Information Technology Policy

Information & Communication Technology Department

Edition 1 rev. 2

Information Technology Policy

Activity	Name	Designation
Prepared By	Mr. Adeel Yousfani CISSP	Deputy General Manager (DGM)
Review & Checked By	Mr. Syed Ahmed Faraz	General Manager (GM)
Approved By	Mr. Khalid-ur-Rehman Barlas	Chief Information Officer (CIO)

Information Systems infrastructure at the Pakistan International Airlines (PIACL) underpins Service delivery capability today. The PIACL will continue to leverage technology solutions to introduce innovative services, while maintaining a sound and secure market image. As such, the security, reliability and integrity of the underlying Information System infrastructure is of vital importance for continued successful operation.

The Corporation "Information Systems Policy" sets out the principles and standards to be applied for secure and effective management of the PIACL Information Systems environment.

All PIACL personnel are responsible for protecting the PIACL information, data, software and hardware according to its proprietary nature, sensitivity, and importance for the Corporation. All personnel must ensure that they:

- Are aware of their responsibilities;
- Comply with the requirements; and
- Report suspected violations, to appropriate authorities on a timely basis.

The IT Policy document, along with future updates, will be available through internal web & Corporation e-mail for easy reference by all PIACL staff.

Khalid-ur-Rehman Barlas

Chief Information Officer

Revision Records

Rev #	Issue Date	Policy Name	Page #
Rev 01	**01 June, 2020**	**6.3 User Access**	**27**
Rev 01	**01 June, 2020**	**6.4 Segregation of Duties**	**28**
Rev 01	**01 June, 2020**	**6.14 Incidents Management Policy**	**38**
Rev 01	**01 June, 2020**	**11.1 Hardware Purchasing, issuance & Identification**	**63**
Rev 01	**01 June, 2020**	**11.8 Emergency Change Control**	**70**
Rev 01	**01 June, 2020**	**12.1 Service Level Agreements (SLAs)**	**71**
Rev 01	**01 June, 2020**	**14.1 IT Help Desk Management**	**74**
Rev 02	**10 December, 2020**	**Documentation & Updates**	**8**
Rev 02	**10 December, 2020**	**6.3 User Access**	**27**
Rev 02	**10 December, 2020**	**6.13 Passwords**	**38**
Rev 02	**10 December, 2020**	**9.1 Backup Plans**	**58**
Rev 02	**10 December, 2020**	**15. Capacity & Performance Management Policy**	**75**

Table of Contents

Introduction

Information processing systems in Pakistan International Airlines Corporation Limited (PIACL) is the basis for most of the client information, processes and record keeping, legal needs, etc. As such security, reliability and integrity of the data, software, firmware, hardware, and cloud are of vital importance to PIACL's continued operations.

The policies and standards contained herein apply to any entity who access information by any means.

Policy Objective

The "PIACL Information Technology Policy" set out the principles and standards to be applied to the management of PIACL's Information Technology environments and maintenance of security controls.

The policies and standards are also designed to assist in the delivery of appropriate levels of availability and reliability of systems and information.

The specific objectives of the "Information Technology Policy" are:

- To prevent unauthorized access, disclosure, modification, manipulation or destruction of PIACL's Information processing components; Software, hardware, firmware, cloud.
- To ensure physical and logical security controls are properly implemented and managed;
- To ensure data / information / system / application owners are aware of their respective responsibilities with regard to system security; and
- To achieve adequate control and management of Information Technology resources in a cost effective and efficient manner.

Structure

PIACL’s Information Technology Policies and Standards are structured as follows:

- Broad policy statements of principle or intent that describe how to achieve the objectives, and;
- Standards for each policy covering statements, conduct, courses of action or responses to a given situation.

Scope / Coverage

These policies and standards cover information technology environments; production, recovery and test / development sites, Software as a Service (SaaS), Infrastructure as a Service (IaaS), cloud deployments, etc. Assets secured include information, data, software, hardware, Firmware, and communications network devices owned/ operated/ used by the Corporation.

These assets may be owned by the PIACL, leased, hired, developed in-house or purchased, and include all devices along with the interconnecting network devices.

Services covered include those that may be:

- Contracted out (“out-sourced”) to other parties, but operated for PIACL; and
- Contracted in (“in-sourced”) from other parties, and operated on behalf of the Corporations’ customers/ clients.

Information Technology Policies and Standards apply to all people within the Corporation, which includes all staff, contractors, consultants and agents engaged by or for PIACL (described in this text as “personnel”).

External Parties (that are not operated by PIACL) but connect to PIACL systems will be responsible for the security of their own IT environment. Such parties will not claim any damages against PIACL in case of system attacks occurring when connected to PIACL systems. Where deemed necessary, those third parties will allow Corporation Internal Audit / IT Department to perform an independent verification or audit of their computer systems.

Where PIACL owns a company jointly with other shareholders, Information Systems Security controls to be applied on the processing systems of that company will be determined by representatives from PIACL and the other stakeholders.

Authority

PIACL Information Technology Policies & Standards is issued under the authority of the President & CEO of PIACL and must be used in conjunction with other environment-specific standards.

Responsibility

All PIACL personnel, whether they are the creators, keepers or users of the Corporation's information assets, must ensure that information, data, hardware, software, firmware is protected according to its sensitivity, proprietary nature and importance to the Corporation.

All personnel have responsibility for safeguarding PIACL’s information, data, software and hardware.

It is the responsibility of all personnel to ensure that:

- They are aware of their responsibilities;
- They comply with the requirements of these policies and standards; and

- Violations or suspected violations of these policies and standards are reported to appropriate authorities on a timely basis.

Application

To each person whom work involves the direct or indirect use of PIACL's Information Systems; these systems are invaluable. PIACL information processing systems represent an important proportion of the Corporation's assets. They therefore must be protected from either accidental or pre-meditated damage.

PIACL intends to ensure that the practical application of such security precautions is based on sound business judgment, the value of the system being protected and the risk associated with the system.

The Corporation will implement these security precautions to ensure:

- People who need to use Information Processing Systems have the necessary access to accomplish their duties;
- There is efficient back-up and speedy recovery in the event of loss of systems, hardware, information or data within defined business requirements; and
- People understand their obligations and personal responsibility flowing from the use of Corporation information and data.

Violation

Violations of Corporation's Information Technology Policies and Standards include any act which:

- Involves the unauthorized use, or disclosure of confidential Corporation information, data, hardware, firmware or software;
- Involves the use of the hardware, software, firmware, information or data for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body; and
- Exposes the Corporation to actual or potential monetary loss through the compromise of Security Systems and Procedures.

Failure to comply with or violation of the Corporation's Information Technology Policies will be dealt with according to the range of actions prescribed for such breaches. Such action may include:

- Suspension;
- Termination of employment or termination of contractual arrangements;
- Civil or criminal prosecution; and
- Any other appropriate disciplinary actions.

Any violation, or suspected violation, should be reported through the Department / Business / Branch Unit where it is observed, to the Manager, PIACL IT Department, at Risk Officer who will conduct further investigations as deemed necessary and recommend appropriate disciplinary action to Senior Management / HR, as appropriate.

Documentation & Updates

This Corporation Information Systems IT Policy document is developed and maintained by Corporation Chief of IT Department. The IT Policy document would be reviewed at least once a year, for possible amendments / revisions, by the competent authority.

For all Work Instructions gathered / compiled for during the period, in consultation / coordination with the respective users, would be put up before the competent authority such as the “IT Steering Committee”.

Appropriate amendments in the document would also be incorporated corresponding to the Changes in the global Information Systems Security arena. Any clarifications or update suggestions regarding this document should be referred to the Chief of IT Department.

Environment Specific Standards

In addition to these Policies & Standards, other control requirements, covered in environment-specific Corporation standards such as those listed below will also be implemented.

- PIACL Logical Access Security Standards.
- PIACL Public and Private Cloud Security Standards.
- PIACL System/network Security Standards.
- Corporation Cryptographic Systems Security Standards
- Corporation Operating System Security Standards.
- Corporation Database Security Standards
- Corporation Virus Control Security Standards (covers computer virus / malicious code control standards)

1. Systems Security Organization Policy

Policy	**1.1 Security Organization**
Objective	To provide adequate guidelines to support implementation and operation of a secure information processing environment throughout PIACL.
Standards	**1.1.1** A Corporation-wide Information Systems Security function will be established and will be responsible for: (a) Articulating, amending and implementation of policies and standard relevant to security of the System. Establishment and rectification of Information Technology Security Policies and Standards. (b) Promotion of Systems Security awareness and its importance to the Corporation. **1.1.2.** The Systems Security function will report to Chief of IT Department.

Policy	**1.2 Management Responsibility**
Objective	To ensure management is aware of their responsibilities regarding development of appropriate security practices and the implementation of PIACL Information Technology Policies and Standards.
Standards	**1.2.1** Managers will be directly responsible for: • Ensuring that all Personnel reporting into them (either directly or through sub-ordinates) are aware of their obligations to safeguard PIACL information processing resources; and • Enforcing the Information Technology Policies & Standards (as set out in this document and other environment-specific documents) in their respective areas. **1.2.2.** Line management will ensure that security incidents / violations are reviewed and actioned on a timely basis. **1.2.3** When a person's services to PIACL ceases for any reason, their systems access rights are to be terminated as soon as possible and the appropriate security and personnel records adjusted accordingly. The manager / supervisor will be accountable for the completion of the appropriate systems security adjustment requests in their respective areas. Further he/she should also return all confidential material/information/data etc. **1.2.4** All Business Unit Heads/ Senior Managers must confirm to the Office of the CEO that: • Staff under them have read and understood current Corporation Information Technology Policies and Standards; and • They will ensure that their respective areas comply with Corporation Information Technology Policies & Standards (ref. Table 1, Item 1).

Policy	1.3 User Responsibility
Objective	To ensure that PIACL Information System resources are safeguarded, properly maintained and utilized in the most efficient way possible.
Standards	**1.3.1** Users must ensure that information and data are used solely for purposes specified and consented by the information / data owner. **1.3.2** Users are required to use PIACL Information System resources for legitimate business purposes only except where explicitly authorized otherwise. **1.3.3** Users shall ensure that information and data owner accessible to the user shall not be disclosed or transferred to any third party.

Policy	**1.4 Deviations (Waivers)**
Objective	To incorporate control to govern administration of deviations from approved Systems Technology Policies / Standards.
Standard	**1.4.1** Deviation from approved Information Technology Policies and Standards will require written approval by Chief of IT Department. The Chief of IT shall not accept any request that may conflict with any applicable laws. **1.4.2** Each IT policy / standard deviation request must provide: • The business case of the Business Unit / Information Technology Department / Project Team / Unit Head justifying the request; • The estimated date by which the deviation is to be regularized (where applicable); • Risk mitigating controls; and • Where applicable, a process to ensure continued monitoring of the potential risk associated with the deviation.

