Government of Sultanate of Oman

Information Technology Authority

ITA Information Security Policy Manual

Created By	**Governance & Advisory Division, ITA**
Effective From	**01 May 2008**
Approving Authority	**Chief Executive Officer, ITA**

Information Technology Authority

P. O. Box: 1807, Postal Code: 130, Al Athaibah, Muscat, Sultanate of Oman

Phone: +968-24691511 / +968-24692797, Fax: +968-24695812

http://www.ita.gov.om

Document Name	ITA Information Security Policy
Document Number	ITA_IS_POL_001
Version Number	1.0
Document Stage	Approved
Published Date	01 May 2008
Standard Number	ITA
Archival Format	Acrobat (Pdf)
Archival Location	ITA INTRANET
Publishing Medium / Media	ITA INTRANET
Author (s) / Document Owner	Governance & Advisory Division, ITA
File Name	Information Security Policy
Copy right information	Not for use outside ITA
Confidentiality Information	ITA Confidential

Revision History

Version	Date of Revision	Prepared / Updated By	Reviewed By	Reason for Change	Affected Sections
1.0	01-May-2008	Governance & Advisory Office		First Version Published	All Sections

Table of Contents

Foreword

Information is one of the most valuable assets of ITA. An Information Security Policy is an important requirement to protect this valuable asset. The **ITA Information Security Policy Manual** covers key areas of concerns related to Information Security.

The policies listed in the manual are brief, simple and direct and are based on industry best practices. The manual is a "living document" and shall be regularly reviewed and updated to take into consideration the changing security landscape, the expanding resources and asset base of ITA and the evolving International Standards / Best Practices.

All ITA Employees and service providers to ITA are responsible for securing information and are required to comply with the Information Security Policy and related requirements. The policy applies to all projects and programs initiated by ITA. All managers and staff managing projects and operations are responsible for implementing effective measures and safeguards to protect information and associated assets.

-Signed-
Dr. Salim Sultan Al Ruzaiqi
Chief Executive Officer

0. Introduction

Information exists in ITA in many forms – stored / transmitted electronically or in a written / printed form or shared during spoken conversations. Information is a valuable asset for ITA and is essential for ITA to:

- Protect this valuable asset from unauthorized or accidental access and modification and
- Ensure availability of this information to the right people at the right time.

This manual outlines the policy framework for establishing Information Security in ITA and discusses how ITA will manage, protect and distribute sensitive information.

The policy manual is divided into two parts: **High-Level Policies** and **Detailed Policies**.

Part I: High-Level Policies. This part discusses policies at a higher level and contains three policies:

- **Information Security Policy**: This policy set by the senior management establishes the management direction, support and commitment for Information Security initiatives in ITA.

- **Acceptable Use Policy**: This policy defines acceptable practices relating to the use of ITA's Information resources which includes but not limited to the computing equipment, software, network services Email, Internet / Intranet and storage media. This policy contains the minimum that every employee should know.

- **Security Awareness Policy**: This policy informs staff that security is everyone's responsibility and that everyone is required to learn about security and to attend events / trainings / workshops concerning security.

Part II: Detailed Policies: This part divides security policies into ten main areas: Data Ownership, Antiviral and Malicious Programs, Internet-related Policies, Access Control, Network Policies, Legacy and Web Applications, Physical Security, Operations Management, Business Continuity Policy and Personnel & Third Party policies. Each area is subdivided into additional policies addressing the totality of information security.

An Information Security Officer will co-ordinate and supervise the implementation of all security policies.

Part I: High-Level Policies

1. Information Security Policy

1.1. Purpose

The purpose of this policy is to:

1.1.1. **Establish** the management direction, support and commitment for Information Security initiatives in ITA.

1.1.2. **Inform** all ITA personnel, other government agencies, customers and business partners who have access to ITA information of their responsibilities and obligations with respect to Information Security.

1.1.3. **Ensure** that adequate resources are applied to implement an effective Information Security Management System.

1.1.4. **Identify and Minimize** risks and the extent of loss or damage from a security breach or exposure to ITA, the Government, customers and business partners

1.1.5. **Ensure** the continuity of services to ITA's customers and business partners

1.1.6. **Identify** and review security metrics on an ongoing basis to ensure the effectiveness of the Information Security measures

1.2. Scope

This policy covers all forms of information and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.

The policy covers:

1.1.7. All Users of ITA information, including service providers of ITA.

1.1.8. **Facilities:** Includes all equipment, as well as the physical and environmental infrastructure:

- Computers of all sizes, whether general or special purpose, including Personal Computers. Peripherals, Workstation and Access Devices.
- Telecommunications and Data Communications cabling and equipment. Local and Wide Area Networks.
- Environmental control systems including air-conditioning and other cooling and safety equipment, alarms and safety equipment
- Utility Services including electricity, gas and water
- Buildings accommodating personnel and equipment.

1.1.9. **Data:** Includes both raw and processed data:

- Electronic data files, regardless of their storage media including hard copies and data in transit
- Information derived from processed data regardless of the storage or presentation media.

1.1.10. **Software:** Includes locally developed programs and those acquired from external sources:

- Application Software, Operating System software and all associated utilities and support programs
- Application enabling software including data base management, middleware, telecommunications and networking software

1.1.11. **Paper Documents:** include systems documentation, user manuals, continuity plans, contracts, guidelines and procedures.

1.1.12. **Personnel:** include employees, contractors, consultants, service providers, representatives of customers and other bodies that access ITA's information and data.

1.3. Policy

1.3.1. ITA shall implement all relevant and all possible measures to achieve the following security objectives.

1.3.1.1. **Availability:** Adequate controls / safeguards shall be in place to ensure accessibility of information and deliverability of services to authorised users, customers and business partners when required and ensure recoverability in the event of a disruption.

1.3.1.2. **Integrity:** Adequate controls / safeguards shall be in place to ensure completeness and accuracy of Information during the capture, storage, processing and presentation of information and protect against unauthorised modification or destruction.

1.3.1.3. **Confidentiality:** Adequate controls / safeguards shall be in place to ensure that information is being made available or disclosed to authorised processes, entities or individuals **ONLY**.

1.3.1.4. **Authenticity:** Adequate controls / safeguards shall be in place to uniquely identify users of information assets to the information being accessed.

1.3.1.5. **Accountability:** Adequate controls / safeguards shall be in place to ensure responsibility for information and actions undertaken by providers and users of information.

