Indian Rare Earths Ltd

IT Security Policy

IREL INFORMATION SECURITY POLICY (Based on ISO 27001)

1. SCOPE

The scope of the information security policy covers information assets of Indian Rare Earths Ltd (IREL) in electronic form, which include computer equipments, operating systems, software, storage media, information in electronic form and network related systems and services

2. TERMS AND DEFINITIONS

A) LAN : Local Area Network.
B) WAN : Wide Area Network.
C) MPLS : Multi Protocol Label Switching
D) CERT-In : Indian Computer Emergency Response Team
E) CISAG : Computer & Information Security Advisory Group
F) NTRO : National Technical Research Organisation
G) ISBRF : Information Security Breach Reporting Form
H) STQC : Standardisation Testing and Quality Certification
I) ANUNET: The Wide Area Network interconnecting various DAE units
J) ANUNET secure channel: Dedicated ANUNET segment for special applications with no connection to any public network.
K) ANUNET normal channel: ANUNET segment, which is, connected unit's network where condition of "no connection to any public network" is not imposed.
L) Secure Internet: Internet segment behind the security systems such as Firewalls.
M) Intranet: Internal network of a IREL.
N) DMZ: Demilitarized zone
O) Classified Applications include creating, Storing, Transmitting classified data and information.
P) Confidentiality : Information is observed by or disclosed to only those who have a right to know.
Q) Integrity : Information is protected against unauthorized modification.

3. SECURITY POLICY

Information Security Policies are the cornerstone of Information Security effectiveness. The objective of this section is to provide direction and support to ISMS (Information Security Management System) from the management of IREL

3.1 Information Security Policy

The information security policy is intended to define what is expected from an organization with respect to security of information systems. The overall objective is to control or guide human behavior in an attempt to reduce the risk to information assets by accidental or deliberate action.

3.1.1 Information Security Policy Document

a) A well documented strategy to protect the information assets of IREL from damaging actions by individuals, either knowingly or unknowingly, with minimum required restrictions on the acceptable usage of the assets.

b) Information assets of Indian Rare Earths Ltd (IREL) located at---

Sr No	Locations	Deptts.
1	Corporate Office (Prabhadevi)	Marketing and Sales (including Dispatch and Transportation) Human Resources Management (Legal and Industrial Relations) Finance and Accounts Technical (Including Project Planning and Purchase) Vigilance
2	Worli	IT and Hindi Deptt
3	MK	Mineral Processing and Production. Finance and Accounts Human Resources Management (Legal and Industrial Relations) Sales Quality Control and Assurance Project Execution Purchase Maintenance (including Mechanical, Electrical and Civil) Vigilance (including Internal Audit) Safety and Environment Stores
4	OSCOM	Mineral Processing and Production. Finance and Accounts Human Resources Management (Legal and Industrial Relations) Sales Quality Control and Assurance Project Execution Purchase Maintenance (including Mechanical, Electrical and Civil) Vigilance (including Internal Audit) Safety and Environment Stores
5	CHAVARA	Mineral Processing and Production. Finance and Accounts Human Resources Management (Legal and Industrial Relations) Sales

		Quality Control and Assurance Project Execution Purchase Maintenance (including Mechanical, Electrical and Civil) Vigilance (including Internal Audit) Safety and Environment Stores
6	RED (Udyogmandal)	Mineral (Chemicals) Processing and Production. Finance and Accounts Human Resources Management (Legal and Industrial Relations) Sales Quality Control and Assurance Project Execution Purchase Maintenance (including Mechanical, Electrical and Civil) Vigilance (including Internal Audit) Safety and Environment Stores
7	IRERC Kollam	
8	BSNL Data Cente	IREL IT systems co-located at BSNL Data centre.

3.1.2 REVIEW AND EVALUATION

1. IREL shall document all important policies and procedures, rules designs , manuals and training materials including the following

    - IT policy
    - IT strategy
    - IT procurement policy
    - System design
    - Network design
    - System operation and maintenance procedures
    - Network operation and maintenance procedure
    - Acceptance and testing procedures
    - Inspection and auditing procedures
    - DR management and BCP
    - Risk assessment and insurance policy
    - Training manuals
    - Roles and responsibilities
    - Change management and development process
    - Back up process
    - Inventory
    - User account creation, deletion forms/access permission forms
    - Vulnerability assessment procedures

- Information classification
- NDAs and SLAs
- Incident management and escalation procedures
- HR
- Outsourcing and contracted staff policy
- IT plan (Refer Annexure for details.)

2. The soft copies in circulation must be in PDF format.
3. All documents must mention
    - Names of the authors, reviewers and approving authority
    - Document purpose and audience
    - Date of creation and modification
    - Control Matrix
        1. to approve the document for adequacy
        2. to review and update the documents as necessary
        3. to ensure the relevant versions of applicable documents are available at points of use and are recorded in the following format.