2. Security Awareness Policy

Policy	**2.1 Security Awareness Programs**
Objective	To increase awareness of information systems security features within PIACL and create an environment with sound computer security practices.
Standards	**2.1.1** All personnel should undergo appropriate ongoing computer security awareness programs to be able to understand potential threats to PIACL's Information Systems and their specific systems security responsibilities and to timely report the same to the relevant department for rectification. **2.1.2** Sectional Heads are responsible for ensuring their staff is informed and understand all IT policies and standards, changes made to them from time to time and to ensure staff attendance at appropriate awareness training courses. **2.1.3** HR Department will ensure that security awareness programs are available for all PIACL personnel and security awareness programs be included into JMC, MMC, SMC courses.

Policy	**2.2 Use of PIACL Policies and Standards**
Objective	To ensure that personnel are aware of the appropriate procedures required when carrying out their roles and responsibilities using information processing resources.
Standards	**2.2.1** All new personnel must have access to the most recent Corporation Information Systems IT Policies and Standards. **2.2.2** New personnel should acknowledge (in writing) to Human Resources Department that he / she has read, understand and will comply with these policies and standards. **2.2.3** Please include internal certifications that shall be acquired by personnel especially those whose job description includes use/access and processing of information data. Such certifications shall be in tiers and accorded after crash courses relevant to each tier.

3. Human Resources Policy

Policy	3.1 Personnel Practices
Objective	To ensure that all Personnel are aware of the requirement of, and the obligations to PIACL IT Policies, Standards and Practices.
Standards	**3.1.1** Employee's chronic problems in adhering to Information Technology policies and standards will be considered during the performance evaluation process. **3.1.2** All information resource users have a responsibility to ensure the security and integrity of information and equipment and must comply with the Corporation's Information Technology Policies and Standards. Individuals will be held accountable for their usage of PIACL information processing resources. Non-compliance or violation of these Information Technology Policies & Standards will result in action that may include, but not be limited to, the following: • Suspension of employment; • Termination of employment; • Other disciplinary action; and / or • Civil and / or criminal prosecution. **3.1.3** Sanctions against contract employees will be in accordance with the terms of their contract.

4. Workstation / End User Device Policy

Policy	**4.1 End user Device Purchasing**
Objective	Only IT related device that comply with PIACL standards will be purchased or leased.
Standards	**4.1.1** The Devices will be purchased or leased through approved suppliers. **4.1.2** Only Devices that comply with PIACL standards will be included on PIACL approved device list. **4.1.3** All requests for end user Devices must be sent to Information Technology management who will arrange for acquisition and installation.

Policy	**4.2 User Training**
Objective	To ensure all users are sufficiently productive by having been adequately trained in: • The use of Hardware and Software; • The functionality of their equipment and Software; and • Best practices.
Standards	**4.2.1** Appropriate training courses are to be scheduled for all users to enable them to understand and use their devices and applicable application software efficiently and effectively. **4.2.2** Training Courses to be scheduled prior to the issuing of equipment or software, or as near as possible to the date the equipment is received. **4.2.3** Business Units/ Sectional Managers will ensure that staff is adequately trained in respective systems / Project Teams / Information Technology Department etc. **4.2.4** Users shall be required to pursue appropriate certifications based on use/access and processing of information data for the purposes of their job. Such certifications shall be in tiers and accorded after crash courses relevant to each tier.

Policy	**4.3 Device Security**
Objective	To ensure that access to the device and the associated network components is restricted to authorized personnel.
Standards	**4.3.1** Network ports (data points) installed in PIACL areas accessible to public / customers must be configured to provide connectivity to devices specified by the IT department only. **4.3.2** Logical access to any PIACL terminal will be restricted to Corporation's personnel or authorized consultants or technicians. **4.3.3** Sensitive information (such as customer profile information, financial data, vendor contracts, corporate level strategic plans, litigation strategy memos, etc.) must not be stored in the user Devices. **4.3.4** If a Device holds sensitive work-in-progress information, power-on and screen saver passwords will be used to restrict access to the authorized user(s) only. Where power-on passwords are enabled, the passwords must be recorded, sealed and kept by the respective Unit Managers. **4.3.5** Production workstations (in local operations, centralized operations, etc.) must not have active floppy / CD drives / USB/ external storage (this excludes general-purpose office workstations and laptops). **4.3.6** All standalone PCs, laptops, devices, etc. must be turned off when the assigned user leaves PIACL premises at the end of the day.

5. Software / App Security Policy

Policy	**5.1 Authorized Software/App**
Objective	To ensure that all software / Application in use in PAICL's is authorized, appropriate and fully tested.
Standards	**5.1.1** Corporation's Information Technology Department shall maintain an updated list of approved software. **5.1.2** All software used must be clearly defined / documented to reflect its purpose, developer, version number etc. **5.1.3 Chief of Information Technology** to review and recommend software to the Corporation for inclusion / deletion from the approved software list. **5.1.4** The Evaluation / demo software will not be installed on PIACL information processing systems without approval from the IT Department.

Policy	**5.2 Software / App Acquisition**
Objective	To ensure that only software/App that complies with PIACL Standards is approved, purchased or leased.
Standard	**5.2.1** All requests for software acquisition must be sent to IT Helpdesk who will arrange for acquisition and installation with the approval of Chief of IT. Once purchased, the User Acceptance Testing (UAT) will be performed and then Software will be installed and commissioned for production processing without any delay. **5.2.2** Appropriate corporate software licenses must be obtained (where possible) for all PIACL products. **5.2.3** All software used within PIACL must be supported by a standard maintenance agreement. **5.2.4** All software must be maintained in accordance with the suppliers' maintenance agreements. **5.2.5** Where software must be purchased without a supplier's maintenance agreement, approval shall be obtained from Chief of IT, prior to its purchase.

Policy	**5.3 Access To Software / App**
Objective	In order to maintain the integrity of PIACL systems, access to production application Software and system software libraries must be restricted to authorized users.
Standards	**5.3.1** All software must be protected from unauthorized or accidental access as per the protection mechanism devised by the IT department and the Chief of IT. **5.3.2** In Inappropriate use, such as attempted access or unauthorized usage of software (including system utilities), must be escalated to IT Department by User manager / Supervisor **5.3.3** All installed / non-installed software must be maintained in a secure manner. This requirement is also applicable when the software is not in use and when changes to the software are being made.

Policy	5.4 Software/ App Modification
Objective	To ensure that changes are implemented in a controlled manner and that they do not affect the integrity of information and data.
Standards	**5.4.1** All changes / modification of software must be performed via the approved change control mechanism. **5.4.2** New releases of software must be documented in accordance with Corporation documentation guidelines. **5.4.3** New releases / fixes of software/App and in-house changes to system / application software/App must be fully tested in a test / development environment prior to implementation in the production environment. **5.4.4** Prior to any amended software version, releases / vendor supplied fixes, etc. going into production environment, IT Department and / or the end user (or their designates) must review the associated documentation to ensure that the documentation accurately reflects the modified status of the software. **5.4.5** At least three previous versions of the software, related documentation & user ids / passwords, must be available to enable recovery in the event that the new release or modification fails. **5.4.6** Systems development plus all modifications will be performed and tested in secure testing / development environments. **5.4.7** "Live‟ production data will not be used in the test / development environment without authorization by data / information / system / application owner and IT Department. **5.4.8** Where justified, production data used in the test / development environment will be stored on properly secured machines (security corresponding to that implemented on production machines).

Policy	**5.5 Database Management Systems**
Objective	To ensure that database management systems are appropriately maintained and provide data integrity, availability and confidentiality.
Standards	**5.5.1** The database administrator must ensure that all modifications and fixes to the Data Base Management System are appropriate to the installation's requirements and appropriately authorized by End user. **5.5.2** All modifications and fixes to the DBMS must be tested to ensure that they function properly prior to being transferred to the „live‟ production environment. **5.5.3** Operation and systems documentation must be updated for all changes to the DBMS. **5.5.4** Logical views of the database (e.g. subschemas) must be fully documented and kept updated. **5.5.5** DBMS audit trails and logging options must be selected such that, in the event of failures, the database can be recovered without loss or corruption of data.

Policy	**5.6 Software Storage**
Objective	Original Software and backup storage media should be securely stored so as to enable full recovery of the installed Software in the event of a hardware malfunction or disaster.
Standards	**5.6.1** Media containing original / backup software will be stored in environmentally-controlled lockable storage areas. **5.6.2** An updated inventory of all Software media will be maintained. The inventory will contain details of all software purchased or leased. The record shall include but not be limited to: • Software license No.; • Workstation / PC / Server installed; • Software title and version; • Date installed; • Software purchased / leased; • Lease expiry date; • Vendor; and • Maintenance Agreement Conditions. **5.6.3** The software inventory register will be reconciled with the installed software base (ref. Table 1, item 3). **5.6.4** Physical and logical security controls over access to backup copies of vital records and data held in an offsite storage location will provide the same level of protection as these provided at the on-site storage location.

Policy	**5.7 Software Disposal**
Objective	To ensure that all software is disposed of appropriately and unauthorized users do not gain access to information and data.
Standards	**5.7.1** Retired software must be erased from the storage media to make the media non-readable prior to disposal (ref. Table 6, Item 2). **Note:** • A secure deletion method for storage media is one that actually wipes the physical area of storage irreversibly rather than simply removing the disk directory reference to that information. • Care must be taken in disposing of information to ensure that it is no longer required for any audit, legal or compliance purposes. **5.7.2** Chief of IT will authorize disposal / replacement of all system software and appropriate 2details will be recorded in the software inventory register. End users will decide when an application software should be replaced / retired.

6. Information / Data Security Policy

Policy	6.1 Data / Information System / Application / Device Ownership
Objective	To ensure ownership responsibility is assigned for all information / data held in production or test / development systems.
Standards	**6.1.1** All information, systems and applications must have an identified information / systems / applications owner **6.1.2** The application owner can delegate resource responsibilities to a designate. However, the owner will have final responsibility over the resource integrity and security controls. **6.1.3** The information / system / application / device owner is responsible for authorizing changes / enhancements to information, device, business systems and applications that they own. **6.1.4** The information / system / application / device owner is responsible for ensuring that their Business Continuity Plan (BCP) includes the appropriate specification and testing requirements of Information Technology. **6.1.5** Infrastructure owners will be Information Technology Managers with expertise in the infrastructure they own. **6.1.6** Infrastructure owner's responsibility and accountability includes at least: • Application of Corporation Information Technology Policies and the relevant Information Technology Standards to that Infrastructure; • Monitoring vendor and industry vulnerability reports to enable swift application of patches / upgrades in response to known weaknesses; • Monitoring to ensure that actual and recorded configuration correspond; and • Ensuring that security logs are reviewed, intrusion alarms and other alerts are responded to within an acceptable time frame.

