PROGRAM TITLE

IT SOLUTIONS

PROCESS TITLE

Hardware and Software Maintenance

1. SCOPE

This policies and procedures manual establishes policies, systems, procedures and controls on the Hardware and Software Maintenance. All duties and responsibilities stated in this manual are not exclusive to the personnel’s designated responsibilities in this process title.

1. OBJECTIVES

* To ensure that hardware components are properly maintained, secured and accounted for.
* To make sure that software are licensed, documented and secured.
* To ensure that maintenance of hardware and software is properly done and documented.
* To ensure that backup procedures are reliable and in place.
* To clearly define the duties and responsibilities of all personnel involved in this process title.

1. PERSONNEL INVOLVED
   1. Department Supervisor / Staff
      1. Initiates/Receives the requisition for password.
      2. Fills-out the IT Request, Assessment and Acceptance Form (IRAAF).
      3. Forwards the following:
         * Duly filled-out IRAAF to Department Manager for verification;
         * Duly filled-out and verified IRAAF to IT Supervisor for assessment.
      4. Accepts password and signs “accepted” portion of the IRAAF.
   2. Department Manager
      1. Receives the duly filled-out IRAAF from Department Supervisor/Staff.
      2. Verifies the duly filled-out IRAAF.
   3. IT Supervisor
      1. Receives the following:
         * Duly filled-out and verified IRAAF from Department Supervisor/Staff;
         * Duly approved IRAAF from IT Manager;
         * Resignation/Termination Checklist (RTC) from employee.
      2. Assesses the duly filled-out and verified IRAAF.
      3. Updates the system and gives to designated employee the password and system access.
      4. Updates the system for the deactivation of employee’s password and system access and signs the RTC.
      5. Forwards the following:
         * Duly filled-out, verified and assessed IRAAF to IT Manager for approval;
         * Forwards the duly signed RTC to employee after updating the system.
      6. Files IRAAF chronologically.
   4. IT Manager
      1. Receives duly filled-out, verified and assessed IRAAF from IT Supervisor.
      2. Approves the duly filled-out, verified and assessed IRAAF.
      3. Forwards duly approved IRAAF to IT Supervisor.
   5. Employee
      1. Forwards to IT Supervisor the RTC.
      2. Receives duly signed RTC from IT Supervisor.
2. KEY TERMS
   1. *Hardware* – is the physical aspect of computers, telecommunications, and other devices.
   2. *Software* – is a general term for the various kinds of programs used to operate computers and related devices.
   3. *Copyrights* – is a legal right created by the law of a country that grants the creator of an original work exclusive rights for its use and distribution.
   4. *Backup* – is the saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
   5. *Bug* – an error, flaw, failure or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.
   6. *GUI or graphical user interface* – is a type of user interface that allows users to interact with electronic devices through graphical icons and visual indicators such as secondary notation, instead of text-based user interfaces, typed command labels or text navigation.
   7. *Interface* – is a set of commands or menus through which a user communicates with a program.
   8. *Bit* – is a basic unit of information used in computing and digital communications.
   9. *Data* – is an information processed or stored by a computer.
3. POLICIES
   1. **General**
      1. The IT department shall be responsible on the overall maintenance of the Company’s hardware and software assets. However, each personnel and department heads are responsible in taking care of the hardware and software under their custody.
      2. The IT department shall prepare a schedule of hardware and software maintenance taking into consideration the activities of the departments so as not to interrupt the operations.
      3. The IT department should observe good housekeeping and maintain cleanliness of during and after maintenance.
   2. **Hardware Maintenance**
      1. The IT department should conduct a preventive maintenance on all IT hardware which includes the following (at a minimum):
4. Cleaning of CPUs and Servers to avoid dust and rust;
5. Checking of cables and routers;
6. Checking of computer performance;
7. Testing
   * 1. All requests for repair should be covered with IT Request, Assessment and Acceptance Form (IRAAF).
   1. **Software Maintenance**
      1. Software programs should be properly maintained. The following are the four (4) kinds of software maintenance:

|  |  |
| --- | --- |
| **Type** | **Description** |
| Corrective | Corrective maintenance is concerned with fixing errors that are observed when the software is in use. This may include bug fixes due to a bad code, or a major system repair if the problem is advanced. |
| Adaptive | Adaptive maintenance is concerned with the change in the software that takes place to make the software adaptable to new environment such as to run the software on a new operating system. |
| Perfective | Perfective maintenance is concerned with the change in the software that occurs while adding new functionalities in the software. It can simply range from changing the GUI of the software to make it more attractive and user friendly to making drastic changes in the core code to improve the runtime and performance. |
| Preventive | Preventive maintenance involves routine checks and tests to prevent software problems and errors (i.e. defragmentation, disk check, full virus scan, etc.). |