Sr. No.	Information Security Policy	Effective Date	Approval Status	Review Schedule	Revision Proposed By	Proposed Revision	Changes Done	New Revision Number	Revision
1		8-4-15	8-4-15						

- Content
- Document title and IREL logo on all pages
- Document classification, page no of total pages

4. ORGANIZATIONAL SECURITY

4.1.1 *(Review and approval Information Security Policy and over all responsibilities).*

Chief Information Security Officer (CISO) is nominated at IREL. The CISO shall be responsible to :-

- Secure servers by hardening.
- Ensure that antivirus solution is installed, updated and available on all the systems.
- Implement guidelines issued by CISAG,CERT-In, NTRO etc.
- In the event of a Cyber Security Emergency or incident, IREL will take assistance from BARC IT team CISOs of BARC shall provide additional contact/resource persons. BARC shall have at least one resource person visit the unit under it once a year, study the setup and recommend steps to be taken to tighten its IT security and offer advice on how to prepare ISMS documents, how to monitor networks, as well as prepare for IT security audits.

- Get 3rd party audit done on servers and devices connected to Internet through CERT-In approved auditors like STQC, at least once in a year and disconnect systems that are found vulnerable till problem is rectified.

  (Every auditing firm and its auditors (personnel) engage shall sign Non-Disclosure Agreements (NDAs) before being allowed to commence the cyber security audit work. To the extent feasible, it may be ensured that any data collected during the auditing work and report prepared thereof is not allowed to be taken out of the IREL premises by such auditors / firms.

  NOC from MHA shall be obtained before engaging non-Indian firm for auditing requirement.)

- Shall lock / disconnect systems that are found to cause problems on the network or are not following the IREL's security guidelines.
- Audit internal networks and servers periodically (at least once in a quarter) and send the quarterly report to CISAG, as per the format attached at Annexure -1.

4.1.2 Information Security Coordination.

The Information Security Committee (ISC) constituted by the Management will coordinate with various departments / units across organization.

An Information Security Committee (ISC) comprising of following members to be constituted at units.

1. Chief Information Security Officer (CISO)
2. IT Coordinator OSCOM
3. IT Coordinator MK
4 IT Coordinator Chavra and IRERC Kollam
5 IT Coordinator RED

to ensure all products, procedures, and personnel involved in this process implement and maintain the security objectives defined in the policy**.** In case of any emergencies ISC shall extend help via telephone, e-mail to counter the problem. The ISC will coordinate with various departments / units across organization, conduct internal audits, operational reviews and will submit a report to Management from time to time.

4.1.3 Allocation of information security responsibilities.

4.1.3.1 Computer User responsibilities

1. Screen savers should activate itself within 15 min of inactivity. It should be password protected. Third party or freely available screensavers must not be installed.

2. Users must not share their passwords with anyone. Users not write down Their passwords in clear text.
3. Passwords must be hard coded in software, shell script, batch jobs or data processing jobs.
4. Passwords must not be easily associated with the user (e.g Date of birth, employee number, address, numerical equivalent of names, pet names) Passwords must not contain words from a dictionary, movie, geographical Location.
5. Users should be beware of shoulder surfing and social engineering.
6. Users should avoid tailgating while entering or exiting a secure area.

4.1.3.2 Departmental

1. A catalogue of all IT assets may be maintained by all stake holders (Dept In charges), who are in-charge of the system.
2. This catalogue may be updated and reviewed annually in the month of March.
3. The catalogue must include the following(non-exhaustive) list:

    - Item Type (H/W, S/W, databases, web contents, training material etc.)
    - Date of Procurement
    - Cost
    - Owner
    - Purpose

4. IT Dept will assist in creation and maintenance of this catalogue.
5. Hard as well as soft copies of this catalogue will be maintained in Read only mode.
6. Assets may be procured , Commissioned , moved, renowned, Scrapped, sold discarded and archived
7. IT users may maintain their own asset catalogue and include the following in the list (non- exhaustive).
    - Service Provider contacts
    - AMC start and expiry dates
    - Environment and power supply information
    - Criticality and use
8. Government guidelines shall be followed, to decide upon and execute the scrapping process. The same process may be communicated to planning unit, at least annually or as and when required.

4.1.3.3 Centralised IT services

Mass e-mailing only through centralized IT services.

4.1.4 Authorization process for information processing facilities

The allotment of Computer Hardware / Software / Services will be as per policy and need basis. Approval from respective Head of Department is required for getting new facilities or connections.

Standard configuration will be provided to the user as mentioned in this policy. Any deviation should be approved by HOD. The user is responsible for Damage / Theft of the assets issue to him.

4.1.5 Specialist information security advice

*CISAG DAE, CERT-In, **NTRO***

4.1.6 Independent review of information security.

There will be an IT security audits by CISAG team.

4.2 Security of third – party access

When there is a proper business reason for a third party to be given access to IREL system or security domain, a risk assessment shall be carried out to determine security implications and control requirements. The control shall then be agreed with the third party and incorporated into a contract with any relevant penalties for breach clearly defined.

4.2.1 Identification of risks from third-party access.

IREL to identify and assess the risks associated with allowing third parties to access its information processing facilities and to implement appropriate controls.