Policy	**6.2 Data / Information Systems / Application Classification**
Objective	To identify and classify Information, systems and Applications to ensure security is provided in accordance with the importance and sensitivity to the Corporation.
Standards	**6.2.1** All business data / information will be classified according to confidentiality, integrity and availability (ref. Appendix 1). • Confidentiality will be graded HIGH, MEDIUM or LOW; • Integrity will be graded HIGH, MEDIUM or LOW; and • Availability will be graded HIGH, MEDIUM or LOW. **Note:** Information / Data may be for Internal usage which shall be (marked "For Internal Use Only", such information shall include PIACL telephone directory, new staff training materials, internal policy manuals, source codes, system logs, etc.) or for "Public Usage" such information shall include product brochures, advertisements, job opening announcements, press releases etc. **6.2.2** An application owner must nominate the appropriate classification for their information / applications. System / Application will be classified as CRITICAL, IMPORTANT or LOW according to the information classification factor assigned by the data / information / system / application owner i.e. HIGH across confidentiality, integrity or availability means that the System / Application as a whole will be classified as CRITICAL. **6.2.3** All application systems must undergo a risk analysis during the initial phase to determine the overall classification. **6.2.4** Data / Information classification will dictate the level of control required to protect that data / information regardless of where it resides and the form it takes. Data / Information will be consistently protected throughout its life cycle, i.e. from its origination to its destruction. IT team / Risk officer will be responsible for determining this classification in conjunction with information / system / application owner. **6.2.5** Information / data confidentiality, integrity and availability control aspects will be implemented (ref. tables 2-3)

Policy	**6.3 User Access**
Objective	To ensure that only authorized users gain access to PIACL information systems, and consequently assure: • The confidentiality of sensitive information and data; • Preservation of the integrity of information and data against unauthorized manipulation, fraud and damage; and • The availability of this information and data for authorized day-to-day PIACL operations. .
Standards	**6.3.1** Access control features within system software /application must be used to control access to the information/data in a manner commensurate with its classification. In this connection, highly sensitive application / data must be accessed through multi-factor authentication and classification of application / data would be determined by user department with consultation of IT steering committee. **6.3.2** Authorized changes to user access rights must be actioned promptly. If Personnel no longer require the level of access they have been granted, it must be revoked, e.g. upon transfers. **6.3.3** The users who are unable to physically join the office due to situations like riots, natural disaster, pandemic, user's health issues, etc. will be facilitated to Securely access to systems, participate in the meetings and share the documents online from home. The work from home and access right permission will be granted through Line Manager and request will be sent to IT Department for the action. The duration of the permission must clearly be defined in the request by Line Manager. The access rights will be revoked on the request of Line Manager or upon the permission time expires. **6.3.4** Where users with access to highly sensitive information are terminated or have resigned from PIACL service, the employee's immediate manager / supervisor/ HR is responsible for directly coordinating the removal of that staff access rights in the systems and ensuring they abide by the confidentiality and non-compete clause in their service agreements. He/she shall also return all material that is provided by PIACL for the purposes of the job that may be considered Data/information/Hardware/Software **6.3.5** All access rights are to be suspended in the case of Personnel under suspension. **6.3.6** Any unauthorized transfer or copy or usage of company's data is a criminal offence and may lead to punishment or termination of service.

	6.3.7 All user accounts which are in active or dormant for 45 days shall be disabled. The reactivation of account request shall be passed through line-manager.

Policy	**6.4 Segregation Of Duties**
Objective	To provide adequate segregation of duties and ensuring that at least two individuals are responsible for the separate parts of any task to prevent error and fraud. Where segregation of duties are not possible, the adequate technical controls should be well placed.
Standards	**6.4.1** The information / system / application owner and HR will be responsible for ensuring that no single individual has the capability of executing a particular task/set of tasks. The segregation of duties (SoD) will ensure accountability as well as limit the ability of individuals to negatively impact the Confidentiality, Integrity, or Availability of the particular Information System. Following are some examples and samples of segregation of duties' requirements include (but are not limited to) the following: • Development and Administration; Separating of development of software and Administration of system. Allow the process to be followed in updating the code that is tested and reviewed. • Development and Operation; Separation of software development and the operation of related systems and services. Allow problems with software to be reported accurately and managed within the process. • DB and System Administration; separation of Database and system administration. Allow confidentiality and integrity of the system to be ensured and accounted for. • End users should not have access to production data except through the features and functions of the administrative applications; in particular, they should not have the ability to bypass or circumvent the applications' validation and audit procedures. • Functional users should not access or modify application code. • Access to system logs and system audits should be limited to the system security analyst, and all such access should be reviewed by the Chief / Head of IT. • Access to firewalls and other network security systems should be limited to the network security analyst, and all such access should be reviewed by the Chief / Head of IT.

Policy	**6.5 Logical Access**
Objective	To ensure that a user granted access to any system is uniquely defined, thus facilitating an effective audit trail of all user actions on all Information systems / applications.
Standards	**6.5.1** Prior to accessing any PIACL Information Processing System, the user must input some means of authentication which is unique (such as a user ID and a password). Such user id and password may be assigned by IT department. **6.5.2** All users must be validated against previously established access rights prior to being granted access to the system. **6.5.3** Access violation attempts must be assessed / reviewed and actioned by the reporting officer before a request is approved to enable (restore) a locked user profile.

Policy	**6.6 Access Control**
Objective	Access to production information / data files, application software and system software libraries should be restricted to authorized users only. Users will be granted access based upon the principle of applying the least privilege required for achieving their assigned job functions.
Standards	**6.6.1** Hardware / Software security controls must be installed / enabled and maintained to defined standards. **6.6.2** Changes to system parameters that define access controls must be subject to management authorization and subject to regular independent reviews. **6.6.3** Human Resources (HR) department to notify IT Department of personnel movements for appropriate action.

Policy	**6.7 Data / Information Accessibility**
Objective	To ensure production data/information is only accessed by the authorized system / application.
Standards	**6.7.1** All access to sensitive data and usage of powerful system utility programs, high-level system profiles etc. must be logged and audit trails generated must be subjected to independent review. **6.7.2** Access to system utilities by systems support staff must be restricted on an "as-needs" basis. **6.7.3** Sensitive data/information such as installed system configuration, network topology, etc. will not be disclosed to third parties without approval from Chief of IT Department or unless NDA (non-disclosure Agreement) is signed. **6.7.4** Update access to production data must only be by: (a) Application software; (b) Authorized utilities (c) Database administrator (for authorized activities).

Policy	6.8 Upload & Download Capabilities
Objective	To ensure that all information/Data up-loaded and downloaded between systems is transferred in a controlled manner and with an adequate audit trail of amendments made.
Standards	**6.8.1** Information and data upload and download facilities must only be available to users who have been granted the right by the relevant authority. **6.8.2** Access to all information and Data that has been held for upload, or that has been downloaded, must be restricted to users who are normally granted the right to access the information and data in the original environment. Sensitive business data / information must not be downloaded / stored in public work areas (e.g. Public server drives) or private systems. **6.8.3** All information / data up-loaded from a Device / PC must be secured by adequate audit trails and application controls. This may include a temporary receiving facility to verify the integrity of the information and data before releasing it to a "live‟ environment.

Policy	**6.9 Control Over Output**
Objective	To ensure that hardcopy printouts will be available to authorized users only and must not be amended prior to distribution.
Standards	**6.9.1** Documents will be classified as Highly Confidential, Confidential, For Internal Use Only, Private etc. (ref. Table 5). **6.9.2** Access to hard copy output containing sensitive PIACL information and data must be restricted to authorized recipients only. **6.9.3** Access to print spools must be restricted to department staff only and monitored **6.9.4** All document output must undergo a secure disposal process commensurate with their classification (ref. Table 6, Item 1).

Policy	6.10 Emergency Plans
Objective	To ensure that bypassing normal controls due to emergency situations does not affect the integrity of PIACL information / data.
Standards	**6.10.1** All actions that bypass normal access control procedures must be logged and reported for immediate review by the appropriate / designated reviewer. **6.10.2** Emergency amendments made to production systems/applications relevant to data shall must be retrospectively reviewed by the requisite Data/information owner. Data / information owner (or nominee) must retrospectively review all emergency amendments to production systems / applications.

Policy	**6.11 Use Of Sensitive System Utilities**
Objective	To protect Software, information and data from access / modification using unauthorized system utilities.
Standards	**6.11.1** All installed system utilities that may be used to alter information; data or software must be justifiable or authorized by Chief of IT Department. All alteration or changes made using such system utilities shall be recorded either electronically or manually. The utilities must be identified and documented. **6.11.2** Access to system utilities must be restricted to authorized Personnel in accordance with their job functions. **6.11.3** The system administrator (or designated reviewer) must review sensitive utilities usage. **6.11.4** All unnecessary sensitive utilities must be removed from production systems / applications.

Policy	**6.12 Computer Virus**
Objective	To ensure that information, data, and software are protected against viruses / malicious codes attacks.
Standards	**6.12.1** Anti-virus software must be installed on all Hardware devices but not limited to workstations, laptops, standalone PCs and servers to ensure PIACL's data / information and software is protected against virus / malicious code attacks.

Policy	6.13 Passwords
Objective	To ensure adequate password management controls are maintained throughout PIACL.
Standards	**6.13.1** Passwords should not be obvious or easy to guess and must be kept confidential. Passwords must: • Not be same as User ID. • Not contain words like PIA, PIAC. • Be minimum eight (08) characters long and contain (01) upper case letter and one (01) numeric and one (01) special character. • Have zero (01) day minimum age. • Have ninety (90) days maximum age. • Not be same as last two (02) passwords. • Be blocked after ten (10) failed sign-in attempts and unlocked after 30 minutes. **6.13.2** User profiles, passwords will not to be disclosed to anybody other than the profile holder. **6.13.3** The Passwords of privileged or administrators accounts should be stored in secure electronic vault.