1.3.2. Information assets owned, leased or rented by ITA shall be solely for the conduct of ITA business; no private use, or use for any other purpose shall be permitted.

1.3.3. All of ITA's critical assets (e.g. hardware, software, equipment and data) should be identified and appropriately protected. A formal Inventory of all assets should be compiled. All Assets and Information should be appropriately classified and labelled as per the business's requirements.

1.3.4. Information security education, awareness and training shall be made available to ITA personnel.

1.3.5. This Information Security Policy and supporting Policies, Procedures and Guidelines not limited to Information Security will be made available online format through the Intranet System.

1.3.6. The Information Security policy, supporting policies, guidelines and procedures should be reviewed on a half-yearly basis.

1.3.7. Compliance with the Policy will be monitored on a regular basis. Security logs and audit trails will be produced to monitor the activities of users in their usage of information assets.

1.3.8. All access to corporate resources and information should be on a 'Need to Know' basis. Resource rights which are not explicitly assigned should be assumed to be denied.

1.3.9. An Information Security Officer should be nominated to co-ordinate the implementation of all security policies and related security initiatives and tasks. An "Information Security Forum" and / or an "Information Security Steering Committee" may be created as appropriate.

1.3.10. The Information Security Officer will ensure that security issues are addressed and will devise a mechanism to prevent recurrence in the future.

1.3.11. When information is transmitted outside ITA, special measures should be taken to secure it.

1.3.12. The software developed for or used in ITA should undergo a proper security approval prior to moving to the production environment.

1.3.13. ITA reserves the right to monitor information traffic and all communication regardless of the medium being used.

1.3.14. The perimeter network should be appropriately protected with proper hardware and software. Proper monitoring of the perimeter network and internal network should be done on a regular basis.

1.3.15. To provide protection against common threats to ITA, appropriate safeguards should be in place, including anti-virus programs, firewalls, Intrusion Prevention Systems (IDS) and other technology requirements.

1.3.16. Regular checks on network, servers and other equipment should be conducted in order to make sure that the network is secure.

1.3.17. Proper and detailed procedures should be developed for implementing security.
1.3.18. All sensitive logs should be written on a CDROM to avoid alteration attempts. Only authorized persons should review the logs.
1.3.19. All documentation in the company should have a version control page with the document's history. All pages should be numbered.
1.3.20. All security incidents, weaknesses and breaches of information security, actual or suspected shall be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response.
1.3.21. Disciplinary action, ranging from verbal reprimand to termination of employment, depending on the severity of the violation, may be taken.
1.3.22. The Computer Incident Response Team should have a documented Computer Emergency Response Plan which includes all necessary procedures.
1.3.23. Proper checking for vulnerability of all systems should be carried out on a regular basis with the help of a Penetration Test.
1.3.24. Physical security is of prime importance. All efforts should be made to secure the physical perimeter, physical entry points, office rooms and delivery/loading areas.
1.3.25. Proper measures should be taken for securing all equipment, power supplies and cables.
1.3.26. Security of equipment while being maintained off-premises should be assured.
1.3.27. All employees and contractors should wear their identity badges and ensure it is visible when on the company premises.
1.3.28. Discussion of sensitive information in public places such as elevators or cafés is strictly prohibited.
1.3.29. All advertisements for jobs and help should be reviewed thoroughly and should not disclose any sensitive information.
1.3.30. If an ITA employee is presenting a paper, giving a presentation or delivering a speech in a public forum or conference, all material must be reviewed by his/her immediate manager prior to presentation.
1.3.31. An annual Information Security Audit should be performed to check the effectiveness of implemented controls. The report of the audit shall be reviewed by the management and appropriate measures taken to enhance security within ITA on an ongoing basis.
1.3.32. A proper Business Impact Analysis and Risk Assessment should be performed for all critical business systems, either by the Information Security Officer or by an outsourced resource as appropriate.

1.3.33. ITA should comply with all the legal requirements as specified by the Government of Oman. Employees shall not indulge in an activity that is illegal under the local or international law.

1.3.34. All concerned should ensure compliance to this policy, the other policies included in the manual and related standards, procedures and guidelines (outside this manual).

1.4. Approach

An **Information Security Management System (ISMS)** is a systematic approach to manage information so that it remains secure. ITA shall adopt international standards and best practices to implement an ISMS. The ISMS shall include all of the policies, procedures, plans, processes, practices, roles, responsibilities, structures, resources (Hardware and Software), that are used to protect and preserve information.

As a part of the ISMS, risk management techniques and processes shall be continuously employed to:

- Identify and determine the value of Information Assets to ITA and
- Implement appropriate protection measures based on the identified value and associated risks**.**

The risk management process shall take into consideration the relevant legal and statutory compliance requirements.

1.5. Enforcement

In the case of violation of the policy, guidelines or procedures, disciplinary action will be taken which may include the termination of employment.

1.6. Responsibilities

1.6.1. The Manager responsible for Information Security, shall co-ordinate the development of guidelines and procedures for the implementation of this policy, and will be responsible for an on-going review of their effectiveness. The Manager must ensure that all personnel are fully informed of their obligations and responsibilities with respect to these guidelines and procedures.

1.6.2. All personnel, whether employees, contractors, consultants or visitors, are required to comply with the information security policies, guidelines,

procedures and mechanisms and to play an active role in protecting the information assets of ITA. They must not access or operate these assets without authority and must report security breaches or exposures coming to their attention to the Manager responsible for Information Security.

1.6.3. Managers have a responsibility as custodians of the data and other information assets that support the business activities performed under their supervision to ensure that those assets are adequately secured. They must also ensure that the appropriate information security guidelines, procedures and mechanisms are observed in the performance of these activities.

1.6.4. The Information Security Officer is responsible for the day-to-day administration of the information security procedures and practices. This person reports directly to the Manager responsible for Information Security on the performance of the information security procedures and practices.

2. Acceptable Use Policy

2.1. Purpose

The purpose of the Acceptable Use Policy is to communicate the acceptable behavior of the employee which is necessary to ensure security of the systems, assets and information.

2.2. Scope

The scope of this policy covers all permanent/contract employees, consultants and vendor/third parties' assigned persons working for ITA.

2.3. Policy

2.3.1. Security is everyone's responsibility every day. All employees of ITA should follow the security policies applicable to their area.

