the Agency.

## VIII. NETWORK ACCESS REQUIREMENTS

- A. All employees with permission from their respective department heads to access the PCSO network will be given user accounts with passwords by the ITSD. These usernames and passwords will be used by the employees when logging into the PCSO network and accessing the Internet.
- B. An initial or default password will be given by the ITSD and it is the sole responsibility of the user to change and secure his or her password. A standardized username will be given by the ITSD for every user.

## IX. INTERNET ACCESS

Internet Access Privileges. Each user shall use the account issued for them to log-in to their desktop/laptop. Once the employee logged-in to the network, they will gain access to the PCSO Internet service, subject to the following conditions:

- A. Blocked Sites. For security reasons, certain websites are blocked for the employees to access.
- a. Security Risk - web sites which may either directly constitute a risk to IT resources, or are associated with activities suspected to increase risk of exposure to internet dangers.
  - b. Liability - web sites that may be in conflict with applicable legal and/or policy compliance obligations such as Hacking, Pornography, Criminal Activities, etc.

B. Website categories blocked from (8:00 am – 12:00 pm) and (2:00 pm – 5:00 pm)

- a. Bandwidth Intensive - web sites w/c may result in large amount of data to be uploaded or downloaded like streaming media, video download, file download, etc.
- b. Online Communities or Social Networking Sites - web sites w/c provide dynamic content for the purpose of social networking.
- c. Employees may be given access to Online Community & Streaming Media sites provided that it is necessary and consistent with his/her duties and responsibilities. Employee should seek a written approval from the Chairperson or General Manager for him/her to be allowed to access these websites.

## X. ANTIVIRUS

Only antivirus software from the ITSD should be installed in all agency computers and laptops. As such, only ITSD personnel are allowed to install the antivirus software but it is the responsibility of the user to keep the installed antivirus updated.

## XI. CORPORATE E-MAIL ACCOUNT

- A. Corporate e-mail accounts will be given by ITSD to PCSO employees with permission from their respective department heads. Each email disk space is limited to 1 GB per user with an attachment not to exceed 100 MB per message.
- B. It is the responsibility of the user to maintain his or her e-mail account, email accounts are privilege given to employees and should therefore be used for work related purposes only.
- C. If in the event the employee with email account be separated or terminated from the agency, it is the right of the agency to withdraw the email privileges given including all the email files of the user. Termination of email accounts of terminated/separated employees shall be done upon receipt of written advice from the Human Resources Department.

## **XII. CORPORATE WEBSITE**

- A. It is the responsibility of ITSD personnel to host, manage and secure the server of the corporate website inside the ITSD Data Centre.
- B. All the contents (materials/documents/articles etc.) shall go thru the following, before they are posted in the PCSO website by the ITS Department:
- Contents are reviewed, evaluated and edited by the Corporate Planning Department.
  - AGM for Management Services Sector shall then recommend the approval of the contents reviewed, evaluated and edited by the CPD before posting
  - The Head of the Agency/General Manager shall then approve the contents to be posted in the PCSO website
  - News articles, photos and other materials which are two (2) years or older shall be archived for a maximum of one (1) year.
- C. In the event that the Web Administrator notices outdated contents that need to be removed/replaced from the website, the Web admin shall then prepare a memorandum to the concerned department/s or office/s indicating the particular contents to be removed, signed by the ITSD Department Manager, to be recommended for approval by the AGM for Management Services Sector and approved by the General Manager.
- D. In cases where in the ITSD and/or any other Department/Office personnel sees or notices wrong/inconsistent information posted in the Agency website, he/she will immediately inform the Corporate Planning Department about the wrong information. The CPD will then evaluate, verify and correct the data and immediately submit the corrected document to the ITSD, informing the concerned Department/Office about the correction.

## **XIII. NETWORK MONITORING AND TECHNICAL SUPPORT**

- A. All ICT resources requisitioned by the employee shall be the responsibility of the user but the right to monitor the usage of the equipment, monitor network based activity, and bandwidth usage shall rest upon the ITSD. The ITSD has the right to report to the management any event wherein the employee is not using the ICT equipment or device properly.

- B. For technical support, the employee should call the ITSD and not repair or remove any programs, applications and computer peripherals on their own. ITSD personnel will then ask the user to fill up a Job Order/Request Form indicating the Nature/Purpose of Request of the user and Diagnosis/Procedure done by the ITSD personnel to solve the problem among others.
- C. If the ITSD monitors any problem in the user's computer, the ITSD shall then inform the user of the problem detected, ITSD personnel shall ask the user to save the files to a separate external hard drive and pull out the computer for repair if necessary. The user shall then sign a waiver form stating that in case any files or data are lost in the repair process, the ITSD will not be liable.