Policy	**6.14 Incidents Management Policy**
Objective	To identify incidents, characterize the nature and severity of those incidents, record the incident and provide immediate diagnostics and corrective action.
Standards	**6.14.1** PIACL systems will be configured to trigger IT incidents to the line management and/or to designated personnel/section in the Corporation. Incidents arising from user activity (such as policy / standards violations) will be reported to the line management. **6.14.2** Incidents will be documented and classified as either Critical, Major or Minor. **Note**: "**Critical"** incidents include intentional/highly impacted incidents that are likely to cause adverse effects Corporation wide and disrupts the business. These incidents will be escalated to the Chief/Head of IT through the line management. **"Major"** incidents are urgent that require team to act quickly to resolve the issue. These type of incidents may effect a large number of end user. The delay in resolution may also effect the business. These incidents will be escalated to the Chief / Head of IT through the line management. "**Minor" i**ncidents include all incidents that are not considered as serious as defined above. **6.14.3** The alert/warning recipient will record details of the incident as indicated below: • Nature of the incident; • System/records/facilities affected; • Likely cause of the incident; • Whether it was malicious or accidental (indicating if the incident is seemingly part of a routine job or it is an unusual set of circumstances); • Whether any possible motives (if malicious) are suspected; • The impact of the incident (operational, financial, reputation etc.); • Action taken to avoid escalation and further incidents; • The Process to recover from the incident; • To whom it has been escalated; • Whether the incident is classified as "**Critical"** or **"Major"** or "**Minor";** and

- The effects (if any), on other PIACL systems and services, to establish whether other end users need to be warned / advised.

6.14.4 Some incidents will be identified during applications / system / network activity reviews.

In addition, where staff believes that an incident has occurred, that incident must be reported to the line management for appropriate administrative action.

6.14.5 When an Incident is identified / suspected; the escalation /investigation process will include the following steps:

- Inform line management and/or designated personnel;
- Line Management and/or designated personnel and/or designated section to carry out initial investigations and if the incident did not occur take no further action;
- If the incident occurred line management to classify the incident ("serious" incidents to be reported to the Head/Chief of IT Department for investigations / guidance);
- The Incident must be recorded and service request must be generated.
- Chief of IT will constitute the Incident Response Team.
- Line Management to conclude investigations on minor incidents and take appropriate administrative action;
- IT Department, in consultation with the affected Unit's management to conclude investigations on "serious" incidents and decide / advise on the appropriate administrative action to be taken.

6.14.6 Based on the results of the investigations / analysis, the Incidence Response Team to determine the best way to restore the affected applications /systems / area including whether it is necessary to physically isolate the affected systems from the rest of the computing Response actions taken during an incident must be adequately documented for both technical and law-enforcement purposes.

6.14.7 Response actions taken during an incident must be adequately documented for both technical and law-enforcement purposes.

Note:

Technically, the documentation provides a basis for reviewing and improving both the computing infrastructure and the response procedures and for law enforcement; the documentation may provide a basis for assessing the impact of the incident and evidence in future litigations.

6.14.8 Line manages will take proactive action to ensure an incident does not recur by educating users to pay particular attention to controls derived from experience gained when handling previous incidents.

6.14.9 An incident will be closed:

- Once it is established that the incident did not actually occur;
- Due to lack of evidence or because of faulty evidence; and
- Once the incident is adequately resolved.

6.14.10 After closing the incident, a post-incident analysis will be performed for all “Critical/Major” incidents to record what was learned from the experience and, if necessary, update PIACL incident handling procedures.

- During the post incident analysis, the following details will be examined and recorded in the incident log:
- How the incident started
- How the response personnel became aware of the incident;
- How the incident was resolved;
- Whether existing procedures were adequate or require updating; and
- Lessons learned from the incident.

Note:

The post incident analysis team will include all Personnel, consultants, etc. who participated in the resolution of the incident.

7. Communication & Network Security Policy

Policy	7.1 Logical Network Connection
Objective	To ensure that all logical connections to PIACL network, whether local or external, are secured and that they are authorized.
Standards	**7.1.1** All network and other computing equipment (including servers, routers, multiplexers, front-end processors, etc.) will be installed in secured areas. **Note:** This network equipment must be placed in lockable rooms and cables connecting to this equipment must be protected (concealed) to prevent access by unauthorized persons. PCs, workstations, devices etc. must be placed on shelves / racks and not on the floors / carpets. **7.1.2** Records and diagrams, showing computer hardware attached to the network backbone will be maintained up-to-date. **7.1.3** Unused data ports (data points) will be kept in deactivated / disconnected state. **7.1.4** Logical access / connection to PIACL network will be granted with the approval of Information Technology Management. **7.1.5** Technical Testing and Risk Assessment must be undertaken for all requests to connect new equipment to the network before approval can be given. All equipment to be connected to the network (modems, routers, firewalls, etc.) must only be used in accordance with the findings of the tests/ risk assessment. **7.1.6** Business user profiles that utilize connections across different servers, etc. must be positively validated and the user must be restricted to the information and data they require for their job assignment. The Business Line Manager shall be responsible for validation of access provided and the term for such data access. **7.1.7** Secure VPN (virtual private networking) connection must be used to provide remote access to PIACL computing facilities. VPN users to be authenticated by user IDs and passwords. **7.1.8** Where justified, connection to test/production resources for third parties must be approved by the information/Data / application / device owner upon recommendations from the IT Department. **7.1.9** Third party activities performed over a VPN connection must be monitored and reviewed.

	7.1.10 There should be a signed Non-Disclosure-Agreement (duly vetted by legal department) before a VPN access is granted to external users. **7.1.11** Where feasible, end-to-end VPNs will be implemented rather than firewall-to-firewall VPNs. **7.1.12** VPNs connections are preferred rather than the dial up service. **7.1.13** All requests for non-standard external access must be evaluated via a risk assessment process, undertaken by team constituted by Chief of IT, to ensure that there is no potential risk to the Corporation. Based on the outcome of the risk assessment, the external access request will be approved by the relevant department head and IT Department.

Policy	**7.2 Network Access**
Objective	To ensure that only authorized users are granted access to PIACL network and that users are working in accordance with Information Technology Policies and Standards.
Standards	**7.2.1** All hosts that run applications or contain data that are non-public must be isolated behind a firewall from public external networks. **7.2.2** External access requests must utilize the following minimum controls: (a) Systems / application processing highly confidential data / information must use appropriate encryption methods and predetermined secured lines, in addition to the requirements stipulated for medium / low confidentiality data / information. **7.2.3** All users accessing systems / applications by remote means (e.g. from an approved off-site location) must comply with all sections of the Information Technology Policies and Standards and be subject to the same access controls and authentication controls as if they were accessing the network from within PIACL premises. **7.2.4** Unauthorized access to telecommunication networks must be prevented by the access controls such as ACLs etc.

Policy	**7.3 Data Transmission**
Objective	To ensure that data transmissions are: • Complete; • Accurate; • Legal; and • Not subject to unauthorized disclosure.
Standards	**7.3.1** Controls including the use of error correction software and / or hardware and user procedures will be implemented (where applicable). Chief of IT shall constitute the Team for defining the user procedures. **7.3.2** Strict action shall be taken again unauthorized transmission of Data.

Policy	**7.4 Management Of Modems / Wi-Fi**
Objective	To ensure that all Modem connections to PIACL network, whether local or external are authorized and secured.
Standards	**7.4.1** Use of communication equipment (modems, Wi-Fi, etc) attached directly to computers (standalone and networked computers) with remote control software will be controlled and must be approved by Chief of IT Department after endorsement by Information Technology Management. Information Technology Department will ensure that the equipment being attached complies with Corporation standard security configurations. **7.4.2** Records of all Modems / Wi-Fi and other peripherals attached to PIACL network must be kept updated.

Policy	**7.5 Internet & Intranet Services**
Objective	To ensure that the Internet and Intranet Service are used appropriately.
Standards	**7.5.1** The flow of data to and from any external source must pass through a controlled auditable gateway. **7.5.2** Connections to the Internet must take place from either stand-alone machines or via PIACL controlled gateway. **7.5.3** The Intranets must be shielded from external Internet users by firewalls. **7.5.4** The Internet must not be used to transmit confidential, sensitive or proprietary business information, without appropriate security mechanisms being implemented and without prior approval of the relevant department. **7.5.5** Access to Internet sites that provide pornographic material or other potentially illegal or undesirable material is expressly forbidden. **7.5.6** It is forbidden for PIACL personnel to use the Internet in a way that violates the privacy rights of others or in a way that breaches restrictions under relevant laws and legislation (e.g. advertising, copyright, libel, privacy, data protections, security and defamation). **7.5.7** Internet access must never be used for gambling, games, personal recreation, letter writing campaign, chain letters, solicitation or other activities that might be construed as illegal or unethical. **7.5.8** Gateways and other vulnerable systems will be penetration-tested by a supplier selected by IT Department (ref. Table 1, Item 4). **7.5.9** Staff wishing to publish material, post professional queries etc. on Internet sites, must obtain approval from their departmental heads (or their nominees). **7.5.10** Staff Internet access requests will be approved on the basis of a business justification. **7.5.11** Acceptable use **1.** Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are: **2.** Using Web browsers to obtain business information from commercial Web sites. **3.** Accessing databases for information as needed. **4.** Using e-mail for business contacts. **5.** Sending out our free informational products

7.5.12 Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or nonproductive. Examples of unacceptable use are:

1. Browsing the Internet for issues not related to work.
2. Listening to web radio stations or viewing web TV stations on the computer.
3. Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
4. Broadcasting e-mail, i.e., sending unsolicited messages to a large number of recipients.
5. Conducting any personal business using company resources.
6. Transmitting any content that is offensive, harassing, or fraudulent.
7. Transmitting any proprietary company information.
8. Downloading files not related to work, or downloading large files during peak Internet usage times. Large downloads can be requested through the IT Department.

7.5.13 Personnel who fail to comply with this policy should be subject to disciplinary action which may include, but not be limited to the following:

- Suspension;
- Termination of contractual agreements;
- Civil or Criminal Prosecution; and
- Other Disciplinary Action.

Policy	7.6 Information Transmission via E-mail
Objective	To ensure that the sensitive PIACL information does not fall into the hands of unauthorized individuals.
Standards	**7.6.1** PIACL staff is encouraged to take full advantage of the PIACL electronic mail facility while at the same time ensuring the facility is used according to Corporation Systems Information Technology Standards. **7.6.2** Ensure that all communications are for professional reasons and if not, that they do not interfere with his/her productivity, security of the System and business of PIACL. **7.6.3** Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached. **7.6.4** Avoid transmission of non-public client information. If it is necessary to transmit non-public information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use. Any nonpublic client information must be transferred with the consent of client. **7.6.5** There shall be a trail of all electronic communications which shall be reviewed by the respective department for audit purposes and to ensure security of PIACL's system.