* + 1. All Company computers should be installed with anti-virus/malware programs.
    2. The Company should only install licensed third party programs/applications.
    3. User departments should not be allowed to install any third party programs/applications without the consent of the IT department.
    4. Requests for software repairs, installation and modification shall be duly supported with an approved IRAAF and endorsed to the IT department.
    5. The IT department shall ensure that Company computers are installed with the latest updates on its Operating Systems and applications (i.e. Microsoft Office, virus scanners, etc.)
  1. **Password and Security**
     1. System programs or electronic devices should be duly secured with a password.
     2. Only authorized employee with approved written request (i.e. IRAAF) will be given password and access to the system.
     3. Each password should be unique. Presented below are some guidelines to enforce the use of secure passwords:
        + Passwords must have at least six (6) characters;
        + Passwords cannot contain the user name or parts of the user’s full name (i.e. first name, middle name, last name);
        + Passwords must use at least three of the four available character types (i.e. lowercase letters, uppercase letters, numbers, and symbols).

The IT department shall educate the users on how to make strong passwords.

* + 1. Passwords shall be changed quarterly or at least semi-annually.
    2. Any changes on the access rights/functions by an employee should be duly supported with approved written request (i.e. IRAAF). Moreover, the change on the access rights/functions should take into consideration the segregation of duties (at a minimum) “approval”, “custody”, and “recording”.
    3. Resigned/terminated employee’s account must be **deactivated** on or before the day of effectivity of resignation/termination. However, the HR manager or senior management, for justifiable reason, may advise the IT department to deactivate the accounts of certain employees.
    4. Desktop log-in password should be established in all computers or other Company’s facilities to prevent unauthorized access.
    5. An employee should present and endorse a duly approved written request (i.e. IRAAF) to IT department in case of forgotten passwords in software/system that does not have automated **Forgot Password** functionality.
  1. **Backup Systems** 
     1. The IT Department is responsible in designing a comprehensive and reliable backup systems.
     2. A backup of the Company’s data should be done for archiving and prevent loss of information due to hardware failure, virus/hackers, theft, etc. See system design for the backup and restore procedures under process title of “*Webpage and System Development”* Annex A*.*

The following are the three (3) kinds of backup:

|  |  |
| --- | --- |
| **Type** | **Description** |
| Full backup | Total copying of a complete dataset to a last bit. |
| Partial backup | Copying only data changed after the last backup. There are two kinds of partial backup as follow:   * *Incremental backup* – copying only data changed after the last incremental backup; * *Differential* – copying only data changed after the last full backup. |
| Mixed backup | A sequence of full backup and some differential backups, rotating repeatedly. |

* + 1. Data backup should be done regularly. The importance of the data should be considered in setting the frequency of the backup (i.e. daily, weekly, monthly, quarterly, semiannually, annually).
    2. Aside from the backup in computer hard drives, offsite backups should be maintained.
  1. **Flash drive Usage**

1. Flash drives are strictly prohibited to be used in any of the company's computing device. Sharing/transmitting of data files should be done in the company's own cloud based file storage system.
2. In the case that a flash drive is needed, a company issued flash drive will be provided by the IT department supported with a duly approved written request (i.e. IRAAF).
3. Flash drives should be scanned for viruses/malwares before usage.
4. PROCEDURES

