	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015


DELHI INTERNATIONAL AIRPORT PRIVATE LIMITED

INDIRA GANDHI INTERNATIONAL AIRPORT

Policy for Organization of Information Security

		ISSUED BY	VERIFIED BY	APPROVED BY
Name:		Rajneesh Yadav (Manager IT)	Latif Bin Kosnan (Lead Information Governance & Security)	Davesh Shukla (CIO)
Title:		Information Security Policy	Information Security Policy	Information Security Policy
Date:		17-Mar-2011		
Signature:				
Revision No.	Revision Date	Reviewer Name	Approver Name	Brief Description of Amendments
01	14-Sep-2015	Dheeraj Gehani	Davesh Shukla	Reviewed, No changes

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 1, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015 Effective Date: 14-Sep-2015

1.0 Purpose

The objective of this policy is to ensure effective information security management framework within the organization with clearly laid down roles and responsibilities.

2.0 Scope

This policy is directed by DIAL Senior Management and all the staff / managers identified and assigned with security related tasks for Data Centre / Network Operation Centre / IT Security Operations Centre.

3.0 Policy

3.1 Roles and Responsibilities

3.1.1 Chief Information Security Officer (CISO)

Reports To:

Chief Information Officer (CIO)

Supported By:


Personnel in the System Administration Team, Network Administration Team and Information Security Management Team.

Duties & Responsibilities:

The Information Security Officer is responsible for preparing, maintaining and communicating Information Security Policies & Procedures within DIAL. Being the administrative head of the Security Organization Structure; ISO serves as the focal point for deciding on all Information security issues. ISO is also responsible for creating security awareness in DIAL His/her major responsibilities are to:


- Lead the System Administration Team and Information Security Management Team in the information security related activities.
- Prepare security briefs for Information Security Management Team.
- Maintain ISMS.
- Establish the Security Risk Assessment Process, and Review Risk Assessment Reports and status.

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 2, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

- Establish and support the Risk management process for DIAL Information systems.
- Select controls and risk mitigation.
- Maintain the Statement of Applicability.
- Monitor ongoing compliance with security standards.
- Establish and maintain contacts with external security resources.
- Evaluate changes in asset base and resultant security implications.
- Manage the timely resolution of all issues and questions regarding responsibilities for Information security management within DIAL that relate to achieving and maintaining full compliance with the Information Security Policies and Procedures.
- Ensure that responsibilities are defined for, and that procedures are in effect, to promptly detect, investigate, report and resolve Information security incidents within DIAL.
- Seek legal guidance in case of illegal activities or hacking related to DIAL. Notify such issues to the senior management and to the Information Security Management Team immediately.
- Evaluate and recommend on new security products to be implemented across DIAL.
- Initiate protective and corrective measures if a security problem is discovered.
- Prepare Security Procedures for monitoring the IT infrastructure and processes for DIAL, including procedures for monitoring and reacting to system security warning messages and reports.
- Ensure that the staff members are adequately trained on the domain of physical security to meet the security requirements of DIAL.
- Analyze reports submitted and the work performed by System Administration and Information Security Management Teams and take corrective action.
- In co-ordination with Information Security Management Team, issue

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 3, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

guidelines, incorporate appropriate procedures, conduct routine internal audit checks to verify the compliance to the Information Security Policies and Procedures and detect incidents.

3.1 .2 System Administration Team (one full time SA and one backup from Tech.)

For DIAL External Networks

Reporting To:

Technical Manager/Information Security Officer (ISO)

Supported By:

- Tech. personnel overseeing:
- Network and telecommunications
- Internet Access
- E Mail System
- Routers, switches and other networking components.
- Firewalls


Duties & Responsibilities:

Summary:

This team is responsible for maintaining security of DIAL networks and information processing facilities. This includes ensuring that all ITC network resources are protected from unauthorized access, initiating corrective measures and reporting security breaches.

Description:

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 4, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

- Enforce logical security measures over networking systems
- Ensure that all ITC networking resources are protected from unauthorized access
- Assess vulnerabilities in the present networking system
- Monitor Firewall Security
- Monitor Router Security
- Review network logs and incidents
- Ensure security of network O/S

Reporting Responsibilities:

To report on:

- Status of implementation of Information Security Policies & Procedures relating to Networking
- Any problems encountered in their implementation
- Security breaches / incidents

Profile:

- System Administrator Team members will be employees of DIAL.
- They will have a sound technical knowledge of WAN & networking systems used in Information technology.
- They must have prior experience in Information systems security.

For Local Area Networks

Reporting To:


Technical Manager /Information Security Officer (ISO)

Duties & Responsibilities:

Summary:

This team is responsible for implementing Information Security Policies & Procedures relating to Local Area Networks and desktops. This includes enforcing logical and

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 5, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

physical security measures over Local Area Networks, initiating protective and corrective measures if a security problem is discovered and reporting security breaches.

Description:

- Ensure that LAN access is duly authorised
- Ensure that user privileges at the L N level are based on a “need to know/ need to do” basis
- Review LAN security parameter settings & network logs
- Monitor network security breaches, unusual login times, password change history, locked-out user-ids, etc.