2.3.2. ITA resources (including but not limited to Email and Internet) are meant for business use and should be used for business purposes only.

2.3.3. From time to time ITA's nominated Information Security Officer will be issuing guidelines that need to be followed.

2.3.4. An excuse of unawareness of a security policy will not be acceptable.

2.3.5. All of the information stored on or transmitted over ITA's resources remains ITA's property and ITA has the right to monitor and audit them.

2.3.6. All of ITA's confidential information should be treated in strict confidence. Copying or transmitting of the information is strictly prohibited except when required for ITA business.

2.3.7. It is the employee's responsibility to protect all of the passwords and pass phrases assigned to them. They should not share these with any other person.

2.3.8. A password should be changed as per the password policy.

2.3.9. All desktop computers and laptops must have a password-protected screensaver which should activate after a period of no longer than 10 minutes of non-usage.

2.3.10. All sensitive information stored in a laptop should be password protected.

2.3.11. All computers and related devices should run the latest antiviral software. No employee is allowed to disable are deactivate the virus detection engine.

2.3.12. The e-mail and Internet policies should be followed while using e-mail or the Internet.
2.3.13. No unauthorized copying of software is allowed.
2.3.14. No ITA resources should be used to test software as it may malfunction or be malicious in nature. An exception is made for software that is to be used in ITA.
2.3.15. No person is allowed to browse the company network from his PC or any other resource.
2.3.16. Probing and port scanning of external and internal servers is strictly prohibited unless it is part of the official penetration test undertaken by ITA and appropriate counter measures are taken.
2.3.17. No vulnerability probing or similar software should reside on any computer except when being used by the system administrator for the purposes of assessment. As soon as the assessment has been completed, all such software should be removed from the system.
2.3.18. At the end of a meeting, all white boards should be cleaned and flip-chart paper removed.
2.3.19. A 'Clean Desk' policy should be observed throughout ITA.
2.3.20. No games should be stored or played on ITA computers.

2.4. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

2.5. Responsibility

All Employees.

3. Security Awareness Policy

3.1. Purpose

The purpose of this policy is to keep employees up to date with information security which is changing at an astonishing pace.

3.2. Scope

The policy applies to all employees, irrespective of the positions being held.

3.3. Policy

3.3.1. The Information Security Officer will organize at least one workshop per year and the attendance of every employee will be mandatory.

3.3.2. In the case where an employee has not attended the workshop, his/her respective manager will be informed.

3.3.3. If necessary, the Information Security Officer takes help of brochures, Posters and/or special Security Awareness Screen Saver to increase the Information Security.

3.3.4. A Security Awareness Booklet and Brochure will be given to every new employee. The last page will be the “Undertaking” that needs to be signed by the employee.

3.3.5. It is the responsibility of every individual to keep him/herself up to date through involvement in security trainings conducted by ITA. .

3.3.6. Any security breach or query about security should be communicated to the Information Security Officer immediately.

3.3.7. Knowledge of security policies is one of the areas that will be assessed during appraisal of the employee.

3.4. Enforcement

In case of a policy violation, disciplinary action will be taken which may include the termination of employment.

3.5. Responsibility

All employees, especially the Information Security Officer and IT manager.

Part II: Detailed Policies

Data Protection and Ownership Policies

4. Data Protection Policy

4.1. Purpose

The purpose of the policy is to implement proper data ownership for Information Security. The owner of the data needs to be clearly specified with corresponding duties and responsibilities.

4.2. Scope

The policy applies to all employees who at any time are responsible for data handling, using and owning.

4.3. Policy

4.3.1. The Data Owner should be specified for each application. The Data Owner is the person who heads or leads the business unit. For example, the finance department manager owns finance data, not the IT Department. IT is merely the “Data Custodian” or the “Data Trustee”.

4.3.2. The Data Owner will communicate the importance of the data, level of sensitivity, controls and monitoring requirements to the Data Custodian.

4.3.3. The Data Custodian may not take any action on the data without the permission of the Data Owner.

4.3.4. It is the responsibility of the Data Custodian to ensure that data is backed up and stored at a secure place.

4.3.5. The Data Custodian will make sure that there are proper safeguards in place to recover from any Disaster.

4.3.6. Any data which is not on the server or is not backed up by the corporate backup facility, e.g. laptop or workstation data will be the responsibility of the end-user to make sure that recovery is possible in the case of system failure or hard disk crash.

4.3.7. The Data Custodian will make sure that all adequate controls are in place, as specified by the Data Owner.

4.3.8. The Data Custodian should maintain proper documentation of all activities involving the Owner's data.

4.3.9. The Data Custodian will inform the Data Owner of any risk or shortcomings as soon as they are identified.

4.4. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

4.5. Responsibility

Data Owner, Data Custodians, Information Security Officer and IT manager.

5. Information Safeguarding Policy

5.1. Purpose

This policy specifies the control and proper safeguard of information generated, stored and transmitted in ITA.

5.2. Scope

The policy applies to all forms of information regardless of what medium is used for their storage and communication.

5.3. Policy

5.3.1. The desktop owner will decide about the frequency of their data being backed up, on the basis of importance and retention period of the information.

5.3.2. Corporate Server backup frequency and retention should be defined and implemented by coordination of data owner, IT manager and Information Security Officer.

5.3.3. All backup should be verified to ensure that it is restorable.

5.3.4. Off-site backup of data and applications on critical machines is highly recommended, and should be carried out at least fortnightly.

5.3.5. Use of floppy discs should be avoided. CD-ROMs should be used for the backup of configuration and other files.

5.3.6. The Data Owner should specify the data retention period.

5.3.7. No pirated or other illegal software may be used in ITA.

5.3.8. Any software bought from outside vendors or contractors should be installed only after proper permission from the department head and Information Security Officer has been obtained.

5.3.9. The Application Program and data should be separated for security purposes.

5.3.10. All software should be tested in the test environment prior to being moved to the production machines.

5.3.11. Proper measures such as the installation of anti-virus software, firewalls, IDS, sniffer and others should be taken to address external and internal threats.

5.4. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

5.5. Responsibility

All employees, Departmental Managers and Information Security Officer.

Anti-Virus and Malicious Program Policy

6. Antiviral Policy

6.1. Purpose

This document specifies ITA's policy related to malicious programs i.e. Viruses, Worms, Trojans and others.

