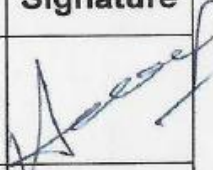

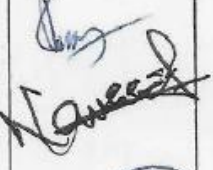


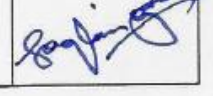




ICT System Backup Policy & Procedure

10th Edition

Activity	Name	Designation	Signature
Prepared By	Adeel Yousfani CISSP	Deputy General Manager (DGM) Information Security	
Review & Checked By	Irfan Ayub	Deputy General Manager System Administration	
	Riaz Zeeshan	Deputy General Manager IT Infra. & Data Center	
	Naveed Azhar	Deputy General Manager Application Development	
	Nadeem M.Khan	Deputy General Manager ERP Technical	
	Syed Ahmed Faraz	General Manager IT Infrastructure	
Approved By	Muhammad Saqlain Gardezi	Chief Information Officer CIO	

Distribution List: Copy on Corporate Intranet

Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY	Page 2
	Doc# : ICT/SBP/03	Rev#: 03 06th May, 2024

System Backup Policy & Procedure

Records of Revisions

Edition Number	Revision Number	Issue Date	Effective Date	Inserted By & Date
1 st Edition	Revision No.0	Dec 30, 2005	Dec 30, 2005	Manager Computer Operations (30 th Dec, 2005)
2 nd Edition	Revision No.0	Mar 02, 2006	Mar 02, 2006	Manager Computer Operations (2 nd Mar, 2006)
3 rd Edition	Revision No.0	Jan 22, 2007	Jan 22, 2007	Manager Computer Operations (22 nd Jan, 2007)
4 th Edition	Revision No.0	Feb 12, 2008	Feb 12, 2008	Manager Computer Operations (12 nd Feb, 2008)
5 th Edition	Revision No.0	Dec 23, 2008	Dec 23, 2008	Manager Computer Operations (23 rd Dec, 2008)
6 th Edition	Revision No.0	Jul 14, 2010	Jul 14, 2010	Manager Computer Operations (14 Jul, 2010)
7 th Edition	Revision No.0	Feb 02, 2015	Feb 02, 2015	Dy. General Manager System Support (2 nd Feb, 2015)
8 th Edition	Revision No.0	Jan 01, 2017	Jan 01, 2017	Manager Database Administration (1 st Jan, 2017)
9 th Edition	Revision No.0	Dec 07, 2018	Jan 01, 2019	Manager Database Administration (1 st Jan, 2019)
10 th Edition	Revision No.01	Aug 31, 2020	Sep 01, 2020	DGM. IT Policy & Governance (1 st Sep, 2020)
10 th Edition	Revision No.02	Apr 28, 2022	Apr 29, 2022	DGM. Information Security (29 th Apr, 2022)
10 th Edition	Revision No.03	May 06, 2024	May 07, 2024	DGM. Information Security (6 th May, 2024)

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 3 Rev#: 03 06th May , 2024
---	---	---

LIST OF EFFECTIVE PAGES (LEF)

Chapter No.	Chapter Name	From	To	Date
1	Plan Introduction	6	11	Apr. 29, 2022
2	DRP Summary	12	14	Apr. 29, 2022
3	Identification and Declaration of a Disaster	15	16	Apr. 29, 2022
4	What to Do in theFirst Instance	17	18	Apr. 29, 2022
5	Activation of DisasterRecovery Process	19	20	Apr. 29, 2022
6	Recovery Considerations	21	23	Apr. 29, 2022
7	Training and Exercises	24	26	Apr. 29, 2022
1.3	PIACL ICT Applications & Database	06	07	May 06 , 2024
1.3	ITBKP-Corporate Systems / Services Hosted on Cloud / Managed by 3rd Party	07	07	May 06 , 2024
1.4	Backup Policy	08	08	May 06 , 2024

Amendment Sheet/Summary: -

Changes from previous Edition are indicated by a vertical line on the right side of the effective pages as indicated in LEF above.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 4 Rev#: 03 06th May , 2024
---	---	---