4.2.2 Security requirements in third-party contracts.

IREL to incorporate its arrangement involving third party access into formal contracts that contain all the necessary requirements.

4.3 Outsourcing

4.3.1 Security requirements in outsourcing contracts

a) The Internet / Telecom service provider, Data Centre service provider , Web hosting provider shall be either central Govt. owned or PSU companies.
b) The Data centre of the service provider should be ISO 27001 and Tier 3 certified.
c) In case of hosting of IREL website on the cloud services offered by either central Govt or PSU companies, the website should be audited by CERT-in empanelled auditors based on OWASP guidelines and only after the removal of all vulnerabilities , the website should be

hosted online on the web server. At present IREL website is hosted on NIC web server http://www.irel.gov.in after going through security audits.

d) Source code to be obtained for any specific software developed by third party.

e) E-mail services shall be subscribed from National Informatics Centre, Govt of India. under the irel.gov.in domain.

f) AMC work for equipments will be carried out in presence of the concerned official. There must be Non-disclosure clause in Purchase Order, MoUs, Work orders etc

g) The outsider maintenance engineer should not be allowed to install his own keyboards and other accessories as an interim measures till repaired part is returned, as his accessories may have data capturing tools like key logger. When his accessory is taken back, it may have valuable data captured from the computer**.**

5. ASSET CLASSIFICATION AND CONTROL

5.1 Accountability of assets

There should be accountability of Assets at each location.

a) Information assets :To maintain appropriate protection of information assets to ensure right people given right access at the right time to access Information Systems and other organizational assets using :-

- Authentication : Verifying a user's (or a system's) identity
- Access Control : Permitting access only to authorized resources
- Directory Management: Storing user identity information and related configuration, rule, and policy information in a centralized repository.
- User management – creating, maintaining, changing and deleting the digital identities of users.

b) Software asset: The Original Software with Licenses should be kept centrally at One Location, may be with the Head of Unit.

c) Physical assets :

List of Software installed at each location should be kept with either Head of the unit or HRM dept.

The list of software installed at each location of IREL is attached. Annexure – 2.

d) Servers

5.2 Information Classification.

5.2.1 <u>Classification guidelines</u>

1. In order to protect and efficiently distribute the information assets, information be classified under the following categories.
    - Secret
    - Confidential
    - For internal use only
    - Public

2. Information owners can decide the classification categories on the use and criticality on the use and also general organization rules, except following classification guidelines are to be strictly followed :
    - All work flow , emails , files, intranet content , office PC contents, documents and training material may be classified as either confidential or for internal use only.
    - Default classification of all information will be "for internal use only".

3. No information can be downgraded to lower classification levels or declassified without the formal approval Head of the unit.
4. All media must be labeled according to classification type. All printed (or soft) documents must mention the classification level on each page of the document.
5. The secret and confidential data may be encrypted while using a public network or while storing on movable media.
   The hard copies may be sealed during transfer or kept in a lock.
6. The information content and its classification may be periodically reviewed and reported.
7. Privacy policy may be formulated for customer data
8. NDAs (Non Disclosure Agreement) and undertaking may be signed by all IT users and external vendors and contactors. Performa's for these may be formulated and widely circulated.
9. IREL shall take appropriate actions to protect IT IP rights.

5.2.2 Information Labeling and Handling

An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.

6. PERSONNEL SECURITY

6.1 Security in job definition and resourcing.

6.1.1 Including security in job responsibilities

Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

6.1.2 Personal screening and policy.

Verification of Character and antecedents certificate is required at the time of joining IREL, from the District authority for a person for the last 5 years, where he / she has resided for more than one year. In case of stay at abroad including Pakistan / Bangladesh particulars of all places where he had resided for more than one year after attaining the age of 21 years/

6.1.3 Confidentiality agreements.

A per " Atomic Energy Act 1962 " and the " Indian Official Secrets Act, 1923" Employees shall sign a confidentiality undertaking at the time of joining organization.

6.1.4 Terms and conditions of employment

As per Organizational policy

6.2 User Training.

6.2.1 Information Security education and training

1. IREL shall conduct on job training courses related to the field of Information Communication Technology (ICT) on a regular basis. IREL shall identify the key areas in IT and set up facilities for carrying out classrooms and hands on training courses.
2. Vendors shall assist in system O & M training where ever applicable.
3. IREL shall invite external experts when ever required
4. IREL shall arrange training courses in external institutions whenever required.
5. All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

6.3 Responding to security incidents and malfunctions.

6.3.1 Reporting security incidents.

When a System Administrator, finds that some abnormal behaviour in server performance or alarms through incident detection tools are noted the following steps shall be taken.

User should report such security incidents through appropriate management channels to CISO. CISO shall report to CISAG DAE and CERT-In.

After reporting the incident to CERT-In, advisory notes of CERT-In should be followed for recovering from incident.

Any information security breach shall be sent to NTRO through Chairman CISAG in the Information Security Breach Reporting Form (ISBRF) sent by NTRO vide letter dated 29/7/2013. (Copy of ISBRF enclosed).