6.2. Scope

The scope of the policy includes all electronic communication mediums as well as all storage media which can be infected or can store or propagate malicious programs.

6.3. Policy

6.3.1. All computers and devices should run the latest anti-virus software as approved by ITA management.

6.3.2. E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail which he/she thinks may contain virus.

6.3.3. All removable media (e.g. floppy and others) should be scanned for viruses before being used.

6.3.4. No pirated software should be used on the corporate network.

6.3.5. In the case of a virus being found, the Information Security Officer should be informed immediately. The Information Security Officer will investigate and take proper measures to avoid the event in future.

6.3.6. No user should clean a virus from a computer unless authorized by the Information Security Officer.

6.3.7. All encrypted material should be decrypted and checked for viruses before being used.

6.3.8. The e-mail Server should have the antiviral program installed and must check all of the e-mail attachments before sending it to individual mail box.

6.3.9. All of the updates to the antiviral program should be automatic from the web or from a central server.

6.3.10. Antiviral Program should be supplemented by following components:

- Personal Firewall
- Antispyware and related safeguards

6.4. Enforcement

In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination.

6.5. Responsibility

All employees, IT Manager and Information Security Officer.

Internet-Related Policies

7. Internet Usage Policy

7.1. Purpose

This document specifies ITA policy related to Internet Usage.

7.2. Scope

The scope of the policy includes all employees, irrespective of their position.

7.3. Policy

7.3.1. Only official Internet connections should be used. No one is allowed to connect to the Internet through a PC modem, as this would open an unsecured backdoor to ITA.

7.3.2. Internet facilities will be provided to only those employees who need them for business use. No Internet usage for personal purposes is allowed.

7.3.3. While using the Internet, no person is allowed to abuse, defame, stalk, harass or threaten any other person, or violate local or international legal rights.

7.3.4. No person is allowed to upload, post, publish or distribute any inappropriate, indecent, obscene, profane, infringing, defamatory or unlawful information or material on the Internet while using the corporate resources.

7.3.5. No person is allowed to post personal advertisements or offer any goods or services using ITA's resources.

7.3.6. A visit to any obscene or socially unacceptable sites or sites which are non-business related will be considered a serious offence.

7.3.7. No one is allowed to use the chat services such as MSN, Yahoo and ICQ. If any of these are to be used to communicate with a foreign consultant for problem solving or discussion purposes, prior permission from the relevant manager is required.

7.3.8. Internet Telephone facilities or Internet NetMeeting should not be used to discuss sensitive business information.

7.4. Enforcement

In the case of a violation of the security policy disciplinary action will be taken, up to and including employment termination.

7.5. Responsibility

All employees, IT Manager and Information Security Officer.

8. E-Mail Usage Policy

8.1. Purpose

This document specifies ITA policy related to e-mail usage, including the receiving, replying, forwarding and auto reply functions.

8.2. Scope

The scope of the policy includes all permanent and contract employee irrespective of their position in ITA.

8.3. Policy

8.3.1. The e-mail facility is for business use only. The e-mail address allocated to an employee should not be used for personal purposes.

8.3.2. No free e-mail facility should be used to receive or send business-related information.

8.3.3. No non-business-related newsgroup may be added to your ITA e-mail address book.

8.3.4. The e-mail facility of ITA should not be used to spam others users, whether inside or outside ITA.

8.3.5. No harassing or insulting messages should be sent inside or outside of ITA.

8.3.6. No person is allowed to forward chain letters or pyramid schemes using the corporate e-mail.

8.3.7. No confidential document belonging to ITA may be sent to any one, including to your own personal free-mail account.

8.3.8. If sensitive information needs to be sent to someone outside ITA, proper measures should be taken as specified by the Information Security Officer.

8.3.9. ITA e-mail address should not be used when posting to newsgroups, as it may disclose ITA information. However, business-related newsgroups could be subscribed to using ITA e-mail address, provided permission is obtained from the respective manager.

8.4. Enforcement

In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination.

8.5. Responsibility

All employees, Departmental Managers and Information Security Officer.

Access Control Policies

9. Login Policy

9.1. Purpose

This document specifies ITA policy relating to login access to ITA information systems and computer resources and discusses in detail the related standards.

9.2. Scope

The scope of the policy includes all logins to applications and servers, irrespective of their operating platforms.

9.3. Policy

9.3.1. Every user should have a uniquely assigned login name and password to access corporate computer systems.

9.3.2. Each person is responsible for the login name assigned to him/her.

9.3.3. User login should be disabled after three unsuccessful attempts, and reactivated upon request to the system administrator.

9.3.4. A password should not be displayed in the screen.

9.3.5. In the case where an incorrect login name or password is entered, no response which reveals any information should be given. For example, systems should not respond with “Incorrect Password for xxx login name". This message will reveal that such a valid user name exists leaving the attacker having only to crack the password.

9.3.6. The login system should display the last login date and time. This will alert the user to any use of the system by an unauthorized person.

9.3.7. The system should log-off automatically after inactivity of fifteen minutes or a period specified by the Information Security Officer

9.3.8. In the case where a job function is based on a general USER ID, the USER ID should be changed to unique one.

9.3.9. Time-based access should be implemented for the user login, where possible.

9.3.10. In the case of a “Critical Corporate Core System”, the end user should not be able to access the operating system command line.

9.3.11. For the issue of a new login name, a signed form indicating the relevant privileges is required, either in hardcopy or as part of the internal workflow software.

9.3.12. All login names and privileges should be reviewed at regular intervals in close co-operation with the Human Resources functions.

9.3.13. A login which is not successful should be logged and the logs should be reviewed at regular intervals.

9.3.14. In the case of an employee leaving ITA, the Department Manager will be responsible for making sure that all the employee's system IDs are revoked prior to final settlement.

9.3.15. A login ID not used for 90 days will be disabled and later deleted with the permission of the employee's Department Manager.

9.4. Enforcement

In the case of a violation of the security policy, disciplinary action would be taken, up to and including employment termination.

9.5. Responsibility

All employees, Departmental Managers and the Information Security Officer.

10. Password Protection Policy

10.1. Purpose

This document specifies ITA policy related to password protection, change and maintenance.

10.2. Scope

The scope of the policy includes all employees, irrespective of their position.