Table Of Content

1 Plan Introduction	5
1.1 Business Impact	5
1.2 PIA Backup Strategy	5
1.3 PIACL ICT Applications & Database	6
1.4 Backup Policy	7
1.5 Recovery Strategy	9
1.6 Backup Process Diagram	10
1.7 Resource for Disaster Recovery (Within & beyond 48 hours)	11
1.8 Recovery Script/Procedure	11
1.9 Recovery Exercise/Drills	11
2 DRP Summary	12
2.1 Disaster Recovery Preparedness	12
2.2 Objectives of Disaster Recovery Preparedness (DRP)	13
2.3 Business Objectives	14
2.4 Plan Objectives	14
2.5 Assumptions (Check List)	14
3 Identification and Declaration of a Disaster	15
3.1 Criteria For Declaring A Disaster	15
3.2 Who Can Declare A Disaster	15
3.3 The People To Advise	15
3.4 How And When To Get In Touch With Them	16
4 What to Do in the First Instance	17
4.1 Safety Concerns	17
4.2 Critical Resources To Be Retrieved	17
4.3 Critical Resources To Be Retrieved Performa	18
5 Activation of Disaster Recovery Process	19
5.1 Roles & Responsibilities	19
6 Recovery Considerations	21
6.1 Key Functions Necessary For Continued Operation	21
6.2 Recovery Status Report Form	22
6.3 Recovery Steps	22
7 Training and Exercises	24

Copy on Corporate intranet  PAKISTAN International Airlines <i>Great People to Fly With</i>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 5 Rev#: 03 06th May , 2024
---	---	---

Chapter 1

1. Plan Introduction

The prime purpose of a backup plan is to ensure business continuity and disaster recovery due to any unforeseen incident. In view of the business critical data residing in Computer Servers, it is imperative for PIA to protect/secure its critical data through regular archiving process and ensure business continuity in case of any unforeseen incident.

A comprehensive backup procedure and recovery plan is defined and implemented to meet the eventualities in case of a disaster at the data center. Back-up procedure consists of complete assessment process and schedule of steps to execute the task at the shortest possible notice.

1.1 Business Impact

In order to efficiently maintain/run ICT data center from airlines perspective, it is essential to secure the operations and business critical information/data at all times. Regular Data backup procedures and its defined retention period play a vital role to keep the system operational and avoid any loss of critical data during disaster.

A pre-defined backup policy will always ensure protection of business critical data with an option to revert back to secondary backup storage devices without any loss.

PIA ICT has always given high priority to this critical task and made all possible arrangements to maintain a complete back-up procedure to comply with industrial rules and standards.

1.2 PIA Backup Strategy

In order to secure data and system availability in case of system disaster, a backup procedure of systems which includes all application software and database is in place. At present, a regular backup of the system is taken on backup media on daily, monthly and yearly basis. Backup cartridges/media are transported and stored away from the computer building at a remote location in Jinnah Terminal, Karachi.

Backup process is strictly followed as per predefined schedule intervals and frequency to ensure continuity. The rotational days of data backup are pre-determined on the basis of its nature/importance and are accordingly retained to avoid inconsistency.

Copy on Corporate intranet  PAKISTAN International Airlines <i>Great People to Fly With</i>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 6 Rev#: 03 May, 2024
--	---	--

1.3 PIACL ICT Applications & Database

The Following systems in ICT are hosted in PIA Data Center

1. Action On Time
2. Active Directory
3. AIMS Core Application
4. AIMS In-house Reports (Adhoc)
5. Aircraft Analytic & Maintenance Tool
6. Aircraft Floating License Application
7. Aircraft Quality Assurance & Maintenance
8. Aircraft Quality Findings
9. Aircraft Technical Publication
10. Basic Salary Structure of Employee
11. Central Discipline Unit for HR
12. Centralized Authentication Database Server
13. Continued Airworthiness Assessment & Surveillance
14. Corporate Digital Minute
15. Corporate E-mail
16. Corporate Manuals Policy & Procedure
17. Crew Document Management System
18. Crew Website
19. Decision Support System
20. Emergency Response Center ERC
21. Employee Complain management
22. End Point Security System
23. Enterprise Resource Planning ERP
24. Face Recognition System
25. File Storage and Transfer System
26. Fleet Movement Plan and Coverage
27. Flight Data Monitoring (FDM) Airfase
28. Flight Log System (Web)
29. Fly Smart Air Bus Application
30. Frepak System
31. Fuel Management & Analysis System
32. Fund Management, Monitoring
33. Human Resources Management (HR) System
34. IT Workshop
35. Maintain Record of Cockpit Crew Training
36. PIA Dispensary Medical system
37. MyID Staff Travel Web Services
38. Network Devices Authentication Application
39. Network Equipment Credentials Management
40. PAMMIS
41. PHS DPR (Daily Performance Report) Website
42. PIA Administration & Discipline System
43. PIA Connect Mobile Application for Manuals and Circular

Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 7 Rev#: 03 May, 2024
--	---	--

44. PIA Dashboard for Flight Management
45. PIA Pension System
46. PIA Awards +Plus Complaint Management System & NORS
47. PRIMS (PIA Recipe Management System)
48. Provident Fund
49. Quality Assurance & Maintenance
50. Route Performance & Profitability System
51. Safety Information Management System (SIMS).
52. Safety Management System (SMS)
53. Safety Risk Management
54. Security Operation Center (SOC)
55. System Request Manager (ERP & IT)
56. Systems Monitoring System
57. Telephone Exchange Management System
58. Time Management System (TMS)
59. Training Database Management System (TDMS)
60. Wings Middleware (Engg)

There are various Corporate Systems / Services hosted on cloud which are managed by 3rd party. These have been provided as separate attachment: -

- ITBKP-Corporate Systems / Services Hosted on Cloud / Managed by 3rd Party

1.4 **Backup Policy**

The above mentioned Databases and Applications are backed up regularly and backup copies are sent to the off-site location.