6.3.2 Reporting security weaknesses

User should report any Computer security weakness through appropriate management channels to ISC. ISC will report to Management as well as DAE.

6.3.3 Reporting software malfunctions

User should report any Computer security weakness through appropriate management channels to ISC.

6.3.4 Learning from incidents

User should report any Computer security incidents through appropriate management channels to ISC and not tamper with the Logs of incidents / Computer / Networks. Logs of incidents are kept, action taken is documented.

6.3.5 Disciplinary Process

In case of any breach/ violation of the organization security procedures , there shall be departmental enquiry and employees shall be dealt with through a formal disciplinary process / as per the relevant service rules applicable to him.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

7.1 Secure Areas

1. All data centers, server rooms , operation rooms, switch rooms, storage facilities , utility rooms and network equipment rooms shall be declared as restricted areas. .
2. Only authorized staff shall be allowed access in these areas. Access shall be permitted after a written permission from the departmental head, not lower than rank of DGM. Temporary access may be allowed to third parties, contractors, sweepers, other IREL Staff and visitors after written permission from the department head. Such personnel must be accompanied at least one authorized person all the time.
3. An access register shall be maintained on the entrance of critical sites. It shall record the name, official address, purpose, signature, entry time and exit time of all persons entering the site.
4. A security guard shall be appointed on the entrance of critical sites, who's duties shall be documented and communication to him. the guard shall be responsible for:
    - Allowing entry for only authorized staff
    - Entry in the access register
    - Safe keeping the eyes
    - Checking the baggage on entry and after exit
    - Monitoring alarms
    - Making emergency calls
    - any other security tasks assigned by the department head

5. The sites shall be kept locked when not in use. All windows, doors, fire exits must be kept closed/ locked. All AC ducts, risers etc shall be blocked by suitable grills bars. All doors be automatically
6. All access shall be immediately revoked in case of an employee retirement, dismissal, suspension or long leaves/
7. Access records shall be backed up regularly and preserved for a suitable time.

7.1.1 Physical security perimeter.

All sites have different requirements depending on their criticality and levels of risks. Each security practitioner need to select appropriate techniques and equipments based on the result of a physical risk assessment and associated counter measure costs or benefit analysis.

7.1.2 Physical Entry Control

Following procedures shall be followed across the organization:-

Entry to visitors is allowed against the visitor pass and records of visitor pass is maintained in register with in / out time and purpose of the visitor. Visitors are normally not allowed during Lunch time.

Access to Server room is restricted.

7.1.3 Securing offices, rooms and facilities

All rooms / cabins of officers are lockable and shall be kept locked when the officer is not in office. Departments are provided with storage space with lock and key to store information. Security to ensure that everything is in order and any unusual thing noticed shall be reported immediately to authority.

7.1.4 Working in secure areas.

i. Photography / Recording not allowed.
ii. Mobile phones with cameras not allowed.
iii. Visitors not allowed to carry Floppy Disk/ Pen Drive etc within office premises.

7.1.5 Isolated delivery and loading areas

a) Inspection of incoming material for potential hazards
b) Registration of incoming materials
c) Designated supply area for incoming materials (for restricted access to material delivery staff)
    a. Pre-dispatch inspection by indenter and Security check up at security counter.

b. All material accounting is carried by Central Stores Unit (CSU).
c. Material delivery is at reception section of stores (CSU) situated outside the office premises.

7.2 Equipment Security.

1. All equipment shall be installed in secure rooms, with secure fire proof. Doors and windows should not be any means accessing or connecting to the equipment from outside the secure area. Fire exits may be provided at all sites.
2. Power supplies shall have a UPS or battery backup. The power cables shall be concealed and tamper proof. Redundant power supply shall be installed.
3. Suitable fire fighting arrangements shall be done. The fire extinguishers shall be re-filled regularly. At critical site automatic fire detection and suppression systems may be employed.
4. The equipment shall be installed on a raised floor or above. Water leakage detection systems may be employed at critical sites.
5. All communication cables must run through ducts and should be tamper proof. The cables must be disconnected when not in use. Redundant cables must be laid to ensure fast recovery of the connection.
6. Critical sites should have fire brick lining and should not contain any inflammable material , such as wooden furniture, curtains or carpets.
7. Suitable air conditioning and humidity controls shall be provided.
8. Eating, drinking and smoking shall be strictly prohibited inside the secure area.
9. The DR sites and data storage sites shall be planned at far removed places from the main site.
10. Spare , faulty , scrapped , discarded equipment or storage media must be stored in a separate room which must be locked all the times.
11. The equipment room and the racks must not have any kind of sign writing describing its name, purpose, network diagram, port numbers, IP addresses etc.

7.2.1 Equipment siting and protection.

a) Equipments to be kept at secure locations to avoid theft.
b) Fire alarm systems provided at all critical facilities.
c) Critical Equipments are kept on platform at higher levels to safeguard from Water.
d) Regular cleaning is carried out to avoid Dust.
e) Eating / drinking is not allowed in the rooms, where critical equipments are kept to avoid Cable cut by Rat.
f) Humidity and temperature meters are provided to monitor environment.