10.3. Policy

10.3.1. All default passwords should be changed by the user prior to use of the system.

10.3.2. A password should not be less than 8 characters made up of a mixture of alphabetic and numeric characters, incorporating upper and lowercase letters.

10.3.3. A password should be changed every 30 days or whenever compromised.

10.3.4. No common name or personal information should be used as a password e.g. dates of birth, spouse's name, pet name or phone number.

10.3.5. A password should be different from the last 12 passwords.

10.3.6. A password should always be kept secret and should never be disclosed to co- workers and colleagues.

10.3.7. No person should leave his/her PC or terminal without logging off or password protecting the screen.

10.3.8. A password should be stored in encrypted format and should never be in text format.

10.3.9. The System Administrator or Security Administrator will give the password in a sealed envelope to the manager or as specified by Information Security Officer.

10.3.10. In case of emergency and unavailability of the System Administrator the password would be obtained from the person nominated by Information Security Officer.

10.4. Enforcement

In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination.

10.5. Responsibility

All employees, Departmental Managers and the Information Security Officer.

Network Policies

11. Router and Firewall Security Policy

11.1. Purpose

Routers and Firewalls are the most vulnerable components of perimeter security. This policy specifies the minimum security protection requirement for the perimeter routers and firewalls.

11.2. Scope

The scope covers the firewall and routers at the perimeter network. The policy is also applicable to devices such as proxy servers and ADSL routers.

11.3. Policy

11.3.1. Routers and firewalls should be placed in a physically secure area.

11.3.2. Local User Accounts should not be configured on the router. The firewall management terminal should be separate from the main box.

11.3.3. The password for routers should be encrypted using the "Enable Encryption" option.

11.3.4. Any service not explicitly allowed on firewall should be denied.

11.3.5. The Firewall computer should be a dedicated machine. It should not be used to run proxy, web or any other services.

11.3.6. Routers and firewalls should disallow all invalid IP addresses coming from the Internet i.e. 10.0.0.1 to 10.255.255.254 and 172.16.0.1 to 172.16.255.254, 192.168.0.1 to 192.168.255.254

11.3.7. Routers and firewalls should not allow IP broadcasts.

11.3.8. IP-directed broadcasts should not be allowed on the firewalls and routers.

11.3.9. Source routing should be disabled on the routers.

11.3.10. SNMP should not be enabled on either the firewalls or the routers. In cases where SNMP is needed for system management , a standardized SNMP community string should be used.

11.3.11. The firewall should be configured to stop SYN attack.

11.3.12. Firewall should stop IP spoofing, fragmented packets and tear-drop.

11.3.13. The relevant Department Manager should approve the list of Access rules prior to deployment on routers.

11.3.14. Backup of the configuration files of the firewall and routers should be stored at a safe place.

11.3.15. The Audit log of the firewall should be regularly checked.

11.3.16. The firewall must hide all internal network addresses from the outside world.
11.3.17. A Firewall should filter the entire ActiveX and Java program.
11.3.18. Egress, i.e. the outgoing traffic should also be checked by the firewall.
11.3.19. Provided performance is not an issue, user level checking should be done at the firewall level, rather than at IP address level.
11.3.20. The Login Banner on the router should not display any welcome message. A warning message should rather appear:
"Warning: This is a Private Network. Any UNAUTHORIZED ACCESS TO THE SYSTEM IS STRICTLY PROHIBITED. If you are not authorized logoff now. All activities are logged. Any violator will be prosecuted."

11.4. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

11.5. Responsibility

Network administrator, Firewall administrator, Information Security Officer.

12. Dial-up Connection Security Policy

12.1. Purpose

This document specifies ITA policy related to Dialup lines for computers and fax machines.

12.2. Scope

The scope of the policy includes all lines for the purpose of computer and fax connections.

12.3. Policy

12.3.1. No external modem should be connected to any computer.
12.3.2. The internal modems of desktops and laptops should not be used while connected to the corporate network.
12.3.3. If there is any business need to use the modem, prior permission is required from the Information Security Officer.
12.3.4. Fax machines should be used for business purposes only.
12.3.5. No analog phone line will be extended to an employee except for managers.
12.3.6. No faxes should be sent directly from a computer except for corporate fax server, where available.
12.3.7. Anything downloaded should be scanned for viruses prior to use.

12.4. Enforcement

In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination

12.5. Responsibility

All employees, Departmental Managers and the Information Security Officer.

13. DMZ Policy

13.1. Purpose

Demilitarized Zone (DMZ) is one of the most important components of the corporate network. This policy defines the requirement for all equipment which is operated within ITA's DMZ, whether owned, leased, borrowed or brought by vendors for testing.

13.2. Scope

All DMZ equipment owned by ITA or outsourced.

13.3. Policy

13.3.1. Servers accessible from the Internet should be placed on DMZ.

13.3.2. There should be a defined owner for each DMZ equipment.

13.3.3. All equipment should be hardened to the maximum possible extent. There should be a System Hardening Checklist developed by the System Administrator for each DMZ component.

13.3.4. All required patches and fixes should be applied to all components of the DMZ and should be cross checked.

13.3.5. Only approved hardware, software and operating systems should be deployed in the DMZ.

13.3.6. All insecure services and protocols which are not needed, should be disabled.

13.3.7. If remote administration is required, a secured channel such as SSH or IPSEC should be used.

13.3.8. All security-related events should be logged.
Complete documentation of the system should be maintained with major emphasis on the following:

- Configuration Management
- Change Management

13.3.9. In the case where a DNS is deployed, special care should be taken to protect the DNS server and to protect against DNS poisoning.

13.3.10. Proper auditing should be done at regular intervals; all logs of critical systems such as the Firewall should be checked on a regular basis.

13.3.11. Any new service should be approved by the Information Security Manager prior to being moved to the DMZ production environment.

13.3.12. All equipment belonging to outsourced companies, vendors or service providers must meet the corporate security criteria.

13.4. Enforcement

Any employees who violate the security policy will be subject to disciplinary action, which may include employment termination.

Vendors, outsourced ITAs and others may be subject to financial penalties including contract termination.

13.5. Responsibility

All employees, Departmental Managers and the Information Security Officer.

14. Virtual Private Network (VPN) Policy

14.1. Purpose

The purpose of the VPN policy is to provide guidelines for secure remote access to the local networks.

14.2. Scope

The VPN policy applies to connections to ITA and to third parties including consultant, vendors and contractors.