All the application and database backups are managed by a **Centralized Backup Management System** (CBMS) that runs on separate host machine coupled with backup media library. The backup server runs enterprise backup software and agent software is installed on client/remote machines. Centralized backup allows collecting data from client machines that host different services like database,

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 8 Rev#: 03 May, 2024
---	---	--

web, email, FTP, DNS, DHCP, etc. All backup schedules for every client are defined on centralized backup server. The “Full/Complete” backup is performed for all databases and application with different incremental frequencies and data retention as mentioned in the “ITBK-System Backup Policy and Responsibility Matrix” document provided as a separate attachment.

The re-writable data cartridges / backup media are scratched and rotated after completing each backup cycle. Each backup media is maintained with a stamped date/time.

Comprehensive Executive Summary for all backup being performed along with their respective frequencies and data retention as well as various sample forms for backup/restoration has been provided as following separate attachments: -

- ITBKP-System Backup Policy and Responsibility Matrix
- ITBKP-Backup Media Naming Convention
- ITBKP-Offsite Relocation – Backup Media Position (Sample Form)
- ITBKP-Virtual Machine Request Form (Sample Form)
- ITBKP-Backup Restore Request Form (Sample Form)


The off site location at Jinnah terminal room is only accessible by two authorized/responsible personnel (Sr. ICT Officer, Mgr. IT Operations South at JIAP) of ICT to ensure its secrecy and effective access control. Furthermore, a 3rd set of keys is kept in the sealed custody of GM IT Infrastructure as backup and further security.

This protected room has secured locking system which can only be opened by specially designed key. Two persons are sent to this secure room to ensure proper security of data. Random checks are carried out by supervisor. The building premises where this room is located is manned by security personnel on 24 X 7 basis.

In an effort to enhance data protection, ensure zero downtime, and maintain seamless operations, PIACL - ICT has established a Disaster Recovery (DR) site in Islamabad. Currently, various stages of setup, comprehensive testing, and implementation of the disaster recovery plan have been completed, making the site fully operational.

However, the DR site has been operational for Oracle EBS at NTC colocation services. The ERP system DR procedures are summarized and provided as following separate attachment: -


- ITBKP-ERP System DR Procedure

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY	Page 9
	Doc# : ICT/SBP/03	Rev#: 03 May, 2024