Policy	**7.7 Use Of Electronic Commerce Facilities**
Objective	To ensure that only valid authorized transactions are transmitted and fraudulent alterations to transactions are detected on a timely basis.
Standards	**7.7.1** Transactions audit trails must be reviewed and issues followed-up in a timely manner. **7.7.2** Security Measures: (a) Message Confidentiality Sensitive information to be transmitted via a public network must be encrypted using an approved encryption mechanism. (b) Message Authentication Sensitive information to be transmitted via a public network must be “electronically signed” by the authorized Personnel. Such electronic signatures shall be assigned by PIACL and shall have a hash significantly different from other electronic signatures. (c) Electronic Signatures Authentication Such electronic signatures shall be assigned by PIACL and shall have a hash significantly different from other electronic signatures. Forgery of electronic signature shall be dealt with in accordance with applicable law.

Policy	**7.9 Management Systems**
Objective	Ensure that monitoring or other access to business and other sensitive information is controlled.
Standards	**7.9.1** All management system operators / administrators must be held accountable for their actions through audit record reviews. The management system must log operator activities to a specific audit trail covering both the access time (when they logged on) and a brief record of activity whilst logged on. Introduce such security software that shall help monitor use of Hardware/data/information/Software etc. **7.9.2** Any form of logical access to management System facilities must be denied unless specifically authorized. Management activities must take place under a specific operator/ administrator ID allocated to an individual. **7.9.3** Management system facilities must not be used by operator / administrator to inspect or modify business information on systems / networks. **7.9.4** Breach of the Clause 7.9 will shall lead to: i. Suspension; ii. Termination of contractual agreements; iii. Civil or Criminal Prosecution; and iv. Other Disciplinary Action.

8 Software Copyright Policy

Policy	8.1 Use Of Unauthorized Software
Objective	To ensure that only authorized Software that has been purchased will be used on the Corporation information processing systems.
Standards	**8.1.1** Unlicensed Software will not be used on PIACL Hardware. **8.1.2** Designated Software owners must ensure that software, once installed on a system, is not copied other than for backup purposes by the or with the authorization of the IT department. **8.1.3** Copying PIACL licensed software for use on computers that do not belong to the Corporation, or for purposes not related to supporting PIACL's business is not permitted and breach of this clause shall attract penalization as per PIACL policy and applicable law. **8.1.4** Where possible, latest versions of software will be installed. **8.1.5** In order to maintain proper consistency measures, the same version of software must be used throughout the Corporation. **8.1.6** Use of personal software in production environments where workstations follow a standard configuration is prohibited. **8.1.7** Where personal software may be used pursuant to prior approval of the IT Department before the software is installed on PIACL machines. That software must be recorded in the software inventory and the user must lodge a copy of the license agreement with the support team, or any other team responsible for maintaining the inventory.

Policy	**8.2 Provision Of Software**
Objective	To minimize the need for staff to use personal /private software by providing sufficient legitimate software.
Standards	**8.2.1** All Software required for supporting business functions will be provided by the Corporation. **8.2.2** Request for Software must be routed through the software requisition process and must be approved by the requester's reporting officer and Chief of IT Department. **8.2.3** The IT department shall be responsible to endeavor review, search, solicit, test and introduce new and advanced Software to meet with the need of various business units. **8.2.4** Each business unit in dire need to use personal data/ private software for the purposes of Corporations business shall inform and procure written consent from Chief IT. Chief IT shall be responsible thereafter to monitor/audit such use to ensure that there is no data breach.

Policy	**8.3 Purchasing & Regulating Software Usage**
Objective	PIACL Personnel must comply with all licensing terms to ensure that conditions are not breached resulting in fines or other penalties.
Standards	**8.3.1** The only Software that complies with the Corporation's standards should be included in the Corporation's approved Software list. Such list shall be formulated by the IT department after considering the requirements of all business units. **8.3.2** License agreements must be vetted by the legal department before it is signed by IT department and the software vendor. **8.3.3** Where Software is obtained as free or limited use evaluation copy or in other forms is relied on for production after a period of evaluation, then its use should be regularized with suppliers/vendors within an appropriate contract and a license agreement. Such Software shall not be used for processing critical data or significant business operations for reason security of data. **8.3.4** IT department will be responsible for ensuring that all requirements of the license agreement are observed.

Policy	**8.4 Unauthorized usage**
Objective	Ensure Corporation personnel abide by copyright, confidentiality conditions and understand the penalties associated with breaches.
Standards	**8.4.1** Personnel who breach copyright, confidentiality agreements by unauthorized copying, transmitting or downloading of Software/Data/ Information failing to comply with Software license agreements, SLA Agreement should be subject to disciplinary action which may include, but not be limited to the following: i. Suspension; ii. Termination of contractual agreements; iii. Civil or Criminal Prosecution; and iv. Other Disciplinary Action.

Policy	8.5 Notification Of Illegal Software/Data/Information Copying /Transmitting/Downloading.
Objective	Ensure that any illegal software/documentation copying/transmitting and downloading is identified and appropriate action taken.
Standards	**8.5.1** All Personnel are required to notify their Manager and IT Department if they become aware of any illegal copying/transmitting or downloading of software or related documentation. **8.5.2** Regular reviews should be performed to ensure that all software used is appropriately licensed and is the current standard version. **8.5.3** In the event a Personnel/User/Owner is found illegally copying Software or Data that he shall be penalized as per PIACL policy and prevalent law

9 Contingency, Redundancy & Backup Policies

Policy	9.1 Backup Plans
Objective	Ensure that processing can be restored in the event of a loss of part or all the computing facilities.
Standards	**9.1.1** All PIACL information / data should be backed up on a regular basis. Backup cycles (covers data retention periods) should, as a minimum include: a. Be performed before and after major changes to the operating system (system software), such as an upgrade (to include system programs and configuration information in this case). b. Ensure application software is backed up after each change (e.g. following a new release of the application or following maintenance to the production Software). c. Ensure that all information, Data and Software is backed up in a manner commensurate with the frequency with which that Software, information or Data changes (e.g. systems with daily data entry or modification would require daily backup). System / application / device owners to ratify the acceptability of the backup frequency (ref. Table 1, Item 5) **9.1.2** Backup scope, frequency and number of cycles / generations will be determined by the IT Department in consultation with the system / application / device owner and will be documented in the SLA (if any). A cycle of backups should be used with at least one copy in each cycle stored Off-site. A sole backup must not be repeatedly used (i.e. should not overwrite the only copy of a backup with a new backup). **9.1.3** Backups held on-site should be stored in secure areas that are accessible by authorized Personnel only. **9.1.4** The Data backups shall be tested periodically, and restore activity logs must be maintained. **9.1.5** Backup copies must be stored in a secure location and on removable media (e.g. floppy disk, tape and cartridge), remote from the operations environment to which they belong. The Off-site location may, typically although not necessarily, be the DRP site. The main requirement is for the primary data and backups to be stored at separate locations. **9.1.6** The Off-site storage facilities should be: • Fitted with appropriate environmental controls devices such as HVAC etc.; and • Provided adequate protection against fire, water flooding, disasters etc.

	9.1.7 During transportation to and from offsite storage locations, back-up media should be protected with defined levels of physical security. Registers recording the contents of back-up media held in Off-site storage locations must be maintained. All backup media (e.g. disks, tapes) must be transported using containers and methods appropriate for the classification of the information they hold (ref. Table 4). **9.1.8** Media stored Off-site will be inspected periodically for signs of deterioration (ref. Table 1, Item 5).

Policy	**9.2 Contingency Plans**
Objective	To develop contingency plans and ensure that all critical System/ applications can be restored on a timely basis in the event of disaster as per the disaster recovery strategic plan.
Standards	**9.2.1** A disaster recovery strategic plan must be documented and copies to be stored at both the primary site and the back-up site. **9.2.2** A recovery strategy should be implemented for all critical Systems/applications/devices. The strategic implementation will be influenced by: a. The importance of the System/applications/devices to business operations; and b. The ability to recover the system within the business tolerance period as per the DR plan. **9.2.3** Information Technology Department will be responsible for the development and the maintenance of disaster recovery plans. **9.2.4** The disaster recovery plans should include, as a minimum: a. The criteria to activate the plan including detection of a disaster and notification of relevant Personnel; b. Procedures to implement the recovery strategy and recover all systems / applications in a minimum impact of business as per the DR plan; c. List of Personnel responsible for each aspect of the disaster recovery procedures shall as per their roles work towards reverting to normal processing; d. Testing procedures; and e. The responsibility for coordinating on-going maintenance of the plan. **9.2.5** Business Units must determine and document the manner in which business operations will be continued while the Information Technology recovery strategy is being implemented. **9.2.6** Disaster Recovery Processing must be tested periodically and the test results must be properly documented (ref. Table 1, Item 2). **9.2.7** The level of security over the disaster recovery facilities and Systems / applications must be at least at the same level of stringency as on the primary facilities. **9.2.8** The Disaster Recovery Plan must be updated after: • Disaster Recovery Tests; • Configuration changes; • Application changes; • New vendor agreements; and • New outsource agreements.

Policy	**9.3 Redundancy Plans**
Objective	To ensure that critical applications / systems / devices are available for processing as required by the applications / systems / device owner.
Standards	**9.3.1**. Applications / systems / devices will be classified as "High Availability", "Medium Availability" or "Low Availability" systems. **9.3.2**. The Corporation will ensure that "High Availability" systems are implemented in a way to survive single point of failure by: • Installing redundant hardware; • Supporting / enabling redundant online storage; • Providing fall back or hot standby facilities; • Implementing appropriate standby systems (hardware, software, network devices etc.) to be able to deliver the required / agreed service level; and • Supporting remote management / recovery capability. **9.3.3.** All critical applications/Systems/devices whether "High Availability", "Medium Availability" or "Low Availability" must: • Be supported by a Service Level Agreement (SLA) signed between the Information Technology management and service Provider; and • Have a regularly tested Disaster Recovery arrangement. **9.3.4** Redundant links (routers, hubs, interfaces, etc.) shall be implemented to ensure critical applications / Systems are available as required by System/Application owner to provide the high availability to corporate users. **9.3.5** Hot swap networking devices will be implemented (where justified) to ensure that redundant devices are available in case of device failure.

10 Physical Security Policy

Policy	**10.1 Protecting Portable Machines**
Objective	To ensure that portable hardware / components that store information located outside Corporation's controlled environment are properly safeguarded and accounted for.
Standards	**10.1.1** End User of Hardware, shall take reasonable steps to protect valuable removable devices and computer accessories, including portable computers from the threat of theft / loss and unauthorized access. **10.1.2** The equipment owner / user with the help of IT Department must ensure that appropriate encryption and / or other protective measures are used to protect the information / data stored on portable devices. **10.1.3** Non-members of staff must not use portable equipment owned by PIACL (includes laptops).