14.3. Policy

14.3.1. As VPN is an extension of the corporate network, all of the security rules apply to the remote client as if they were within ITA.
14.3.2. All critical connections to the outside should use the safe channel. It is highly recommended to use IPSEC for VPN, where available.
14.3.3. It is highly recommended that an one time password be used.
14.3.4. "Tunnel Mode" is preferred whenever the VPN is used. If performance is an issue, "Transport Mode" may be used with the permission of the Information Security Officer.
14.3.5. All files transferred through VPNs should be subject to antiviral scanning.
14.3.6. The VPN timeout period is 30 minutes of inactivity.

14.4. Enforcement

Any Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

14.5. Responsibility

Network administrator, VPN user and the Information Security Officer.

15. Wireless Communication Policy

15.1. Purpose

The Purpose of the policy is to provide guidelines for network connections via wireless communication.

15.2. Scope

The policy covers all wireless devices such as mobile phones, PDA and laptop computers and others, which are connected to ITA corporate network.

15.3. Policy

15.3.1. The Information Security Officer should approve all wireless devices connected to the corporate network.

15.3.2. A Strong Authentication server should be used to grant permission to the wireless devices.

15.3.3. All wireless devices should use encryption while communicating.

15.3.4. Prior to the granting of a connection to the network devices, it would be preferable that the authentication server verify the hardware level address check (e.g. the MAC address) or in case of mobile phone the serial number.

15.4. Enforcement

Any Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

15.5. Responsibility

Network Administrator, mobile equipment user and the Information Security Officer.

16. Remote Access Policy

16.1. Purpose

This policy describes acceptable ways of connecting to the ITA corporate network.

16.2. Scope

The scope of the policy covers all connections which are dialed in (rather than dialed-up) by employees and third parties, including consultants, vendors and contractors.

16.3. Policy

16.3.1. Remote Access should be used for the business purpose only.
16.3.2. A remote connection extends the corporate network, so all corporate policies apply to the remote connection.
16.3.3. For a Dial-in remote connection, the Call Back feature should be implemented. The Call Back feature should authenticate the call back number, from the authorized list of the database prior to dialing.
16.3.4. The remote connection should be secured by a strong authentication mechanism as specified by the Information Security Officer.
16.3.5. In the case where ISDN is used, the CHAP protocol should be used for authentication.
16.3.6. Preferably, dial-in connections should use the firewall.
16.3.7. In the case where ITA uses Frame Relay, the proper authentication for DLCI should be performed.
16.3.8. An anti-virus check should be performed on all files downloaded through remote connections.
16.3.9. All remote connections should be logged and monitored.
16.3.10. In case, Intrusion Detection System is deployed it should generate alert to the system administrator if attack is detected.

16.4. Enforcement

A Policy Violation will be the subject to disciplinary action, which may go so far as employment termination.

16.5. Responsibility

Network Administrator, remote connection user and the Information Security Officer

Application Development Policies

17. General Application Development and Deployment Policy

17.1. Purpose

This policy specifies the requirements for application development both in-house and outsourced by ITA.

17.2. Scope

This policy is applicable to all core business software and other software. However, it excludes the operating systems.

17.3. Policy

17.3.1. Formal security specifications are required for all systems developed in-house or outsourced.
17.3.2. No test account should be present on the production machine.
17.3.3. The production and development/test environments should be separate.
17.3.4. Any error in a system should be reported and must be traced to the programmer who developed the program.
17.3.5. Prior to the system being moved to production, proper documentation should be done.
17.3.6. No trial version, beta version or free software may be used in the production environment unless approved by management.
17.3.7. Proprietary business logic should reside on the central core machine rather than on the desktop systems.
17.3.8. Mission critical software should have the escrow arrangement, and the software should be tested and validated by a third party and must be demonstrated to perform as specified.
17.3.9. All computer programs, routines, applets and documentation should display the copyright statement.
17.3.10. After authentication, the username and password should not be recorded on the server.
17.3.11. All access should be on a “Need to Know” basis.
17.3.12. The application file storing the information should be password protected.
17.3.13. ITA should either own all of the core application Source Codes or there should be escrow agreements with the vendors who have provided the applications.

17.3.14. Prior to moving program to the production environment, there should be exhaustive testing of the application.
17.3.15. No application should be moved to the production environment without the proper signing of a UAT (User Acceptance Test).
17.3.16. The developer should not have any account on the production machine; prior to moving to the production environment all such accounts should be removed.
17.3.17. Databases should follow the password policy.
17.3.18. An update to the database should be carried out on a well-defined, secure channel
17.3.19. In the case where a Data Warehouse application is used, access should be restricted to top and middle management.

17.4. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

17.5. Responsibility

IT Manager, Systems Analyst, Programmer and the Information Security Officer

18. Web Application Development Policy

18.1. Purpose

This policy specifies the requirements for web application development in-house or out-sourced by ITA.

18.2. Scope

This policy is applicable to all web applications currently deployed, developed or would be developed in future.

18.3. Policy

18.3.1. A proper User ID and Password should be created for the Web Application User. Any Web Pages that communicate password and user name data should use the SSL protocol.
18.3.2. The Web Application password should not be displayed on the screen. The "Copy and Paste" feature on the password field should be disabled.
18.3.3. The Password should preferably be stored in a one way hash.
18.3.4. For Data that is of confidential nature, a secure channel should be used.
18.3.5. The 'Press Back' button should clear the fields containing sensitive data.
18.3.6. An SSL connection should have an expiry time.
18.3.7. The Application should be programmed in such a way that in case of an error, there should be a standard error page rather than a system-generated error (e.g. 404) returned to the user as this would reveal the internal network.
18.3.8. The Web Server should not provide banner information.
18.3.9. The Directory listing of the CGI-BIN should not be accessible from the client.
18.3.10. The Input string from the customer should be validated prior to processing, as it may be manipulated to contain some secret command.
18.3.11. There should be an incident response procedure if something goes wrong on the server or if there is any security breach.
18.3.12. A Penetration test should be performed on the application as specified by the Information Security Officer.

18.4. Enforcement

Any Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

18.5. Responsibilities

IT Manager, Systems Analyst, Web-Master, Web-Programmer and the Information Security Officer.

Physical Security Polices

19. General Physical Security Policy

19.1. Purpose

This policy specifies the requirements for physical security at ITA.