1.5 Recovery Strategy

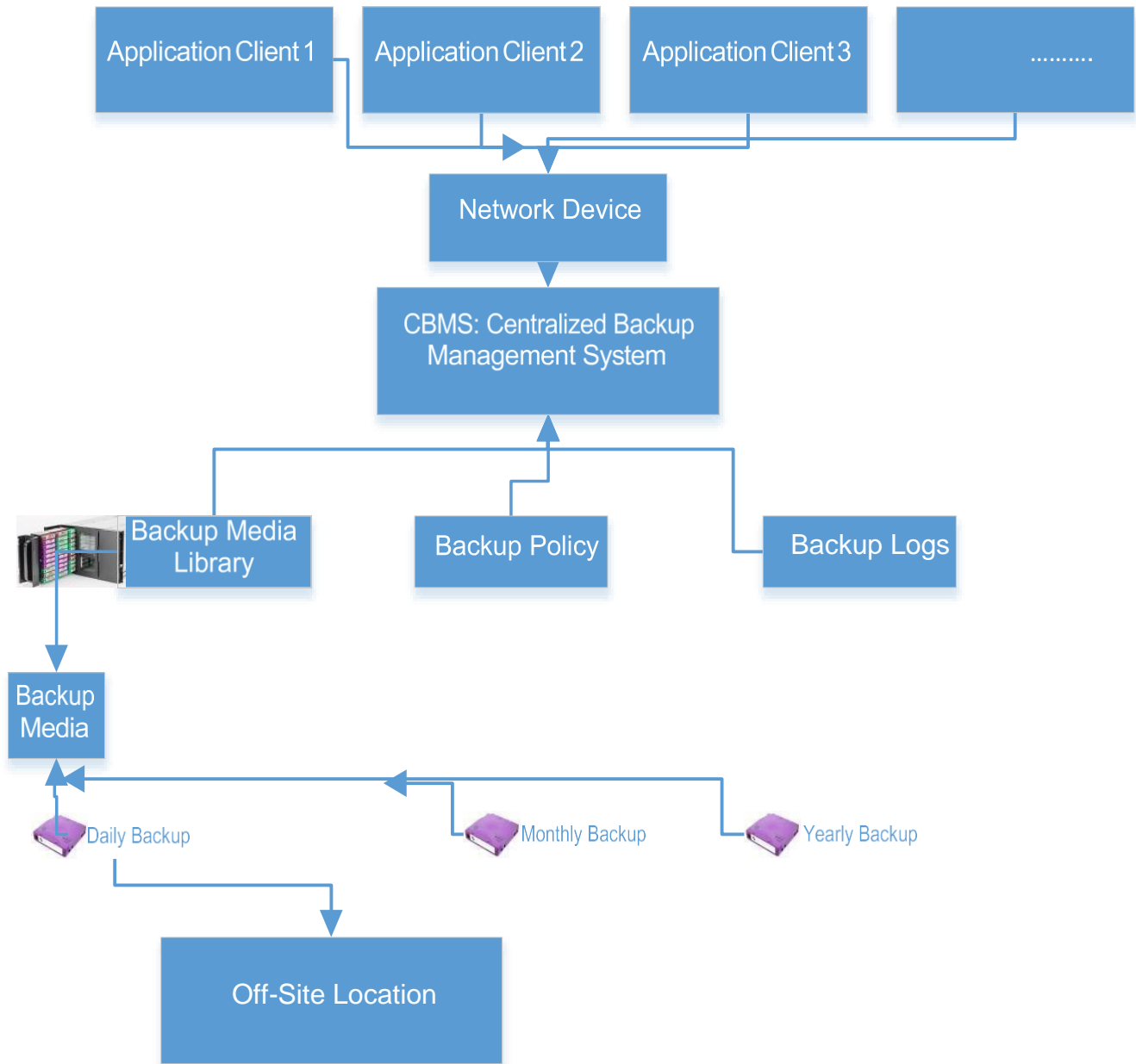
In case of any disaster or data loss, the real loss is determined first and the back-up cartridges can be retrieved from the library with the focus and endeavor that the restoration process can take place at a very short notice.

Once the restoration process is complete the data is verified and the system can be made live.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY	Page 10
	Doc# : ICT/SBP/03	Rev#: 03 May, 2024

1.6 Backup Process

BACKUP PROCESS



Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 11 Rev#: 03 May, 2024
---	---	--

1.7 Resources for Disaster Recovery (Within & beyond 48 Hours)

Following resources will be required to recover the System in an event of Disaster.

Resources	Status	Location
Last Backup storage media	Available	PIA Computer Center / Jinnah Terminal Room
UPS	Installed at the site	PIA Computer Center
Power	Available	PIA Computer Center
Network	Available	PIA Computer Center

1.8 Recovery Script/Procedure

After the disaster declaration, following procedure will be un/resorted for database recovery.

Tasks	Responsibility
Check System Operating System & Application Configuration.	DGM IT Infrastructure & Data Centre
Select correct data cartridge / storage media to retrieve backup	DGM Information Security
Check backup media operability	DGM Information Security
Execute the recovery script from Cartridge / Storage media	System Admin Officer

1.9 Recovery Exercise/Drills

In order to ensure that all backups meet the recovery criteria and are in a position to bring back the system in working condition, a recovery exercise/drill is carried out on quarterly basis meeting the IOSA requirement.

The recovery exercise is effusively comprehensive covering different aspects of possible disaster which may include but not limited to the following: -

- Machine and Hardware Failure
- Human Error
- Viral Attack
- Cyber Attack
- Data Corruption
- Natural Disasters
- Customers Care... Management and various Agencies requirement e.g. Govt. agencies, Tax reports, Auditors...etc.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 12 Rev#: 03 May, 2024
---	---	--

DISASTER RECOVERY PLAN (DRP)

Chapter- 2 **DRP Summary**

2.1 Disaster Recovery Preparedness plan is vital for PIACL ICT department's mission-critical business environment. There are three possible airline data center specific scenarios which can occur at any given time.

The following incidents can become a case study for a disaster preparedness plan:

- 1. System Crash/Down.**
- 2. System Slow Response Time.**
- 3. Office/Computer Centre Site Down (Inaccessible)**

2.1.1 System Crash/Down

This scenario occurs when the systems are inaccessible for number of reasons, i.e., machine failure, fire, power, virus attacks, sabotage etc. The system-down is considered a disruption of services which is less than 48 hours in duration 99.99% of time.

2.1.2 System Slow Response Time

This scenario occurs when the systems response is slow and effects the operations in terms of its response time. This snag can be removed with the assistance of support services of vendor and/or administrator's effort to streamline the processes and fine tune the systems processing capacity. The system slow response time is considered to be disruption of services if response time exceeds 30 seconds for 99.99% of queries.