| Password and System Access Requisition | | | |
| --- | --- | --- | --- |
| Step No. | Activity | Personnel  Involved | Business  Forms |
| 1 | Initiates/Receives the requisition for password. | Department Supervisor / Staff |  |
| 2 | Fills-out the IT Request, Assessment and Acceptance Form (IRAAF). Forwards duly filled-out IRAAF to Department Manager for verification. | Department Supervisor /  Staff | Duly filled-out IRAAF |
| 3 | Receives from Department Supervisor/Staff the duly filled-out IRAAF. | Department Manager |  |
| 4 | Verifies the duly filled-out IRAAF. | Department Manager | Duly verified IRAAF |
| 5 | Forwards to IT Supervisor the duly filled-out and verified IRAAF. | Department Supervisor / Staff |  |
| 6 | Receives duly filled-out and verified IRAAF from Department Supervisor/Staff. | IT Supervisor |  |
| 7 | Assesses the duly filled-out and verified IRAAF. | IT Supervisor | Duly signed “assessed by” portion of IRAAF |
| 8 | Forwards duly filled-out, verified and assessed IRAAF to IT Manager for approval. | IT Supervisor |  |
| 9 | Receives duly filled-out, verified and assessed IRAAF from IT Supervisor. | IT Manager |  |
| 10 | Approves the duly filled-out, verified and assessed IRAAF. | IT Manager | Duly approved IRAAF |
| 11 | Forwards duly approved IRAAF to IT Supervisor. | IT Manager |  |
| 12 | Receives duly approved IRAAF from IT Manager. | IT Supervisor |  |
| 13 | Updates the system and gives to designated employee the password and system access. | IT Supervisor |  |
| 14 | Accepts password and signs “accepted” portion of the IRAAF. | Department Supervisor / Staff | Duly accepted IRAAF |
| 15 | Files the IRAAF chronologically. | IT Supervisor |  |

| Password and System Access Deactivation | | | |
| --- | --- | --- | --- |
| Step No. | Activity | Personnel  Involved | Business  Forms |
| 1 | *(During the processing of the employee’s exit clearance)*  Forwards to IT Supervisor the Resignation / Termination Checklist (RTC). | Employee |  |
| 2 | Receives RTC from employee. | IT Supervisor |  |
| 3 | Updates the system and signs the RTC. | IT Supervisor | Duly signed RTC |
| 4 | Forwards the duly signed RTC to employee after updating the system. | IT Supervisor |  |
| 5 | Receives duly signed RTC from IT Supervisor. | Employee |  |

1. FLOWCHARTS





1. EFFECTIVITY

This Policies and Procedures Manual shall take effect upon approval and shall supersede any memorandum/SOP inconsistent with this Policies and Procedures Manual. Any changes to the manual shall comply with the policies and procedures indicated in the process title *“Amendment of Manual”*.

**ANNEX**

ANNEX A

Hardware Preventive Maintenance Guidelines

1. If electronic devices are used for how many hours at a time during the day, then plan to restart it at least once. This way, temporary files would not build up and slow down use over time.
2. Never leave electronic devices on overnight, unless necessary, either to save electricity and to prevent wear-and-tear.
3. Always turn off and unplug the system before cleaning any of its components. Never apply any liquid directly to a component. Spray or pour the liquid on a lint-free cloth, and wipe the electronic device with the cloth.
4. Wipe the case and clear its ventilation ports of any obstructions. Keep all cables firmly attached to their connectors on the case.
5. Turn the keyboard upside down and shake it to clear the crumbs from between the keys. If that does not suffice, blast it (briefly) with compressed air. If the keys stick or keyboard is really dirty, pry the keys off for easier cleaning.
6. When blowing the equipment with air, pay attention not to push the dust under the electronic components (resistors and capacitors), because this could worsen the problem. Additionally, ensure that the air pressure is not so high that it damages the electronic components.
7. Clean the screen with a standard glass cleaner and a lint-free cloth.
8. Gently wipe each disc with a moistened, soft cloth. Use a motion that starts at the center of the disc and then moves outward toward the edge. Never wipe a disc in a circular motion.
9. Keep the door closed during maintenance operations to prevent the dust from entering inside room.
10. Only skilled operators should clean the equipment.
11. User departments are not allowed to repair hardware components. Whenever there are errors/malfunction noted, the IT department should be communicated for checking and repairs.
12. User departments should avoid placing beverages on top or near the computers.
13. User departments should take care of the computers and electronic devices under their custody by keeping it clean, well-ventilated and ensure that it is properly shutdown.