19.2. Scope

This policy is applicable to all physical areas of the office/s of ITA, including those available now and those which may be added in the future.

19.3. Policy

19.3.1. The Information Security Officer should define security zones within ITA. For example:

- Zone A: The reception area where anyone can walk in (Minimum Security).
- Zone B: Area accessible to employees and authorized visitors
- Zone C: Area to which only selected employees have access such as the Computer room and other business-critical areas.

19.3.2. The Information Security Officer should apply appropriate measures for each of the zones.

19.3.3. Office floor plans and diagrams of telephone, electrical, water and network cabling lines, as well as extinguisher locations should be documented and maintained.

19.3.4. A proper Access Control List with corresponding work times should be maintained.

19.3.5. The entrance of ITA should be properly guarded.

19.3.6. Proper fire prevention and detection mechanisms should be in place

19.3.7. A Telephone Directory for emergency phone numbers should be maintained and must be easily accessible.

19.3.8. A First Aid Box should be provided and must be easily accessible and regularly checked and replenished.

19.3.9. All areas of the office should be properly lighted

19.4. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

19.5. Responsibilities

Administration & HR Department/representative and Information Security Officer. In future, some of the tasks relating to physical security may be delegated to the Corporate Security Officer when that post is created. For the time being, the Information Security Office will handle these tasks.

20. Computer Room / Data Center Security Policy

20.1. Purpose

This policy discusses the requirements for safeguarding the computer systems and personnel operating in the computer room / data center.

20.2. Scope

This policy is applicable to all physical areas of the office/s of ITA, including those which are available now and those which may be added in the future.

20.3. Policy

20.3.1. Access to the computer room will be restricted to ITA authorized persons only.
20.3.2. No public visits or tours of the computer room are allowed.
20.3.3. Vendor and third party representatives, if they visit the room, should be escorted.
20.3.4. A time-in and time-out register should be maintained for the computer room.
20.3.5. A proper fire alarm and fire extinguisher system should be in place.
20.3.6. Humidity control should be implemented and monitored.
20.3.7. A proper temperature should be maintained and monitored.
20.3.8. A proper Emergency procedure for the Computer room should be developed and be easily accessible. Personnel should be trained so that the procedure is executed efficiently, when required. All procedures should be audited at regular intervals.
20.3.9. The Information Security Officer will co-ordinate the development of computer room standards.
20.3.10. The Information Security Officer will co-ordinate measures to ensure that a reliable power supply to the computer room is in place and that adequate safeguards are there to protect the equipment.
20.3.11. No drinking, eating or smoking is allowed in the computer room.
20.3.12. Use of a cellular phone is prohibited in the data center.

20.4. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

20.5. Responsibilities

Information Security Officer and IT Manager.

21. Magnetic Media Policy

21.1. Purpose

This policy discusses the requirements for the handling of Magnetic media.

21.2. Scope

This policy is applicable to all media, i.e. Hard Disk, Compact Disc, Floppy Disk, Laser Disk, Super Floppy, Magnetic Tape Reel, Magneto-Optical Disk, Zip Disk, Magnetic Tape Cartridge and Digital Audio Tape.

21.3. Policy

21.3.1. An inventory of all critical magnetic media should be maintained and kept in the secure magnetic media library.
21.3.2. All magnetic media should be properly labeled.
21.3.3. All magnetic media should be physically destroyed prior to discarding.
21.3.4. The shelf life of all media should be ascertained from the respective vendors and should be monitored.
21.3.5. All media should be scanned for viruses prior to use.

21.4. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

21.5. Responsibilities

Information Security Officer and IT Manager.

22. Server Security Policy

22.1. Purpose

This security policy discusses the issue of securing the internal servers of ITA. This is to make sure that there is no unauthorized access to corporate information.

22.2. Scope

This policy applies to all servers either owned or operated by ITA.

22.3. Policy

22.3.1. The Servers should be located in a physically secure place.
22.3.2. All configurations of the servers should be documented and approved by the IT Manager and Information Security Officer.
22.3.3. Each server should have documentation of configuration, operating system version, patches installed, backup and recovery procedure.
22.3.4. All Change Management Policies should be strictly implemented on the servers.
22.3.5. The Information Security Officer should approve all configurations of servers.
22.3.6. Services not required, such as the web server and others, should be disabled.
22.3.7. The Log of the server should be monitored on a regular basis, as specified by the Information Security Officer.
22.3.8. All security patches should be installed on the server after confirmation that they will not have any adverse effect on the running applications.
22.3.9. All guests and default accounts will be either disabled or their password changed.
22.3.10. If remote management of the server is required, a secure channel should be used for this purpose.
22.3.11. The privileged account like super user and root should only be used when required.
22.3.12. A regular Audit would be performed by the Information Security Officer.

22.4. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

22.5. Responsibilities

System Administrators, Information Security Officer and IT Manager.

Operations Management Policies

23. Configuration Management Policy

23.1. Purpose

This security policy deals with proper documentation for the configuration of critical systems.

23.2. Scope

This policy applies to all servers, network equipment and others, either owned or operated by ITA.

23.3. Policy

23.3.1. All system configurations, including hardware, software and core business software should be documented.
23.3.2. There should be a hard copy and a soft copy of the documentation.
23.3.3. The documentation should contain a configuration baseline. All changes from this baseline should be documented as per Change Management Policy.
23.3.4. Prior to roll out, any modification made to the default configuration should be documented in the configuration management documentation.
23.3.5. The Information Security Officer should approve all configuration documentation.
23.3.6. Configuration management and change management documentation should be used together, in case of recovery.

23.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

23.5. Responsibilities

System Administrators, Information Security Officer and IT Manager.

24. Change Management Policy

24.1. Purpose

This security policy sets out the proper change management documentation for the all critical systems.

24.2. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by ITA.

24.3. Policy

24.3.1. Standardized methods and procedures should be used for the efficient and prompt handling of the changes and revision control.

24.3.2. All changes should be documented and prior approval must be obtained for all changes made to critical production systems.

24.3.3. A "Change Request" should be presented to the relevant manager for approval. The Information Security Officer will co-ordinate the work-flow for change approval.

24.3.4. All requested changes should be evaluated and have their impact assessed before approval or disapproval.

24.3.5. All changes, once approved, should be scheduled in such a way as to ensure the availability of a time slot for a rollback, should something unexpected happen.