2.1.3 Office/Computer Centre Site Down(Inaccessible)

This scenario occurs when the data center remains inaccessible. This situation usually arises due to natural calamity such as earthquake, flood, heavy rains, security reasons or deteriorating law & order situation such as strike, etc.

The site-down situation may cause a disruption of services for a time greater than 48 hours. This situation may encounter two different scenarios:

1. Office remains inaccessible but all database services are running smoothly. In such situation, we have to provide a database services access to an alternate office.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 13 Rev#: 03 May, 2024
---	---	--

This requires an alternate space arrangement with necessary devices such as servers, manpower and necessary network for a remote access. The arrangement can provide a system access within 48 hours.

2. In this scenario the data center premises remain accessible but parts of database services cannot be accessed by the users due to power outage, hardware failure, system malfunctions or sabotage. In such situation the database services can be processed through an alternate facility. These arrangements can fall in greater than 48 hours' slot.

However, it is important to note that the disaster preparedness plans for each of the above scenarios do contain overlapping process in some areas. This is because we view the scenario from end-user's perspective.

The system/site may be considered down regardless of its fault from end-user perspective if they cannot get a response to their screen after hitting a key. The fault may be at the client's site due to local area network components or the main system itself. Thus, defining a "*site down*" disaster preparedness plan each component shall be considered between the end-user's client and the servers.

2.2 Objectives of Disaster Recovery Preparedness (DRP)

The basic objective of this document is to maintain a complete preparedness plan for a disaster like situation, suitably documented with easy access which directs a process that needs to be followed if a "**disaster**" situation arises.

It is hoped and expected that this document will assist the ICT Department as the basis for all actions that needs to be initiated during the recovery from disaster situation.

2.2.1 Objectives of Computer Operations Disaster Recovery Plan (DRP) are:

- A. Ensure that System applications are available for use by all business units.
- B. Minimize the impact on the business users when short-term and/or long-term service outages occur (< 48 Hours and/or > 48 Hours).
- C. Define the roles and responsibilities of the various recovery teams who will be responsible for an overall restoration of services in an event of a disaster or service outage in both < 48 Hours and > 48 Hours.
- D. Provide alternate computing facilities and resources in a timely manner.
- E. Communicate the recovery plans and recovery team responsibilities to Management.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 14 Rev#: 03 May, 2024
---	---	--

2.3 **Business Objectives**

PIACL Operations relies heavily on its computer network infrastructure and systems to carry out its business. Having a very well developed computer network and business critical applications to manage day-to-day operations and functions, the computer operations cannot function without the availability of these Application Systems. The dependency on these Application Systems makes it imperative that all systems shall be made available to the IT Infrastructure Division at all times to ensure continuity of business. Along with that the implicit and explicit business objective of this plan is to ensure that PIA regains the functionality of all its systems in the shortest time possible, in an event of disaster that renders the current systems infrastructure inaccessible, slow and/or “site down” situation.

2.4 **Plan Objectives**

- A. That in the event of a “**DISASTER**” situation, the computing resources and the network infrastructure is restored in the current premises or at an alternate premise in the shortest possible time.
- B. That the risk of loss of business and / or operating environment to the users of computer operations section is reduced.
- C. To alleviate the end-user from a possible event of disaster, damaging the operations and/or render them unsafe in the absence of communications network and/or computing resources.
- D. That the infrastructure and computing resources required to set-up an alternative working environment is achieved in the shortest possible time by using the available resources to their maximum potential.

2.5 **Assumptions (Check List)**

The key assumptions in providing IT Infrastructure Division an alternate site are:

- A. Physical access to the site is available to the Data Centre
- B. Requisite power requirements and backup generators are available.
- C. Necessary power outlets and required furniture is available.
- D. Main site is accessible.
- E. Regional support is available.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 15 Rev#: 03 May, 2024
--	---	--

Chapter - 3 Identification and Declaration of a Disaster

In a site-down situation, PIA ICT Department Leadership Team is only authorized/responsible for declaring a disaster at PIA ICT Department due to any incident. The PIA ICT Department Leadership Team will use the best possible communication method available to declare the disaster to the entire network. The declaration of a “**site down**” situation can also be based on recommendations from internal security organization of a situation that makes the access to the systems or the office infrastructure unsafe or not possible for any reason.

3.1 Criteria for Declaring a DISASTER

The following will be generally used as criteria for declaring a “**site down**” Disaster:

3.1.1 Situation

If conditions exist that make it unsafe to access the systems room from the office premises. This could be due natural calamity such as an earthquake, cyclone, or a law and order situation. The recommendations of our internal security organization will be sought before a decision is taken in this regard.

3.1.2 Identifying the extent of the Problem

The team will examine the situation and measure the extent of problem. After completing the initial examination process and determining the situation a decision will be take on the steps. In case the problem exists for an extended period of time or becomes unsafe to operate, a declaration will be considered.