Policy	10.2 Physical / Environmental Conditions For Computer Rooms
Objective	To prevent unauthorized access/use of computer equipment and secondly, to ensure that computer equipment is adequately protected against natural hazards, theft and damage.
Standards	**10.2.1** Physical access to data center/server rooms will be restricted to those staff that needs access for their normal duties. This restriction includes access to power supplies; telecommunications frame rooms, peripherals devices, etc. Any access granted to third parties for the purpose of maintenance or support must be supervised. **10.2.2** Entry and exit points to data centers and critical server rooms must be protected / monitored by electronic access control systems etc. These access control systems / mechanisms must provide an access log for all traffic in and out of the rooms. **10.2.3** Hazardous and combustible materials should be stored at a safe distance from data center / server rooms. Computer supplies such as stationery should not be stored in the room except in quantities required for daily use. **10.2.4** Temperature and humidity metering equipment, smoke detectors, fire alarms, appropriate fire extinguishing equipment (fixed and portable equipment) and fire escapes will be installed before server systems are commissioned for production processing. Temperature etc. operating parameters / values applicable to each server system and site will be determined by Information Technology Department. Safety equipment must be checked regularly in accordance with the manufactures instructions. Employees must be properly trained in the use and operation of safety equipment. **10.2.5** During unattended periods, buildings / rooms housing Information Technology equipment must be made physically secure. Doors and windows must be locked and intruder detection systems activated. **10.2.6** Unaccompanied non-IT staff, visitors etc. will not be allowed into data center in all hours or into Information Technology area after hours. **10.2.7** Back-up power supplies (generators and Uninterrupted Power Supplies) plus power regulating devices will be installed to server systems.

	10.2.8 All Server systems will be installed in environment-controlled lockable rooms. Eating, drinking and smoking will not be allowed inside server rooms.

11 Computing Hardware & Software Policies

Policy	11.1 Hardware Purchasing, issuance & Identification
Objective	All PIACL computing Hardware purchases and issuance must be recorded and marked to make them readily identifiable as owned by PIACL.
Standards	**11.1.1.** All computing devices, including not limited to computer, laptop, printers, Wireless devices, keyboards must be purchased through ICT Department. **11.1.1** All Hardware must be marked with a unique PIACL identification code. **11.1.2** The mark should be prominently displayed and the marking used must not be removable without trace. The mark should be a unique reference number (normally the asset number) and clearly indicate that the equipment is the property of PIACL. **11.1.3** For Hardware an inventory register/asset register shall be maintained and details of all PIACL Hardware included thereunder, after they are purchased and prior to being issued. The register should include the following details: • Hardware Type (e.g. Computer, Laptop, Printer etc.); • Hardware Model; • Identification No.; • Hardware make; • Purchase Date; • Designated Owner; • Transfer Date; • Serial No; • Location; • Warranty and Expiry Date. **11.1.4** The end user must fill "ICT Hardware Request Form" (ref. Form-1) to obtain a computing device which may include computers, laptops, tablets, printers, etc. After filling "ICT Hardware Request Form" by end users, ICT Department will assess the device request and accept/reject the particular request accordingly. **11.1.5** Where there is a need for hardware to be removed from Corporation premises, approval must be obtained from IT Management and concerned Chief/Head of Department. **11.1.6** All Hardware must be returned to PIACL as soon as possible after the designated owner has completed the required work or upon termination of their employment or contract with the Corporation. IT department must check the returned hardware for damages.

Policy	11.2 Regular Backup & Recovery Arrangements
Objective	To enable recovery of Software, Information and Data in the event of a system malfunction and in a timely manner.
Standards	**11.2.1** Recovery procedures must be documented for all applications / systems. **11.2.2** A copy of each recovery procedure must be stored at the recovery/Off-site location. **11.2.3** Restoration of production data, whether onto “live‟ or test / development environments, must have prior authorization from the relevant IT Manager. **11.2.4** Archives or long-term backups must be associated with read/ recovery processes. In particular, old versions of programs to read archived data must be retained if new versions cannot read the archived data.

Policy	**11.3 Hardware Maintenance & Contracts**
Objective	To ensure all computing facilities are available as required by users and can support acceptable level of customer service with minimal disruption.
Standards	**11.3.1** Appropriate maintenance agreements executed with contractual third parties, will be established and regularly reviewed for critical Hardware. Information Technology Management will approve these agreements. **11.3.2** Maintenance agreements should include formal contracts and include time & materials clauses. **11.3.3** Maintenance agreements should provide adequate coverage to meet the requirements of Users. These requirements should include the provision of replacement Hardware if necessary. **11.3.4** All contracts should allow for the termination and recovery of expenses by the Corporation if Information Technology Policies and Standards are breached and sufficient guarantees by the maintenance provider. **11.3.5** All agreements involving Systems access by contractors, consultants or other external staff must be based on a formal contract. The formal contract must include at least the following elements: • An agreement to abide by the Corporation’s relevant policies and related standards; • An agreement to allow an independent verification or audit of their company or security controls by IT Department (if deemed necessary); and • A confidentiality (non-disclosure) agreement. **11.3.6** Contracts that commit the Corporation to specific security objectives (e.g. Adherence to other organization's security policies and practices) must not be undertaken without reference to Corporation Legal Department.

Policy	**11.4 Hardware Disposal**
Objective	To ensure that hardware is disposed in a manner to ensure that unauthorized personnel cannot obtain access to PIACL confidential information and data.
Standards	**11.4.1** Obsolete or damaged equipment should be disposed of in one of the following ways: • Sold according guidelines; and • Scrapped. **11.4.2** Chief of IT and with the help of custodians of Hardware and Software will authorize disposals (sanctioned by business units), and details relating to the disposal will be entered in the hardware inventory register/asset register. **11.4.3** Information Technology Personnel will erase Software, information/data permanently from storage devices prior to disposing of any computing hardware.

Policy	**11.5 Software Testing**
Objective	To ensure that appropriate test plans and strategies are developed and utilized to ensure software deployed on PIACL production environments is free of errors.
Standards	**11.5.1** When testing software, Personnel must ensure that the: • Testing is undertaken against a test plan and test cases which is developed in accordance with the PIACL methodologies and guidelines; • Software is adequately documented to allow future maintenance; and • Expected and actual test results are recorded in an auditable form

Policy	**11.6 Documentation & Storage Media Security**
Objective	To ensure smooth retrieval of stored information/data for full recovery of a System/application in the event of a software/Hardware malfunction or disaster.
Standards	**11.6.1** All PIACL documentation/Storage Media must be stored securely. **11.6.2** In the event of data loss, off-site backups must be easily retrievable (must be stored sequentially). In the event of data loss will the data subjects shall be informed of such a breach and relevant legal action taken. Further, please specify how and for what period of time is data relevant to customers is stored as this is relevant for compliance with GDPR.

Policy	**11.7 Change Control**
Objective	To minimize disruption of production information systems by ensuring that all system updates/amendments are properly controlled and managed.
Standards	**11.7.1** All proposed production System/application updates must be signed-off (authorized) by the Information Technology Management prior to promotion to production. This process will imply: • Adequate documentation is available; • Testing is completed successfully; and • Applicable Information Technology Policies & Standards have been applied. **11.7.2** An assessment of proposed System/application update/ amendment must be performed to determine potential impact to PIACL's computing systems. **11.7.3** Quality Assurance of the module to be promoted to production must be performed prior to its implementation to production environment. **11.7.4** All documentation related to production changes must be retained. **11.7.5** All change requests must include a back-out procedure if the change fails. **11.7.6** A backup of the affected module must be taken prior to the update. **11.7.7** Development, support, System and applications programmers will not have ongoing access to data in production or recovery sites. Access to resolve problems etc may be granted under the normal change control process. An independent person, must perform production systems/application updates.

Policy	11.8 Emergency Change Control
Objective	An emergency change is implemented when there is an Incident that requires a change. Emergency change requests bypass the normal approval process. When you create an Emergency change the new approval process phase will be used, bypassing the normal change states.
Standards	**11.8.1** Emergency change will be triggered when a major incident occurs or when an important issue is about to happen (like a security upgrade, regulatory requirement, etc.) **11.8.2** Each and every emergency change ticket/request should be recorded so that it could be tracked, monitored, and updated throughout its life cycle, no emergency changes can be implemented based on verbal communications. **11.8.3** Change Manager will validate the need for an Emergency Change in consultation with Incident manager/Line manager who will be the Change Owner in this case. **11.8.4** If an Emergency Change is triggered, Change Owner will be ready with all functional & technical requirements and then document the impact of Change if implemented along with back out readiness. **11.8.5** The Chief of IT or Chief of IT's nominated committee will approve the emergency change convened by change manager **11.8.6** Change Manager will supervise the build, test and implement the change. **11.8.7** Minimal testing will be carried out to gain the confidence and also to avoid post-implementation issues. **11.8.8** Change Manager will ensure that the service is restored at the earliest. In case the change is not successful it would be rolled back.

12 Service Delivery Agreement Policy

Policy	12.1 Service Level Agreements (SLAs)
Objective	To ensure continuity and availability of IT services for both PIACL round the clock operation and customers.
Standards	**12**.1.1 The service level agreement could be signed between • PIA IT and external IT service provider • PIA IT and internal Department of PIACL. • PIA IT and the customer. **12.1.2** SLAs must include but not limited to following components in two areas; Service and Management. • An introduction to the SLA: what does this agreement propose, individual involved, effective/expiry date as well as a general statement on what other details the particular SLA will cover. • Goals and Objectives: the purpose of the agreement including the ability to obtain a mutual agreement. • A Service description: what service this SLA support and details of the service • Mutual responsibilities: who's responsible for what part of the service. • Stakeholders: Parties involved in the agreement. • In-Scope as well as Out of Scope of the SLA • Applicable service hours: from what time till what time is the service available according to the agreement • Service availability: how much is the service available during the service window and outside of the service window • Customer support arrangements during and after working hours • Response time for the Service requests • Clearly defining Severity levels of the incidents that will lead to a specific response time • Planned Maintenance Windows that will not be accounted for as down time. • Problem resolution: Contact points, escalation, communication matrix • Service performance metric and monitoring method • Costs and charging method used • Penalties/Service Credits in case of service degradation preferably as a percentage of the overall service costs. • Periodic review and adjustment for continual service improvement.

	• Termination and escape clause. • Dispute resolution & Indemnification clause • Ownership and duration of validity of the SLA; • Responsibilities for security administration of services including granting and withdrawal of access rights; • Adherence to PIACL Information Systems IT Policies & Standards; • Non-disclosure agreements; • Guarantees to ensure sufficient data protection and the cost of data breach and leakage; and • Warranties and representations. • Regular incident reports in regards to issues detailing date of occurrence, Severity, nature of problem and rectification. • Periodic IT Service Report to show which services met or failed to meet the target. • Periodic Service Level review meetings **12.1.3** PIA corporate policy will take precedence and be followed in case of conflict of organization policies.