#### **XIV. BRING YOUR OWN DEVICE (BYOD)**

- A. Connecting a smart phone or tablet to the PCSO network will be granted to the PCSO employee upon approval of the department head and/or management and the ITSD.
- B. The agency also reserves the right to revoke these privileges in the event the user does not follow the set of rules and policy laid out by ITSD and the agency.
- C. The word device in the title includes, but not limited to, android devices, i-phone, tablet of any platform, black berry, windows mobile etc.

#### **XV. IMPLEMENTING GUIDELINES FOR THE DEVELOPMENT OF APPLICATION SOFTWARE AND DATABASE PROPOSAL Attached as ANNEX A**

#### **XVI. WAIVER**

PCSO or ITSD shall not be responsible for any loss or damage, whether direct or indirect, that may arise from the use of the PCSO ICT equipment and resources by any person or entity.

**XVII. AMENDMENTS AND EFFECTIVITY**

- A. The management and the ITSD may recommend the amendment, editing or modification of any part of this policy to be approved by the Board, as long as it will retain the effectivity and applicability of the policy. The amendments made shall form part of the ICT Usage and Security Policy.
- B. This policy is effective upon the recommendation of the General Manager approval of the PCSO Board.

**Recommending Approval:**

**JULIETA F. ASEO**

**AGM for Management Services Sector**

**ATTY. JOSE FERDINAND ROJAS II**  
**General Manager**  
**Philippine Charity Sweepstakes Office**

## **IMPLEMENTING GUIDELINES FOR THE DEVELOPMENT OF APPLICATION SOFTWARE AND DATABASE PROPOSAL**

---

PCSO business applications and database are considered critical information assets of the institution because they compose a significant part in the PCSO daily operations. Securing these assets is, therefore essential to PCSO's reputation and public reputation.

This document provides guidelines in the development of applications systems and set-up their corresponding databases.

### **SCOPE**

These guidelines apply to all application systems and database developed and/or used by PCSO.

### **DEFINITION OF TERMS**

**Application Systems** – Computer software that is being used for day-to-day PCSO operations.

**Change Control** – an internal control procedure by which only authorized amendments are made to the application system, database, hardware, network access privileges, or business processes and methodology.

**Credentials** – something known (e.g. a password or passphrase) and/or something that identifies a user for authentication (e.g. a username, hardware token, smart cards or biometrics).

**Entitlement** – the level of privilege authorized by the system.

**Binary Code** – the series of computer instructions that the computer executes to run a program.

**Language** – a system of command words, symbols and rules used in the development of application systems.

**LDAP** – Lightweight Directory Access Protocol, a set of protocols for accessing information directories.

**Library** – an area of the server that retains system file in an orderly and secure manner.

**Regression Test** – A test to ensure that an application system as per specification after a revision is made.

**Software Development Life Cycle** – know as SDLC, is the overall process of developing, maintaining, improving and changing an application system through a multistep process from the investigation of its requirements through analysis, design, development, implementation and maintenance.

**Source Code** – the actual program prepared by the software developer, which is compiled into machine language. It is considered as an intellectual property of PCSO.

Stress Test – a test performed on an application system to determine if, following any abnormal condition, the system can revert quickly to normal operation. Such conditions could include: data processing after a system downtime, network failure or peak activity periods.

## **IMPLEMENTING GUIDELINES**

### **Segregation of Duties**

1. Information Technology Services Department (ITSD) shall ensure that proper segregation of duties be applied to all areas dealing with application systems and database development, including its operations and administration.

### **Application System Development**

1. The operation or creation of operational or program source libraries shall be documented and shall follow standard change procedures and changes.
2. Only authorized personnel shall have access to operational or program source libraries. Approval to access source libraries shall be granted to system owners and the ITSD's System, Web and Graphics Division head.
3. Changes to such libraries shall only be made through technical access controls and standard procedures under dual control.
4. Formal change control procedures with audit trails shall be used to control program source libraries and version of old programs. Such changes shall be properly authorized and tested before being moved to the live environment.
5. For an automated library or source code management system, library access permission shall be defined and restricted upon the system's installation. The system's audit reporting shall be enabled to provide a report on any activity performed.