3.1.3 Prognosis

Internal security recommendations will be sought on their prognosis of the problem or situation. If a prognosis exists of a situation that suggests that the access to the systems will become unsafe or not possible, then a decision will be made for the declaration of disaster.

3.2 Who Can Declare A Disaster

In PIA ICT Department, the **CIO (ICT)** can declare a disaster on receiving such recommendations from GM IT Infrastructure.

3.3 The People To Advise

Once a disaster is declared, the concerned people shall be informed of the situation and activation of the Disaster Recovery or Business Continuity Plan.

Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 16 Rev#: 03 May, 2024
---	---	--

Recovery Tasks	Responsibility
CIO declares the Disaster	IT Infrastructure Division's sectional teams and Network, Communication & IT Operational sectional Teams
GM IT Infrastructure Calls a meeting	IT Infrastructure Division, Network, Communication & IT Operation Division DGMs
Initiate DRP recovery of all the services	DGM IT Infrastructure & Data Center, DGM Database Administration, DGM System Administration, DGM Application Support, DGM Network, DGM Information Security
Confirm after complete system recovery/ restoration of services	Manager Database Administrations

3.4 How And When To Get In Touch With Them:

It will be the responsibility of the GM IT Infrastructure or in his absence the DGM Data Center and DGM IT Governance & Security to initiate procedure to contact of each person in the contact list and declare a disaster and activation of immediate Disaster Recovery Plan.

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY	Page 17 Rev#: 03 May, 2024
	Doc# : ICT/SBP/03	

Chapter - 4 What to Do in the First Instance

The first consideration that must be taken into account is the safety of all the Computer Operations Sections Personnel in the event of a “**site down**” situation.

4.1 Safety Concerns

It is the responsibility of the Data Center Manager to contact each person from the section and determine his or her current location. If any person is in a location that is considered unsafe then all arrangements must be made to evacuate the person to a safe location.

The following area shall be considered a safe location:

Karachi: Compound
 Computer Center Building,
 PIA Head Office, Karachi Airport.

All members of the core [Crisis Response Team](#) will be considered essential workers and must be sent to the above safe location.

4.2 Critical Resources To Be Retrieved

Many incidents do not completely destroy contents of offices. Depending on the circumstances, even if backup media such as computer diskettes, tapes and hard drives have been water, smoke or soot damaged, it might be possible to extract the information from them. Do not attempt to do this yourself. Contact your technical support area or facilities staff for help when the incident occurs.

Following the incident, if the Management and IT disaster recovery team facilities staff determine that affected building is safe to enter, IT disaster recovery team might be allowed into the building for a short time. This could be for as little as **15 minutes** or one **half-hour**. Create a list of the critical items that would be needed to retrieve providing entry into IT building is possible. This assumes, of course, that the items are salvageable.

List these items in order of importance.

4.2.1 **Some examples of items/action DGM Data Center need to retrieve include:**

Computer disks, computers, selected paper files and plans for work in process.

4.2.2 **Examples of items that shall not be included in the list:**

Family pictures, unimportant files and information that are duplicated somewhere else.

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 18 Rev#: 03 May, 2024
---	---	--

4.3 Critical Resources To Be Retrieved PROFORMA – CRRP01

The Critical Resource Retrieval Performa – CRRP01 is used to document the materials that shall be retrieved if ICT disaster recovery team is able to enter ICT facility following the incident and the items are not badly damaged.

The CRRP01 Performa documents information regarding the Nature of incident, Building/Floor, Items/materials to be retrieve along with their Complete “Condition” at the time of the incident.

Pivotal areas and corresponding focal action of the CRRP01 Performa is follows: -

PIVOTAL AREAS	FOCAL ACTIONS
CRITICAL RECRDS	
Last back taken on the backup media	To be collected first and stored safely
Data Disks	To be secured and catalogued
Plans / Work in hand	Work in hand secured
Files	Essential files to be retrieved & secured
EQUIPMENT	
Storage systems	To be secured
Systems and Servers	To be secured
Desktop Computers	To be secured
Firewalls	
Routers	
Switches	
OTHER	
UPS Systems	To be Checked
Battery Backups	To be Checked
Generators	To be Checked
Air conditioning systems	To be Checked

The Critical Resource Retrieval Performa – CRRP01 is provided as following separate attachment: -

- ITBKP- Critical Resource Retrieval Performa – CRRP01

Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 19 Rev#: 03 May, 2024
---	---	--

Chapter – 5 Activation of Disaster Recovery Process

It is the responsibility of GM IT Infrastructure to call for an immediate meeting of the Crisis Response Team, at the following location:

Karachi: **Computer Centre Building,**
PIA Head Office, Karachi Airport.