13 Projects Policy

Policy	**13.1 Pre-implementation Security**
Objective	To incorporate security control features / parameters before projects are commissioned for production processing.
Standards	**13.1.1** Information Technology controls / features will be incorporated before Information Technology-related projects are implemented for production processing. **13.1.2** Where the required standards have yet to be published, the project manager will request for appropriate controls from IT Department. **13.1.3** Before implementing a project, the project team in liaison with the Business User will perform classification of both the System / Application and the Information / Data. **13.1.4** Project teams will not access “Live‟ production partition without approval from system / application / data owner and IT Department. **13.1.5** Computer Hardware will only be connected to PIACL network after applying appropriate minimum System Security Policies and Standards. (ref. table 7). **Note:** Users will not modify (by introducing unauthorized programs, utilities etc.) initial configuration of any PIACL workstation / laptop. **13.1.6** Security requirements must be identified and agreed prior to the development of information systems. **13.1.7** Integrated testing will be conducted in a test environment reflecting the secured production environment.

14 IT Help Desk Management

Policy	**14.1 IT Help Desk Management**
Objective	The Helpdesk is the first and single point of contact for technology support for all PIA staff. The Helpdesk provides technology assistance through a telephone Support Center, responds to emails and Web based queries, and provides service points for all business units. It defines the processes necessary to ensure technology problems and requests for service are resolved in an efficient and timely manner.
Standards	**14.1.1** Helpdesk agents are to maintain a courteous and professional manner at all times when interacting with the PIA staff. Calls are to be answered within two rings with a consistent standard greeting, and the help desk staff will identify him or herself to the caller **14.1.2** The Helpdesk will be responsible to provide hardware, software, network, telephone, cable, media, for all IT staff round the clock. Helpdesk Staff are to enter a ticket for each caller, even in the event of a major outage. Helpdesk staff are not to just tell the caller we are aware of the problem without recording the call. **14.1.3** The Helpdesk staff will use Service Desk software to record, forward and track all technology requests to act upon service. **14.1.4** Helpdesk staff is to make every effort for first call resolution. Helpdesk Staff are to use the remote control when possible, always requesting permission prior to taking control of a user’s machine. Helpdesk Staff are to transfer calls to another Engineer of the technology group for problem resolution only when necessary. Helpdesk staff is to advise the caller that the problem is being escalated to a specialist. **14.1.5** Helpdesk staff is to follow up with Tier II or III to ensure resolution is achieved and the ticket is updated. Tier 1 technicians are responsible for keeping the end user informed of the status of his or her ticket and to set realistic expectations. Technicians are responsible to confer with each other and escalate problems to management, that they cannot fix within a reasonable time frame. All technicians are required to meet a certain SLA based on the severity of the problem. **14.1.6** When entering or updating tickets, the Helpdesk staff is to describe the problem accurately and include detail. **14.1.7** An appropriate number of Helpdesk staff will be logged in and available to answer support calls, as well as to monitor Helpdesk email. The number of staff on call will depend upon call volume. The Helpdesk manager will monitor call management software and make appropriate determinations as to resources required. The Helpdesk Manager is responsible for monitoring ongoing performance and productivity of the Helpdesk, striving for continual improvement

15. Capacity & Performance Management

Policy	15. Capacity & Performance Management Policy
Objective	To ensure that the capacity and performance of the IT infrastructure is right-sized and matches the current & future requirements of business and SLAs in effective, cost efficient and timely manner.
Standards	**15.1** A continuous and iterative process shall be in place that will monitor, analyse and evaluate the capacity and performance of IT infrastructure. **15.2** An IT team shall be constituted by respective GM ICT to collect and appraise the required data for allocating the appropriate IT resources for new IT Project. **15.3** The data collection before commencing IT Projects shall cover all business, financial, technical and services, as well as the SLAs, risks information in relation to the project. **15.4** The designated Team will evaluate and analyse the data collected and engage the change management team for increasing or decreasing the IT resources accordingly to meet the envisaged objectives. **15.5** The Change management team shall involve the relative capacity management team to resolve the deficiencies or non-compliances. **15.6** Necessary authority will be delegated to the corresponding Capacity Management team to initiate actions which ensure required levels of IT Service Capacity and reliability. **15.7** The Capacity management team of respective areas shall present the resource utilization reports to their Sectional Heads periodically for review and any anticipated, proactive updating.

Tables

Table 1 - Parameters Item

Item	Control Requirement		Frequency / Parameter	Responsibility
1.	Corporation Information Technology Policies & Standards Self-Assessment (ref. Section 1.2.4).		Annual	All PIACL Units
2.	Disaster Recovery Testing (ref. Section 9.2.6).		6 Months	Information Technology
3.	Software Inventory Reconciliation (ref. Section 5.6.3).		Annual	Information Technology Department
4.	Backup Media Inspection (ref. Section 9.1.7).		Annual	Information Technology Department
5.	Data Retention (ref. Section 9.1.1)	Daily Incremental Backups.	At least 30 Days retention	Information Technology
		Full Monthly Backups.	At least 12 Months retention	Information Technology

Table 2 - Ensuring Integrity
(ref. Section 6.2, Item 6.2.5)

Item	High Integrity / medium	Low Integrity
1.	Must be protected by a logical access system.	Information should be protected against unauthorized creation, modification, deletion, replacement or replication using authentication, logical access controls and physical access controls.
2.	Must be protected against unauthorized creation, modification, deletion, replacement or replication, electronic forgery through logical access controls. Transmission (in any form) must be protected against unauthorized creation, modification, deletion or replication using an approved encryption process.	-
3.	Any changes to the information must be logged including date, time, nature of change, person responsible, person authorizing the change and the log secured from modification or unauthorized deletion. Logs will be retained for period agreed with the Applications/Systems / Information / Data Owner.	-
4.	Any attempts to destroy or otherwise make unauthorized changes to information must be automatically logged. Such logs must be regularly reviewed.	-

Table 3 - Ensuring Availability
(ref. Section 6.2, Item 6.2.5)

Item	High Availability	Medium/Low Availability
1.	Systems/Applications are implemented in a way to survive single point of failure by: • Installing back-up power supplies; • Supporting/enabling redundant online storage; • Providing fall back or hot standby facilities; • Implementing appropriate standby systems (hardware, software, network devices etc.) to be able to deliver the required / agreed service level; and • Supporting remote management / recovery capability.	All critical Applications / Systems / devices, must: • Be supported by a Service Level Agreement (SLA) signed between the Information Technology management and the Applications / Systems / Devices owner; and • Have a regularly tested Disaster Recovery arrangement.
2.	All critical Applications/ Systems / devices, must: • Be supported by a Service Level Agreement (SLA) signed between the Information Technology management and the applications / systems / devices owner; and • Have a regularly tested Disaster Recovery arrangement.	Existence of a Service Level Agreement (SLA) and Disaster Recovery Plan (DRP).
3.	Existence of a Service Level Agreement (SLA) and Disaster Recovery Plan (DRP)	The SLA should be monitored and regularly reviewed
4.	The SLA must be monitored and regularly reviewed	-

Table 4 - Backup Media Transportation (ref. Section 9.1, Item 9.1.6)

Item	Highly Confidential / Confidential	Internal Use Only/Private
1.	Must be transported by trusted courier or Corporation staff only. Transportation must meet environmental specification of the respected media.	Transportation dispatch and receipt must be logged, checked and acknowledged
2.	Transportation dispatch and receipt must be logged, checked and acknowledged	-

Table 5 - Storage Media
(ref. Section 6.9, Item 6.9.1)

Item	Highly Confidential / Confidential	Internal Use Only/Private
1.	Must not be available outside the Corporation without the permission of the relevant person of authority.	Should not be given to people outside the Corporation without appropriate management and originator authorization.
2.	Must not be communicated electronically without ensuring the medium is appropriately secure.	-
3.	Must be stored securely (e.g. in a safe, lockable cabinet etc.) when not in use.	-
4.	Should be retrieved from staff leaving the Corporation or changing role where that access is no longer required. Corporation shall enter into a covenant with each employee leaving a that he has no copies of data stored in such storage mediums, neither has he tampered with the data provided there under and shall retain the confidentiality of all the information and data he has had access to during his term of employment.	-
5.	Should not be copied or further disseminated without the permission of the relevant person of authority.	-

Table 6 - Documentation / Media Disposal
(ref. Section 5.7, Item 5.7.1 and Section 6.9)

Item	Highly Confidential / Confidential	Internal Use Only/Private
1.	Documents must be disposed by shredding (or other equally irreversible means of destruction).	Should not be given to people outside the Corporation without appropriate management and originator authorization.
2.	Media (magnetic, optical etc.) must be disposed of in a manner that prevents the recovery of the information i.e. by secure deletion (seek advice from IT Department), or by physical destruction.	

Table 7 - Minimum Machine Security Requirements

Note: Tasks listed below are not ordered.

(a) Server Security
1. Install applicable Operating System (Windows, Unix etc.).
2. Harden the Operating Systems using appropriate Corporation Standards.
3. Configure security features such as User Rights, Audit Log, Directory / File permissions etc.
4. Delete / disable expired profiles (if not required).
5. Change default profiles password (if profile is required and enabled).
6. Configure the server to run required applications only (unnecessary programs, applications, options to be removed from the server).
7. Disable unnecessary services.
8. Install / configure appropriate utilities, Icons and shortcuts.
9. Configure services such as Printer etc. (where required).
10 Install Anti-Virus Software.
(b) Workstation Security Controls
1. Install applicable standard Operating System (Windows, etc.).
2. Harden the Operating Systems using Corporation Standards.
3. Configure security features such as User Rights, Audit Log etc.
4. Delete / disable expired profiles (if not required).
5. Change default profiles password (if profile is required and enabled).
6. Configure the workstation to run required applications only (unnecessary programs, applications, options to be removed from the workstation).
7. Disable unnecessary services.
8. Disable CD drive (for operational staff if not required).
9. Install / configure the required application agents, utilities and Icons / shortcut.
10. Configure a network drive for data / information storage.
11. Rename the local administrator Account (for Windows -workstations).
12. Install the Anti-Virus Software.
13. Configure services such as Printer etc. (where required).
(c) Router Security Controls
1. Set up the Access Control List (ACL)

Table 8 - Incidents Management Policy

ref. Section 6.14, Item 6.14.2

Item	Incident
1.	Pre-attack probes.
2.	Unauthorized access attempts (unauthorized user activity).
3.	Denial of service attempts.
4.	Vulnerabilities identified as a result of a scan (serious software vulnerabilities).
5.	Notification by an outside source that they are being attacked from PIACL IP addresses.
6.	A computer virus attacks.
7.	Computer intrusion.
8.	Loss of online or archived data / records.
9.	Unauthorized use of a modem.
10.	Unauthorized attachment of a workstation to PIACL network.
11.	Use of an employee’s own software on PIACL computers.
12.	Use of an illegal copy of any software on PIACL computers.
13.	Intentional entering of false data into a database.
14.	Modifying or deleting production information without authorization.
15.	Changing of production data by a version of an application program that has not been formally tested and released to production.
16.	Modifying computer source code without authorization.
17.	Modifying an operating system or network configuration without authorization.
18.	Changing access permissions in an access control table without authorization.
19.	Unauthorized erasure of data from a hard drive, tape, or other storage system.
20.	Unauthorized removal of PIACL software and system documentation.
21.	Any abusive or offensive message sent by e- mail.
22.	Actions that make excessive or unusual use of resources thus harming normal operation.
23.	Any unauthorized observation of the packet stream on PIACL network (usually aimed at obtaining passwords, commercial or personal information).
24.	Abuse of Internet message services (e-mail) usually involving the sending of large volumes of unsolicited mail.
25.	Any incident involving the use of a program that conceals its true function. This technique is often used to persuade users to install remote control or attack programs.
26.	Employee receiving an electronic mail message with a virus-infected word processing document attached.