### **Development**

1. Any proposed application system shall be properly planned, discussed with the concerned units, authorized and documented before being implemented.
2. Any proposed application system development or enhancement shall be business driven and supported by an agreed business case for which the system owner shall take full responsibility.
3. Out-sourced or in-house development shall address risks, security controls and procedures for information systems, network and desktop environments in their proposals
4. All application systems developed for or by PCSO shall strictly follow a standard development process (*i.e. Software Development Life Cycle or SDLC*) based on industry best practices considering information security throughout the system's life cycle.
5. Only standard and secured programming languages and software shall be considered in the development of an application system.
6. Standard change control and version control procedures shall be developed and used for all changes to any application system. All changes to application systems shall be authorized and evaluated in a test environment before it is moved to the live environment.
7. Emergency changes done on an application system shall be strongly discouraged, except in circumstances designated by management as critical. Such changes shall strictly follow the standard change control procedure.
8. The integrity of PCSO's source codes shall be safeguarded using a combination of technical access controls and restricted privilege allocation and version control procedure

9. All documents relating to system application development (e.g. source codes) shall be secured and classified according to the approved information classification scheme. Declassified shall be disposed through shredding.

### **Testing**

1. The use of live data for testing new or revised application systems shall only be permitted where adequate controls for security of the data are in place.
2. A standard testing process (i.e., system testing, QA testing then UAT) shall be used prior to the release of new or revised application systems for use in the live environment.
3. Security test shall be done on newly developed application systems. Upon completion of such test, the application systems shall be expected to meet or exceed the security requirements of ITSD Database Administration division.

### **Training and Documentation**

1. Training shall be provided to users and technical personnel in the functionality and operations of all newly released application systems.
2. All new enhanced application systems shall be fully supported at all times by comprehensive documentation. Such application systems shall not be introduced to the live environment unless supporting document is available.

## **DATABASE DEVELOPMENT**

### **Database Setup**

1. The information created and stored in the PCSO's database shall be retained at a minimum period of five years while the value of the data continues to meet both the legal and business requirements.
2. The classification of information stored in the PCSO's database shall be classified based on their sensitivity and confidentiality. All financial or data models used as basis for this shall be fully documented and controlled by the system owner.
3. Database shall be fully tested for both business logic and processing, prior to operational usage.
4. Controls shall be implemented to prevent any SQL injection and any bypassing of client-side input controls.
5. Where databases are to contain confidential information, procedures and controls shall be established to restrict unauthorized access.
6. The creation of the database structure shall require approval from system owners with users adhering to the structure. Access restriction to such structures shall be applied to restrict unauthorized access.

### **Database Fields and Tables**

1. The following critical tables shall be secured and restricted:
  - Database server system tables, including user and password tables
  - Library access definition tables
  - Audit trail tables
  - Database dictionary
  - Database utilities
2. Access to certain database fields and logical views to database tables shall be restricted to specific authorized users performing data center operations.

### Retrieval of Data

1. Multiple accesses to data shall be made available at all times to authorized users.
2. Each data item shall be accessed strictly through their application systems. Application system user shall not be given access to the database system itself.
3. Data shall only be processed, viewed or modified using the application system utilizing the database.
4. Data shall not be downloaded to other systems or printed through any means other than the approved application system/software utilizing the database.

### Data and Database Structure Changes

1. Existing database structures shall only be changed after obtaining approvals from the system owners and the ITSD manager. Such changes shall be in accordance with standard change control procedures.
2. Emergency data changes shall only be allowed in extreme circumstances and only in accordance with emergency change management procedure.

### Database Credentials

1. To maintain the security of PCSO's internal database, access by application systems shall be granted only after proper authentication with database credentials.
2. The database credentials used for this type of authentication shall not reside anywhere in the application systems' source code nor in the directory where the application is stored.
3. Database credentials shall only reside on the database server and only in encrypted form.
4. Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as LDAP server used for user authentication.
5. The use of Administrator level username and passwords shall not be allowed when accessing the database remotely, except when credential are properly protected from network sniffing with the use of network traffic encryption.

### Database Username and Password Storage

1. Database passwords shall not be hard-coded into the source code or binary form of the application
2. Database authentication may occur on behalf of a system as part of the user authentication process at the authentication server. In this case, programmatic use of database credential shall no longer be necessary.
3. Pass-through authentication (i.e., Oracle OP\$ authentication) shall not allow access to the database based solely upon a remote user's authentication on the remote host.
4. Passwords or Passphrase used to access a database shall adhere to existing guidelines on passphrase management.
5. Passwords for the default database user (i.e., SA for MS SQL SERVER, and SYS, MANAGER for Oracle) shall be changed immediately right after a successful installation.
6. Default or unnecessary database user accounts shall be disabled or deleted before the application is deployed to production.
7. User credentials and authorization details shall be stored in a separate database table independent from other data sets used by the applications.
8. Passwords or Passphrase shall be in encrypted form at all times.
9. The production database shall have different password information from the test database systems.