The **Crisis Response Team** will be comprised of the following:


Designation	Role
CIO (ICT)	Over all in-charge of all activities
GM IT Infrastructure	To recommend to declare a disaster
GM IT Infrastructure	Convene a meeting accordingly to assess the communication network.
DGM Systems Administration DGM Database Administration DGM IT Infrastructure & Data Centre DGM Communications DGM ERP Technical	To monitor and implement recovery plan
DGM Network	To ensure the operations network
Mgr. Data Center Mgr. Database Administration	To facilitate disaster recovery plan implementation

The Crisis Response Team meeting will be convened and officially informed about the decision to activate the Disaster Recovery Plan. The team will be advised that the Data Centre Manager will henceforth be considered the Project Manager for the Disaster Recovery Plan implementation.

5.1 Roles & Responsibilities

The “Roles & Responsibilities” chart will be discussed and each member asked to confirm that they are clear about their responsibilities.

Each member will be asked to study their responsibility and advise the Data Centre’s Manager on what assistance or resources they would require to complete their part of the activity for the Disaster Recovery Plan.

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY	Page 20 Rev#: 03 May, 2024
	Doc# : ICT/SBP/03	

Services

Infrastructure Services

Telecom Circuits

Network Cabling

PTCL Telephone lines

PABX system

FAX services

BackOffice setup

E-Mail Services

Internet services

Application services

Applications recovery

Data Base recovery

Help Desk & User Management

Computer Operations

Data Management and security

DRP Management

Responsibility

DGM IT Infrastructure & Data Centre
Mgr. Infrastructure Services

GM IT Operations
GM IT Infrastructure
Mgr. Infrastructure Services
DGM Communications
DGM Communications
DGM Communications
DGM Service and Support Centre
DGM IT Infrastructure & Data Centre
DGM Information Security

DGM Systems Administration
Mgr. Collaboration Services

Mgr. Network Services
Mgr. Information & Web Security

DGM Application Support
DGM IT Infrastructure & Data Centre
DGM Application Support
DGM Commercial Systems
DGM Operational Systems
DGM Functional Systems
DGM Software Development
DGM Project Management Office

Mgr. Database Administrator

DGM IT Infrastructure & Data Centre
DGM Service & Support Centre

Mgr. Operating System
Mgr. Database
Mgr. Data Centre

DGM Information Security

GM IT Infrastructure
GM IT Systems
PMO HEAD
DGM IT Infrastructure & Data Centre
DGM Network
DGM Communication
DGM Operations (Regional)
DGM Information Security
DGM Database
DGM Application Support

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY	Page 21 Rev#: 03 May, 2024
	Doc# : ICT/SBP/03	

Chapter – 6 Recovery Considerations:

Assessments of the current systems running at the section are determined; (hardware that is available to be moved to alternate sites). If any systems are physically damaged, backup data of the systems will be retrieved from backup storage sites for restoration.

IT Infrastructure Division maintains different levels of Data Backup of all ICTs systems. It will be the responsibility of the individuals handling the movement and /or setting up the Back Office Servers at the alternative site to load the backups, if necessary, on the main frame.

All queries regarding availability of Backup media, the levels of backup and the storage of backups must be made to the following individuals:

Data Center Section Karachi:

Manager Data Center

6.1 **Key Functions Necessary For Continued Operations**

The following necessary services need to be established to bring up the system at alternate locations.

- Installation and configuration of Network (Routers and Switches) at the alternate locations.
- Installation and configuration of Servers: This will provide connectivity of all users.
- Installation, configuration & set up of Server machines at new locations.
- Set up and connection of Desktop / Servers at the new locations.
- Establish connectivity to Servers.

Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 22 Rev#: 03 May, 2024
---	---	--

6.2 **RECOVERY STATUS REPORT FORM**

To log significant recovery activities, the Manager shall be required to submit written recovery status report(s) as and when required. The status report(s) may be submitted handwritten as long as it is legible. The prescribed form used for the purpose has been provided as separate attachment: -

- ITBKP-STATUS REPORT FORM – RSTRF01

Completed status report(s) shall be submitted to the Crisis Response Team.

6.3 **Recovery Steps**

The following recovery actions are to be used as a guide. During a real disaster circumstances may dictate that some or all of the steps documented may have to be altered. The team leader shall use his/her judgment while managing the recovery operation.

1. The team leader/Manager shall ascertain/determine the following: -
 - Availability of voice communications at all work areas.
 - When servers will be operational and how current/latest the master files will be.
2. Departmental Meeting:

Key department personnel shall meet to determine actions to be taken and establish the priority of restoring business functions based on the work area and resources available. The department leader / Manager shall explain the goals and objectives identified by the Crisis Response Team.