7.2.2 Power Supplies.

Equipment shall be protected from power failures and other electrical anomalies) using Multiple feeds / backup/ Generator.

a) Emergency power supplies are backup by D.G.
b) UPS provided to All Critical Equipments
c) Unarmed cables are laid in conduits / Capon -casing

7.2.3 Cabling security.

7.2.4 Equipment maintenance.

a) Only authorized personnel carry out maintenance / service

1. Maintenance units shall enter into SLA and AMC with approved vendors immediately after taking over.
2. The clauses in these agreements shall business interests of IREL. The clauses shall specify the QoS, availability, response time, spare policies, payment terms etc. IREL legal unit shall approve the agreements.
3. Units shall maintain SLA/ AMC register to keep track of Units work, payments made, performance quality and expiry of such agreements.
4. System administrators / Network administrators/Database administrators may approve the quarterly job performed by the vendors and keep a record of the same.
5. Maintenance or rectification of faults in the computer system should be carried out under proper and close supervision. In case of maintenance of Hardware / Software by an external agency, a responsible computer knowing officer should invariably be present throughout the maintenance. It should be ensured that no data file / program is copied and taken by the outsider maintenance engineer.
6. Maintenance records kept future reference

b) Data in the equipment to be deleted before sending out for repair

7.3 General Control.

1. Clear desk policy may be followed.
2. All confidential documents may be filed in locked cabinets .All discarded documents must be whiteboards must be wiped after use.
3. A PC or server must not be left logged in. Before leaving the machine, user must log off or lock the screen through keyboard or screen saver.
4. All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CDROM) containing Executive , Operational and Development data must be physically secured when not in use.
5. News about virus attacks must be broadcast to all IT staff as top priority mail. News about critical patches must be broadcast to all IT staff as top priority mail. Spam alerts must be broadcast to all IT staff as top priority mail. Same can be posted on the intranet.
6. Malicious emails must not be opened.

7. Any mails with doubtful or suspicious subjects must not be opened without confirmation. Spam messages must not be replied to. Care must be taken while clicking on URLs sent in emails. Dangerous attachments must be blocked.
8. Emails that are very important or have financial or security implications should be sent with a digital signature and should be encrypted.
9. Emails that are very important or have financial or security implications not received with a digital signature must not be trusted.
10. A clear warning must be displayed at log in prompt / screen at the time of user log in , stating that the system he/she is going to access is a property of IREL and unauthorized login is prohibited.
11. Equipment safety standards and ergonomics standards shall be documented and followed.

7.3.1 Clear desk and clear screen policy.

a) Computer media to be stored in a Cabinet with Lock and Key facility.
b) Fire resistant cabinet for sensitive documents / media
c) Idle timeout for computers and network equipments should be maximum 10 minutes.

7.3.2 Removal of property.

Authorization from the competent authority is required.

8. COMMUNICATIONS AND OPERATIONS MANAGEMENT

8.1 Operational procedures and responsibilities.

8.1.1 Documented operating procedures.

a) System start up / shutdown and maintenance procedures to be documented.
b) Backup and recovery procedure for each system to be prepared and documented.
c) Support contacts in the case of operational / technical difficulties.
d) Installation of software not directly related to business needs – prohibited
e) Use of Pirated and unauthorized software should be strictly prohibited. Only the Original Licensed Software with high Virus – Resistant / Virus- Proof rating should be procured from the authorized vendors.
f) Freeware – usage beyond validity period is treated as piracy
g) Support of non-standard software – at the discretion of IT

8.1.2 Operational change control.

a) The Information Security committee to take appropriate action in case of changes to equipments / software.
b) Assessment of potential impact of changes
c) Procedure for change of equipment / Equipment configuration to be defined.

8.1.3 Incident management procedures.

a) Procedures for handling security incidents such as Denial of Service (DOS) attacks, loss of service, breaches confidentiality.
b) Contingency plan for systems/ service recovery
c) Audit trails for analyzing the cause of incident
d) Reporting the action to the appropriate authority.

8.1.4 Segregation of duties.

8.1.5 Separation of development and operational facilities.

Development and operations to be handled separately therefore separate systems recommended for development / testing and operations.

8.1.6 External Facilities management.

All critical application should be developed indigenously and maintenance personnel access
Should be only in presence of designated departmental official. No permission to take out any faulty media.

8.2 System planning and acceptance.

8.2.1 Capacity Planning.

a) The capacity planning for computing servers should be based on user requirements & trends in usage.
b) Policy for procurement of hardware & software from approved / authorized supplier only.
c) IREL shall acquire IT system through following methods.

    a. Public Tenders
    b. Limited Tenders
    c. Quotations
    d. EOI
    e. Direct purchase orders

d) Standard tender process according to IREL procurements policy shall be followed for tendering.
e) Payment shall be made as per tender conditions and IREL procurement policy.

8.2.2 System acceptance.

- All IT shall be accepted and commissioned after extensive testing.