24.3.6. Documentation for a change request should be accompanied by detailed, step-by-step procedures to do the change. It should also include detailed roll back procedure, in case the change fails and desired result is not achieved.

24.3.7. Whenever there is a need to change the application software, system software, LAN or any hardware, the change should be appropriately authorized and approved.

24.3.8. Every change should be thoroughly tested and fully documented.

24.3.9. Changes should be made when there is minimum or no activity on the system. In case, where there is more than one change to be carried out at a given time, the changes should be queued on the basis of business and technical priority.

24.3.10. Changes should only be approved after adequate consideration of the associated impact and implications.

24.3.11. Changes, once accepted, should be entered into the Change Management log.
24.3.12. The Change should be fully tested and the result presented to the respective manager.
24.3.13. A Change Management Summary report should be presented to higher management on a weekly basis.

24.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

24.5. Responsibilities

System Administrators, Information Security Officer and IT Manager.

25. Printed Output and Distribution Policy

25.1. Purpose

This security policy sets out the requirements for printed output and its distribution.

25.2. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by ITA.

25.3. Policy

25.3.1. All computer-generated sensitive reports should have a classification level, based on the sensitivity of the report.
25.3.2. The owner of the application will decide the classification level.
25.3.3. In case where the report classification is not 'general', the first page should be the banner page and must indicate the "classification level" and “User Name” for whom the report has been printed.
25.3.4. The Information Security Officer will ensure that a procedure exists that ensures that the report goes only to the authorized individual.
25.3.5. The person who prints the report is responsible for ensuring the proper protection of the information it contains.
25.3.6. Should someone find a report that is classified and is not intended for him/her, s/he should inform the Information Security Officer.

25.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

25.5. Responsibilities

Report Printing User, Information Security Officer and IT Manager.

Business Continuity Policies

26. General Business Continuity Policy

26.1. Purpose

The purpose of this policy is to provide directions regarding business continuity.

26.2. Scope

This policy applies to all business critical systems as referred to in the Business Impact Analysis and Risk Assessment in the Corporate Security Policy.

26.3. Policy

26.3.1. The Information Security Officer will ensure that the availability of the business-critical system is ensured as per the Risk Assessment requirement of the Corporate Policy.

26.3.2. Depending on the Risk Assessment report (as per the Corporate Security Policy),

26.3.3. Senior Management will decide the scope of the recovery plan.

26.3.4. Crucial systems, as per the risk assessment, should have reliable recovery procedure in case of disaster.

26.3.5. The word “Disaster” needs to be defined and the respective risk evaluated by senior management. The Information Security Officer should coordinate this task.

26.3.6. All documentation related to business continuity should be regularly updated.

26.3.7. The Information Security Manager will ensure that there is an appropriate Contingency plan, and "Emergency Response Plan” are in place

26.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

26.5. Responsibilities

Business Department Heads, Information Security Officer and IT Manager.

27. Backup and Recovery Policy

27.1. Purpose

This security policy specifies the backup and recovery standards for ITA.

27.2. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by ITA.

27.3. Policy

27.3.1. Backup of all critical devices, including the server, communication equipment and mission-critical hardware and software, should be undertaken.

27.3.2. Frequency of the backup will be decided according to the nature of the application being used.

27.3.3. The preferred backup method is "Full Backup" followed by a "Differential backup".

27.3.4. Unless there is justification, the “Incremental Backup” method should be avoided because in the case of a data recovery, one backup failure may make the entire backup process fail.

27.3.5. When storing historical data, the shelf life of the media should be considered.

27.3.6. The timing of "Distributed Backups" should be planned to have the minimum impact on the corporate network.

27.3.7. The backup process should not violate the confidentiality of the system

27.3.8. No public computers should be used for backing up sensitive data.

27.3.9. All archive data must be tested on a regular basis.

27.3.10. All backups should be verified to check the validity of the media. The “Read after Write” option should be chosen, where available.

27.3.11. In the case where distributed backup agents are not available, business-critical data should be put in a directory on the server to be backed up. Information Security officer will make the necessary arrangements.

27.3.12. The Information Security Officer, in consultation with the IT Manager, will make arrangement for Electronic Vaulting i.e. storing of the backup data at an off-site location.

27.3.13. Once the backup media is no longer usable, it should be physically destroyed or preferably burnt.

27.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

27.5. Responsibilities

All employees, Information Security Officer and IT Manager.

Personnel and Third Party Polices

28. Personnel Policy

28.1. Purpose

This security policy specifies guidelines and standards related to Human Resource (HR) with special reference to Information Security.

28.2. Scope

This policy applies to all permanent and contract employees.

28.3. Policy

28.3.1. Prior to hiring a prospective employee, HR must do a background check, contact references and validate the education testimonial.
28.3.2. Employees should sign the undertaking accepting responsibility for adherence to security policies.
28.3.3. HR will ensure that security responsibility is included in the job responsibilities of the employee.
28.3.4. The Terms and Conditions of employment shall mention the Information Security policy for each employee
28.3.5. HR will ensure that segregation of duties and job rotation is implemented, where possible.
28.3.6. When an employee leaves the employ of the company, HR will ensure that an exit interview is conducted.
28.3.7. HR will ensure that the person has all computer accounts removed prior to his/her final settlement.
28.3.8. In the case where employment is terminated without the consent of the employee, he/she should be escorted from the premises.

28.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

28.5. Responsibilities

HR, Information Security Officer and Department and IT Manager.

29. Third Party Policy

29.1. Purpose

This security policy specifies the standard and guidelines for the third party and outsourcing.

29.2. Scope

This policy applies to parties whether they are vendors, contractors, consultant or outsourced professionals.

29.3. Policy

29.3.1. The Risks associated with third party involvement and outsourcing should be identified and appropriate measures taken to address them.
29.3.2. A Non-disclosure agreement is essential before sensitive information is shared with a third party.
29.3.3. The role and responsibilities of the third party should be clearly defined.
29.3.4. Third party access to the corporate computer system will be given only after the signing of a formal contract which should contain all security requirements by which the third party is to abide.
29.3.5. All Third party and external users, if defined on the system, should have a mandatory expiry date.
29.3.6. Third party or outsourced tasks which require dial-in and dial-up privileges, should be restricted and monitored.

29.4. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination. For third party it may lead to contract termination.

29.5. Responsibilities

Department Heads, HR, Information Security Officer and IT Manager.