- a. Review tasks to be performed and assign personnel.
- b. Personnel shall be assigned to contact vendors and advise them about the situation and when they can expect service to be restored.
- c. Determine if some personnel will have to travel to the business recovery site.
- d. Distribute copies of any forms that will be needed during the recovery operation.
- e. Distribute copies of the news media statement that has been prepared. Copies can be obtained from the Crisis Response Team. Instruct everyone not to make statements to the news media.
- f. Personnel shall be assigned to provide recovery support needed by other teams, as needed.

Copy on Corporate intranet  PAKISTAN International Airlines <small>Great People to Fly With</small>	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 23 Rev#: 03 May, 2024
---	---	--

g. Identify the category in which personnel shall be alerted. Consider: -

- *Personnel that might be needed to give aid to other teams / departments.*
- *Personnel that will be needed at the work area to resume normal business functions.*
- *Personnel who shall stay home and remain on standby (they will be needed when the initial group needs rest).*

- 3. Contact personnel that will be needed to report to the assigned work area.**
- 4. Designate space for personnel reporting to the work area.**
- 5. Implement procedures to resume time dependent functions based on the priority established.**
- 6. Instruct all department personnel to carry photo identification with them at all times and be prepared to show it to security or local authorities.**
- 7. As progress continues during the recovery operation, the team shall be prepared to move back to the affected facility and resume normal business operations.**

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 24 Rev#: 03 May, 2024
--	---	--

Chapter – 7 Training and Exercises

Updated plans are not enough if the people assigned to recovery teams don't know what is expected of them. Team members shall receive training on recovery concepts in general and their team's functions in particular. Exercises help identify needed improvements in strategies and plans. Exercises also give team members valuable experience in dealing with the challenges inherent in recovery operations.

The Business Continuity Group conducts training and exercises.

Team Member Orientation. This is a one-hour overview of the Business Continuity Plan. Each team member shall attend **once per year**. It is also available for the general employee population. This mainly focus on but not limited to the following: -

1. Introduction to PIA ICT
2. Introduction to Policies and Procedures within ICT
3. Overview of applications / servers
4. Overview of the Backup Policy

Team Exercise. The team participates in a two-hour tabletop exercise with a focus on their recovery strategies.

Team Leader Exercise. All the team leaders and Alternate Team Leaders participate in a two-hour tabletop exercise with a focus on facility wide recovery.

Functional Exercise. Actual hands-on test of hardware or connectivity capability at Work Area Recovery Centers. Actual use of alternate (manual) production process at the home or alternate facility.

Activity Schedule

This document allows Team Leaders to track their own plan review, training and exercise activities for the year. The Business Continuity Group will periodically request a copy of the document to review the team's preparedness status. A new document will be started each year. The Business Continuity Group will keep each year's completed activity schedule on file for audit purposes.

Copy on Corporate intranet  PAKISTAN International Airlines Great People to Fly With	ICT SYSTEM BACKUP POLICY Doc# : ICT/SBP/03	Page 25 Rev#: 03 May, 2024
---	---	--

Performa ACTS01
ACTIVITY SCHEDULE

Plan Reviews

Enter the dates when plan reviews were conducted.

Plan Holders	Due Jan 1	Due Jul 1
Team Leader (Name)		
Alt. Team Leader (Name)		
(Name)		
(Name)		
(Name)		
(Name)		

Training / Exercises

Enter the dates and number of participants for each activity. Each exercise type is expected to be conducted at least once per year.

Activity	Date Conducted	# of Participants	Comments
Orientation			
Team Exercise			
Team Leader Exercise			
Functional Exercise			

Team Leaders: Attach participant sign in sheets, evaluations and comments to this sheet.

Send this page to the Business Continuity Group no later than December 1.

Copy on Corporate intranet 	ICT SYSTEM BACKUP POLICY	Page 26 Rev#: 03 May, 2024
	Doc# : ICT/SBP/03	

Disaster Recovery Team / Business Continuity Group

DGM IT Infrastructure & Data Centre
DGM Database Administration
DGM System Administration
DGM Application Support
DGM Communication
DGM Network
DGM BI & Analytics
DGM Information Security
DGM IT Ops, Central
DGM IT Ops. South
DGM IT Ops. North
DGM Vender Management Office
DGM PMO
DGM ERP Technical
DGM Software Development
DGM Operational Systems
DGM Commercial Systems
DGM Service and Support Centre
DGM Functional Systems

Manager Data Centre (DR)
Manager IT Infrastructure & Data Centre
Manager NOC
Manager Database Administration
Manager Systems Administration
Manager Operational Systems
Manager Commercial Systems
Manager Functional Systems
Manager Software Development
Manager Application Support
Manager Communications
Manager Network Services
Manager Network Security
Manager ICT Risk Assessment
Manager Collaboration Services
Manager Information Security
Manager Information & Web Security
Manager ERP
Manager PMO

Chief Information Officer

General Manager IT Operations
General Manager IT Systems
General Manager IT Infrastructure
PMO-ERP HEAD