- Acceptance Testing (AT) procedures shall be approved by Head (IT) or Head of the unit ,who are the owners of the system
- The test shall be conducted by trained staff of the IT deptt. The results shall be reviewed by Head (IT) or the head of the units, who are the owners of the system. The systems shall be taken over by the users, if the test results are found satisfactory.
    - In case of failure of one of the many tests, the vendor shall be responsible for correcting the problems and the same shall be reoffered for AT.
    - In case the problems remains unresolved, the vendor must offer an alternative solution which must be reviewed by AT team and approved by unit Head concerned.
    - In case of there being no possible solution ,The AT team shall assess the criticality of the problem and may relax the test. This shall be approved by Head (IT) and IT users. If no relaxation is possible the entire system or parts of the system shall be rejected and new system shall be acquired.
    - The Testing shall be in line with IREL IT policy, IREL business objectives and IT best practices.
    - Benchmarking shall be done wherever applicable.
    - Load testing shall be done wherever applicable.
    - Failover tests ,disaster recovery tests and redundancy checks shall be done where ever applicable.
    - critical spare parts shall be ordered during the acquisition process.
    - Technical specification shall clearly define QoS parameters and the same shall be tested during AT.
    - Security probes shall be a part of AT procedure.
    - All systems shall be reviewed periodically and corrective measures shall be taken if found lacking in quality.

8.3 Protection against malicious software.

8.3.1 Controls against malicious software.

1. All Personal computers, laptops, vulnerable servers must have a valid and updated copy of anti virus installed.
2. The anti virus should be set to automatic updated for virus definitions, if directly connected to the Internet. For machine not connected to internet , manual updation should be done once a week. A log of such updations should be maintained in a register.
3. The anti virus should be scheduled to open scan automatically and regularly. The frequency of scans should depend on the criticality, disk size, CPU loads and updation frequency.
4. The anti virus should be configured to auto scan USB disks and CDs immediately after insertion of these. The anti virus should auto scan any files coming via network connections. The anti virus should auto scan emails and attachments. Default action of the anti virus should be quarantine, if an infected file is found.

5. All Personal Computers, Laptops, vulnerable servers must have a valid and updated copy of anti virus software installed. All policies mentioned for anti virus are applicable for anti spyware software also.
6. Trusted sites can be white listed. All email clients in use must block script execution and dangerous attachments by default.
7. The autorun setting of the CD or DVD drives must be disabled.
8. Users of pc must not be allowed to install unauthorized s/w in the PCs. The default access for users must be set to a limited account instead of the default admin account,
9. For critical systems, the machines installed in the network should have their com ports , removable drives and USB ports disabled.
10. An infected machine should be immediately removed from the network and in case of known viruses , should be cleaned , else should be restored from the backup.
11. A virus warning should be broadcast in the whole organization in case of major attacks.
12. Suspicious mails and attachments should not be opened.
13. Content filter must be installed on the email server to block spam. RBLs may be employed to block the spam.

8.4 Housekeeping.

8.4.1 Information back-up

All users must recognize that all forms of data storage are subject to data loss. For example, a disk crash may result in loss of server data. Users must therefore take steps to ensure there are copies of important data, called backups.

1. The user data system data ,system configurations, PC user data and system files emails and surveillance data must be periodically backed up in a reliable media.
2. The recommended frequency of backup is as follows:
   - **a)** Critical user data daily backup, incremental and full backup weekly.
   - **b)** Non critical user data- weekly full back up
   - **c)** System data weekly full back up
   - **d)** System and network configuration weekly full back
   - **e)** PC user data monthly back up
   - **f)** PC system data quarterly full back
   - **g)** Surveillance Data-daily incremental back up
   - **h)** Information stored on central servers is to be backed up regularly by the System Administrator.

3. Suitable media may be used for system back up. Removable media such as CD or DVD ,may be used for PC back up. Tape libraries may be installed for large systems . USB drives must not be used to back up data. Online storage facilities , free storage on the internet mail boxers,

must not be used for purpose of back up. Recycle and damage media must not be used.

4. Critical/ secret backed up data should be encrypted. The storage room should be a secured location . All policies mentioned for secured location such as Assess controls and physical security are application for storage rooms also. The media must be stored in suitable and lockable cabinet. Back up should be stored both onside and offside. The off side back up should be stored at a reasonable distant location.
5. Back up tapes and other media must be labelled according to a standard convention. which must be followed through out IREL. Recommended labelling should include the site name, machine name, drive name, data , time full/incremental
6. A back up register must be maintained on all sites .Registered entries must be signed by concerned employee on duty.
7. Restoration ,exercise must be done periodically to check the integrity of backed up data . The frequency of such checks shall depend on system critically and time factors.
8. The back up archives must be stored for a duration specified by data owners and /or organization roles , Govt policies and laws to prevent loss of archived data due to technology obselence , the data must be re – written using contemporary technology. The decision to transfer the data to new technology shall be taken by Head (IT**)**

8.4.2 Operator Logs.

a) The important field of log entry should be Date, time, name, system errors and corrective actions.
b) Frequency of checking the logs should be once in a week.