Reporting Responsibilities:

To report on:

- Status of implementation of Information Security Policies & Procedures relating to LAN & desktop security
- Any problems encountered in their implementation
- Security breaches / incidents

3.1.3 Information Security Management Team

Reports To:

Information Security Officer (ISO)

Supported by: Members from each department / function


Duties & Responsibilities:

Information Security, Incident Response, Internal Audit, Business Continuity/Disaster Recovery for DIAL

Information Security:

- It is the primary responsibility of this team to maintain information security

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 6, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

within DIAL in accordance with the ISMS

- Implement the ISMS – the policies, procedures, and the controls – administrative, physical, and technical to ensure information security objectives are attained
- Maintain records of the changes made to the systems including the Operating System versions, configurations, patches etc.

Incident Response:


- Prepare to respond to an incident
- Identify/record the incident
- Contain the incident
- Eradicate the intruder
- Methodologies include processes to Identify, escalate, and de-escalate security events
- Assess and maintain organizational security
- Establish external liaisons with local law enforcement agencies, as well as with legal and public relations entities.
- Recover from the intrusion
- Assist in root cause analysis of the incident

Reporting Responsibilities: Report identified incidents and actions taken to ISO.

Internal Audit:

- To conduct the ISMS audit at least once in a year or as directed by the ISO.
- To plan Audit programs by considering the status and importance of the processes and areas being audited as well as the results of previous audits.
- Auditors will not audit their own work

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 7, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015 Effective Date: 14-Sep-2015

- The audit will be conducted to determine whether the control objectives, controls, processes and procedures of ISMS
- Conform to the requirements of the ISO27001 standard
- Conform to the identified information security requirements
- Are effectively implemented and maintained
- Perform as expected (by measuring effectiveness of controls)

Reporting Responsibilities: To report on the reviews with findings and opinions on the required improvements.

Business Continuity / Disaster Recovery

- Assist in identifying critical assets / services / processes required to recover from interruptions
- Assist in defining Recovery Time Objectives, Carrying out business impact analysis
- Participate in conducting tests to recover from interruptions
- Identify and improve upon weaknesses in recovery tests
- Maintain an updated and current BCP / DRP
- Participate in recovery operations in case of business interruptions and disasters.

Reporting Responsibilities:


Report on testing and implementing the business continuity plan.

3.1.4 Information Owner

Duties & Responsibilities:

- a. All Information systems possessed by or used by a business or support unit within DIAL must have a designated owner. Information owners are

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 8, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015


responsible for assigning appropriate sensitivity classifications (confidential, Internal, Public), authorizing access to their Information, assigning an Information custodian, and specifying and communicating the security requirements to Information Security Officer and System Administrator, including any additional protection requirements above the minimum required.

- b. The data owner must also ensure that effective monitoring of the controls and protective measures are in place, and that all security breaches are appropriately investigated and resolved. The data owner may delegate the authority for making these decisions to others in his/her department, but may not delegate the responsibility.
- c. System Administration / Technical Team supports, manage, and maintain much of the information used in DIAL. As for new Information systems, the Information owner is responsible for defining the protection requirements for the systems managing his/her Information. These requirements include, but are not limited to, access control and management, data retention and destruction, backup requirements, and disaster recovery parameters. Information systems with significant business value must be under appropriate change management mechanism, i.e. change management procedures must be authorized and approved by the owner and the departmental head.
- d. The role of Data Owner will be determined based on the following considerations:
 - i. Who originates / manages the data and information
 - ii. Who is responsible for the accuracy and integrity of data / information
 - iii. Who budgets the costs of creating, processing, storing, transmitting and using of data
 - iv. Who has the most knowledge of the Information asset's business value
 - v. Who would be impacted by a security breach of the Information asset

To summarize, following will be the roles and responsibilities of Data Owners:

- a. Identify data that requires restricted access.
- b. Define access authorization privileges for their Information and, where

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 9, Total 4
-----------------------------	----------------------------	-----------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
IT&C	Information Security Policy	Revision No: 01
		Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

relevant, the computer applications that process their Information.

- c. Define security requirements to be built into the system.
- d. Define records retention and destruction schedules for their data which comply with operational, legal and regulatory requirements
- e. Communicate the need for “Information protection” as appropriate to Information security officer.
- f. Along with Information Security officer, decide on the actions in case of violations of the standards by the users.
- g. Review and approve requisition for granting access.
- h. Review and approve requisition for changes to the computer applications that process their Information.

3.1.5 Information User

Duties & Responsibilities:

- a. Information is important and pervasive throughout DIAL. All users have responsibility to protect the Information entrusted to their care.
- b. All users who may come into contact with “sensitive” Information (non-Public) are expected to familiarize themselves with the Information classification policy and the guidelines supporting it, and to consistently apply these in their information creation, handling and processing, distribution and destruction as necessary.


4.0 Point of Contact

Chief Information Security Officer (CISO).

5.0 Enforcement

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of DIAL senior management. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of a DIAL vendor, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Prepared By: Rajneesh Yadav	Approved By: Davesh Shukla	Page 10, Total 4
-----------------------------	----------------------------	------------------

	Information Security Management System	Internal
		DIAL/ISMS/POL/017
		Revision No: 01
IT&C	Information Security Policy	Issue Date: 14-Sep-2015
		Effective Date: 14-Sep-2015

6.0 Reference

- ISO 27001: Control A.5 (Information Security)

7.0 Annexure

- Abbreviations:
DIAL – Delhi International Airport Private Limited.
- Definitions: Nil