### Access to Database Usernames and Passwords

1. Only the Database Administrator shall have direct access to the maintenance of the database usernames and passwords. Audit logs shall be enabled in the database server to ensure that modification to the credentials table are logged.

2. Every application system implementing a single business function shall have a unique entry in the database credentials table. Sharing of credentials between systems shall not be allowed.
3. Database passwords used by application systems are considered system-level passwords and shall be treated as such as far as securing it is concerned, as defined by existing guidelines on password management.
4. Internal software development groups from ITSD and their consultants shall have a process in place to ensure that the use of database passwords is controlled in accordance with existing guidelines on password management. The consultant's use of database credential shall be bound by the Terms and Conditions and Non-Disclosure Agreement with PCSO.

## Responsibilities

1. System Owner
  - Approves the development or revision of an application system
  - Concurs with designs of the application system's database of the Systems, Web & Graphics Division, with the assistance of the Database Administrator.
2. ITSD Head/Manager
  - Acts as an overall supervisor.
3. ITSD Database Administration Division
  - Ensures the development of infrastructure necessary to support the implementing Guidelines for the development of new system and their database, including the standards and procedures in setting the database credentials and access.
  - Participates in discussion on application system and database development related to information security.
  - Develops and performs a security test plan for security tests on application system and database, such as access and system penetration tests, capacity/peak, stress and regression tests as part of UAT.
  - Monitors and maintains the continuing effectiveness of the implementing guidelines in ensuring the confidentiality, integrity and availability of information.
  - Initiates change in the implementing guidelines whenever necessary to mitigate new risks related application systems and their databases.
  - Coordinates with ITSD manager for the information security-related training and orientation program for employees.
  - Assists the Systems, Web and Graphics Division in the establishment of standard process for the development and maintenance of various systems (*i.e.*, SLDC).
  - Develops, tests, and maintains the database for all application systems of PCSO.
  - Develops and maintains procedures for the design, testing, operation, maintenance and documentation of operational databases.
  - Develops and practices version control procedures for all database systems.
  - Assists the SWGD in the development and execution of tests for application systems such as access and system penetration tests, capacity/peak, stress and regression tests.
  - Coordinates with various users through ITSD regarding libraries, database and operations.
4. ITSD Systems, Web and Graphics Division (Systems Development)
  - Establishes and maintains standard processes in the development, testing and maintenance of the various application system (*i.e.*, SLDC) in coordination with the various units of PCSO.
  - Ensures that the test process (*i.e.*, system test, QA test, UAT, parallel run) of new application system is effectively carried out.

- Performs the necessary QA tests on newly developed and revised systems.
- Leads in the development and execution of tests for application systems such as access and system penetration test, capacity/peak, stress and regression tests.
- Develops and practices version control for users and support trainings.
- Provides resource materials for users and support trainings.
- Manages awareness-training and orientation programs for PCSO employees relative to the implementing guidelines
- Develops the application system based on user specifications and on the industry's best practices and SLDC.
- Performs a comprehensive and well-documented system test on newly developed or revised application system.
- Coordinates with various users regarding any issues in the development or change in the application system.
- Develops and practices version control procedures for all application systems.
- Develops and maintains procedures for the design, testing, operation, maintenance and documentation of operational and program source libraries and databases.
- Participates in discussion on application system and database development related to information security.
- Develops and performs a security test plan for security tests on application system and database, such as access and system penetration tests, capacity/peak, stress and regression tests as part of UAT.
- Acts as custodian for source codes and other related documents.

#### 5. Risk Manager

- Performs overall operational risk oversight

### **Violations**

PCSO personnel are expected to hold in strictest confidence information and data relating to business plans and marketing strategies and systems as well as proprietary or other confidential information that they may acquire in the course of their employment.

Care shall be taken to ensure the security of papers and computer files, information and records, including data, programs and vendor software. No one shall attempt to access data, systems, physical documents, and physical areas to which he or she is not authorized.

The obligation to safeguard confidential information shall continue even after the employees leave PCSO (*Republic Act No. 6713 Section 7*).

Users who violate these implementing guidelines shall be subject to the sanctions stipulated in the Code of Conduct and Ethical Standard for Public Officials and Employees (*Republic Act No. 6713 Section 11*).

#### **Additional Provision:**

*The System, Web and Graphics Division shall be responsible in the development and maintenance of the in-house application system and also acts as the Agency counterpart for outsourced applications. In both cases, the System, Web and Graphics Division and any ITSD personnel for that matter shall not be responsible in the encoding or entering of data to be used in the application/s to be developed. Encoding of data and the correctness of information to be encoded shall be the responsibility of the concerned department/end-user of the application.*