8.4.3 Fault Logging.

1. All systems must be configured to log system and application events, errors and access.
2. All relevant events must be logged on any computer or system handling critical information, including but not limited to, login failures, data modifications, use of privileged accounts, changes to access models or file permissions, modifications to installed software , or the operating system, changes to user permissions , or privileges etc.
3. Review frequency of the logs, corrective measures, fault analysis should be once in a week.

8.5 Network Management

8.5.1 Network controls

IREL Network shall be divided into reasonable sub-network and demilitarized zones. The purpose of such zones shall be to prevent un-needed access to all systems from anywhere in the IREL network. The zones may be configured so that all the users within a particular zone can communicate without any restrictions but shall require special access or must go through a demilitarized zone to communicate to other zones in the network.

A single convention for IP addressing must be followed through out IREL.A convention is suggested below:

- IP addresses shall be classified into LAN, WAN and public categories.
- Systems on LAN and WAN shall use private/closed IP addressing scheme.
- System on public network shall use public/open IP addressing scheme.
- System on Network shall use both private and public IP addressing scheme.
- For private IP addresses, various IP pools shall be formed and each application shall be allotted a specific IP pool.

IREL internal addressing schemes shall not be visible to external networks. Routers and firewalls must not accept any traffic coming from external networks if originating address belongs to the internal sub-network IP pool. Traffic from public networks shall be monitored through an Intrusion Detection/Prevention system.

8.6 Media Handling and security

8.6.1 Management of removable computer media

- The removable media should be stored in safe and secure environment
- Movement of media such as **pen drives, CDs, mobiles**, removable disks, notebook PCs etc should be mandatorily controlled. Only authorized Officials should be permitted to carry in/out such media/equipment. The equipment allowed to be carried in/out should be properly marked or sealed so that it can be identified by the unit's security personnel. Notebook PCs used by officials should have antivirus protection installed and updated. Removable media used for sensitive information should be fully accounted for, with maintenance of full log and strict authentication control

8.6.2 Disposal of media.

a) The system / sensitive documents may be disposed after formatting / destroying / shredding.
b) A Log should be maintained of disposal of sensitive information.
c) Sanitization of information systems has been set up.

Date	Number of Floppies / cardridges / CD brought forward	Number of floppies / cartridges tapes / CD received	Total number of floppies / cartridges tape / CD in stock	Serial Number of floppies / cartridges / tapes / CD	Date on which brought into use
1	2	3	4	5	6

Date on which floppies / cartridge tapes / CD was rendered unserviceable	Date and method of destruction	Balance	Remarks	Signature of officer incharge
7	8	9	10	11

8.6.3 Information handling procedures.

Handling and labeling of media

8.6.4 Security of system documentation.

Limited staff member should have access to Security System documentation.

8.7 Exchanges of Information and Software.

Only authorized staff member can exchange information from outside agency / between organizations to prevent loss, modification or misuse of information exchanged between organizations.

8.7.1 Information and software exchange agreements.

(Formal agreements for the exchange of information and software (whether electronic or manual) between organizations).

8.7.2 Security of media in transit

The package should be sealed while Media being transported to protect from unauthorized access, misuse or corruption of sensitive information during the transport

8.7.3 Electronic commerce security.

Implementation of e-tendering solutions based on CVC guidelines vide Circular No 18/04/2010 dated 26/4/2010.

8.7.4 Security of electronic mail (E-mail)

- E-mail ids shall be subscribed from National Informatics Centre (NIC), Govt of India under the irel.gov.in domain and will be allocated to all the officer of the company.
- He / She should not share his / her e-mail id with some one else.
- Any malfunctioning detected from the e-mail id shall be the responsibility of the owner of e-mail id.
- HR deptt shall be the custodian of the allocated e-mail ids allocated to the users.
- HRM deptt at HO, Mumbai to maintain a consolidated list of e-mail ids allocated to person in the following format and review every six months
-

Sr no	Employee computer code	Name of the employee	Designation	Unit	Dept / Section

- In the events of transfers / retirements of concerned employees, he / she to surrender his / her e-mail id with password to his / her successor before being relieved.
- Once the user is transferred / retired then HR deptt should initiate action to de- activate / reassign the e-mail id to a new user. Necessary coordination with NIC shall be done by IT deptt.
- Access rights and privileges of employees shall be granted depending on their roles. Limited rights must be given to all employees , except for system administrators .
- Unique account names and Email IDs shall be allotted to the employees. External email IDs shall not be allowed .

8.7.5 Security of electronic office systems.

a) Management access to PBX. from Local Console ports and Intranet (through firewall) only
b) Remote maintenance policy enabled only on request for specific period.
c) Configuration of lines using permitted modems not to activate connection to lines outside campus in any way e.g. through operators, call transfer or conferencing
d) There should be provision of calling line Id
e) WLAN Permitted only in certain isolated physical areas with approval of competent authority
f) Wireless voice communication is not permitted.
g) Mobility is not permitted on voice and data.
h) Encryption mandatory on WLAN

8.7.6 Security of Plant Control Network

Following measures are recommended for implementation in plant control networks at the earliest.