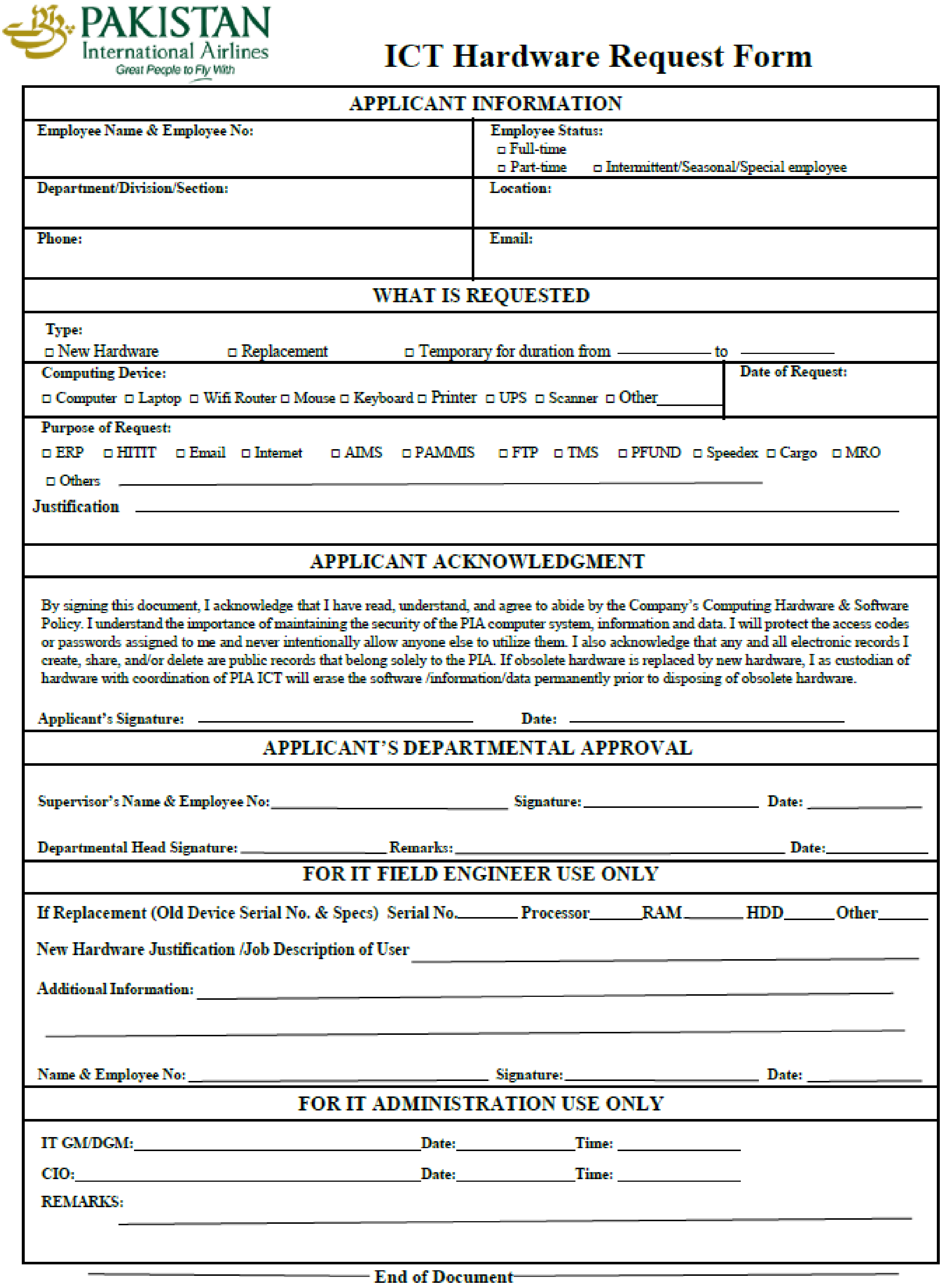
Appendix 1 - Information / Data Classification Matrix (ref. Section 6.2, Item 1)

System classification is based on the applications / systems / devices / end user's tag of confidentiality, Integrity & Availability.

Information / Data Classification Matrix

	Low	Medium	High
Confidentiality	This is standard information for internal use and needs to be protected in accordance with good business practice and regulatory requirements.	The information is important, sensitive to competitors. Direct loss of business and public confidence may be suffered as a result of a disclosure.	Mission critical with long-term effects. Serious long-term damage to business and public confidence may be suffered as a consequence of disclosure resulting in business survival being threatened.
Integrity	PIACL requires complete and accurate information in accordance with good business practice and regulatory requirements.	The information is important. Unauthorized or accidental modification/fabrication of information will have significant consequences resulting in medium or short-term business impact.	Mission critical with long-term effects. Unauthorized or accidental modification/fabrication of information will have serious financial consequences resulting in business survival being threatened.
Availability	Appropriate and timely recovery needs to be ensured in accordance with good business practice.	Failure to have accurate information at hand when required or failure to ensure timely delivery of information may result in incorrect business decisions being made (with medium or short term impact), or individual business transactions being lost to competitors.	Failure to have accurate information at hand when required or failure to ensure timely delivery of information may result in business survival being threatened, or serious trading losses being incurred.

Form 1 - Computing Hardware & Software Policies
(ref. Section 11.1, Item 4)



PAKISTAN
International Airlines
Great People to Fly With

ICT Hardware Request Form

APPLICANT INFORMATION

Employee Name & Employee No:	**Employee Status:** □ Full-time □ Part-time □ Intermittent/Seasonal/Special employee
Department/Division/Section:	**Location:**
Phone:	**Email:**

WHAT IS REQUESTED

Type:
□ New Hardware □ Replacement □ Temporary for duration from ____________ to ____________

Computing Device:
□ Computer □ Laptop □ Wifi Router □ Mouse □ Keyboard □ Printer □ UPS □ Scanner □ Other________

Date of Request:

Purpose of Request:
□ ERP □ HITIT □ Email □ Internet □ AIMS □ PAMMIS □ FTP □ TMS □ PFUND □ Speedex □ Cargo □ MRO
□ Others ____

Justification ____

APPLICANT ACKNOWLEDGMENT

By signing this document, I acknowledge that I have read, understand, and agree to abide by the Company's Computing Hardware & Software Policy. I understand the importance of maintaining the security of the PIA computer system, information and data. I will protect the access codes or passwords assigned to me and never intentionally allow anyone else to utilize them. I also acknowledge that any and all electronic records I create, share, and/or delete are public records that belong solely to the PIA. If obsolete hardware is replaced by new hardware, I as custodian of hardware with coordination of PIA ICT will erase the software /information/data permanently prior to disposing of obsolete hardware.

Applicant's Signature: ____________________ **Date:** ____________________

APPLICANT'S DEPARTMENTAL APPROVAL

Supervisor's Name & Employee No:____________________ **Signature:**____________ **Date:** ____________

Departmental Head Signature:____________ **Remarks:**____________________ **Date:**____________

FOR IT FIELD ENGINEER USE ONLY

If Replacement (Old Device Serial No. & Specs) Serial No.________ **Processor**______**RAM**______ **HDD**______**Other**______

New Hardware Justification /Job Description of User ____

Additional Information: ____

____

Name & Employee No: ____________________ **Signature:**____________ **Date:** ____________

FOR IT ADMINISTRATION USE ONLY

IT GM/DGM:____________________Date:____________Time: ____________

CIO:____________________Date:____________Time: ____________

REMARKS:
____

End of Document

Definitions

Availability The characteristic of data, information and information systems being accessible and useable on a timely basis in the required manner.

Confidentiality The characteristic of data and information being disclosed only to the authorized persons, entities and processes at authorized times and in the authorized manner

Data A representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by human beings or by automatic means.

Data Base A collection of data that is logically organized to reflect the functional requirements and data interdependencies of one or more application systems. A database is usually accessed and updated through the use of a Database Management System

Hardware The equipment used in the operation of computer systems. This includes, but is not restricted to, the CPU, tape drives, direct access devices, printers, terminals, modems and control devices that enable the equipment to work together. Hardware also includes data entry devices that are not directly attached to a computer system

Information The meaning assigned to data by means of convention applied to that data.

Information Systems The computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance.

Integrity The characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

Modem (Modulator/ Demodulator) A device that provides an interface between a communication terminal and a computer system. It converts analog telephone signals into digital signals, and vice versa.

Off-site Location Off-site location is defined as a facility or building physically separate to the one in which the main system is located and to which access would be possible even if the main facility is unavailable.

Personnel The term “personnel” refers to permanent, contracting, and casual staff engaged to provide services to PIACL including but not limited to management, promoters, contractors, consultants and agents, employed directly or indirectly by or for PIACL.

Procedure A series of operations performed in a regular sequence to accomplish a stated purpose. Procedures may be manual or computerized.

Program An ordered series of instructions written in a programming language. If translated into object code, these instructions are potentially executable in a computer.

Quality Assurance The process of ensuring that a computer program or system reflects the intention of its designers and can be successfully run in a production environment.

Software Generic term used to describe all computer programs.

Standards The rules under which personnel work. Standards usually cover, but are not necessary limited to, documentation requirements, technical rules, operation procedures, system development steps and deliverables.

Systems A collection of logically related hardware components and / or computer programs designed to fulfill a set of related functions. A system also includes the manual methods and procedures needed to support computer processing.

User A generic term referring to the individual or organizational unit that is the primary recipient of data from a computer system.