1. Plant control networks should be isolated from Intranet as well as Internet. Plant PC should not have wireless LAN, Bluetooth, modem or any other network enabled.
2. Use of removable media should be highly restricted and regulated. USB ports or removable media should be disabled in plant PCs wherever possible. If removable media needs to be used, then it should be first scanned with latest updated antivirus on some standalone PC to make sure that it is not infected.
3. Separate dedicated removable media to be used in plant control network. If required they may be numbered and issued for use. These removable medias should not be used in any other network.
4. PCs in plant control network shall be scanned with updated standalone antivirus at regular intervals.
5. Operating Systems shall be updated with latest patches.
6. In plant PCs, unnecessary processes shall be disabled and firewall enabled with appropriate rules.
7. Windows share shall be disabled.
8. Administrator account should not be used for normal operations of PC. Ordinary user account should be created and used for these purposes.
9. Use complex passwords for all login accounts.
10. PC BIOS should have password. Booting from removable media should be disabled.

8.7.7 Publicly available systems.

a) Public Servers should be kept on DMZ.
b) Only required application is allowed from outside. Remote login is not permitted even with from outside
c) All servers to run only the required services. All server hardening measures are taken
d) All O.S. patches downloaded and implemented on the servers regular basis
e) All Web contents are approved by Competent Authority

8.7.8 Other forms of information exchange.

Security for sensitive voice / fax communications through Voice encryption used on specific terminals.

9. ACCESS CONTROL

Access control standards are the rules, which IREL shall apply in order to control, access to information assets.

1. Data owners, systems owners shall grant access on a need to know basis. The user must fill an application form, justifying the access, which must be kept safely. The account must be duly approved by department head.
2. The default permissions on any files created must restrict access to general users of the system. System administrators must ensure the operating system restricts "world" access on any new filers created.
3. Access controls must explicitly state the rules and rights of the user. All user access must be driven by business requirements .The requirements for access must be communicated to all involved persons. Users must clearly be separated in reasonable user groups depending on their roles. Multiple accounts for a single user not be allowed.
4. Development of technical solutions must be sought to avoid the need for necessary or extensive privileged access.
5. User accounts that have not been accessed for 90 days will automatically be disabled.
6. All access to computer systems must be controlled by an authentication method involving a minimum of a Username/Password combination. The Username/Password combination must provide verification of the user's identity. Critical systems must use a smart card based or biometric based authentication.
7. Passwords must be strong; using combinations of alphanumeric characters at least 8 characters long. Passwords must expire 120 days automatically. Passwords recycling must not be allowed. Systems must be capable of sensing the password strengths intelligently. e. g number of sequences, repeated characters etc should not be allowed by the system. Operating systems and application must store the passwords in encrypted form or but using the hash method.
8. Simultaneous multiple sessions must not be allowed, Audit trails must be enabled for all account types. Accounts never be deleted and should be disabled instead. Passwords must get blocked automatically after three successive incorrect logins or failed login attempts. Blocked passwords may be re-enabled either after set duration automatically or by SA depending on the criticality of the system.
9. Sessions must expire after 30 mins(max) of user inactivity.
10. Configure access controls for all protected files, directories, devices, and every change or decision not to change each object's permission should be documented along with the rationale.
11. Restrict access of operating system source files, configuration files, and their directories to authorized administrators.
12. For UNIX systems, there should be no group/world-writable files unless specifically required by necessary application programs.
13. For NT systems, there should be no permissions set such that "the Everyone group has Modify permissions to files"
14. Assign minimum level of access permission to all kernel files
15. Establish all log files as "append only" if that option is available .
16. As a goal, preclude users from installing, removing, or editing scripts without

administrative review. Proper procedure for enabling and enforcing the same may be established and fully documented .

17. Pay attention to access control inheritance when defining categories of files and users. Ensure that operating system should be configured so as newly created files and directories inherit appropriate access controls, and that access controls propagate down the directory hierarchies as intended when one assigns them

9.1 Business requirement for access control

9.1.1 Access control Policy.

Access control policy is based on the information classification. Ref. Section 5.2.

Public: IREL WEBSITE.

Read-only access to public on the Web Site of Indian Rare Earths Limited.
Limited Write access on the web site for form filling, given with approval of competency.

Intra-DAE:
Intra-Unit: Employees within physical boundaries of Indian Rare Earths Limited with or without authentication depending upon the type of information. All the IT systems shall be installed behind UTM / Firewall at BSNL Data Centre and shall be accessible through MPLS VPN except e- CRM systems, e-recruitment systems etc which shall be installed on the Di-militarized Zone (DMZ) created through UTMs at the BSNL Data Centre.

Sensitive: Available on isolated, non-networked secure systems only. Access over ANUNET, with or without authentication depending upon the type of information.

9. Change Management

9.1 Development Cycles

1. IREL shall adopt system Development Life Cycle Model(SDLC Model),also known as Classic Life Cycle Model or linear Sequential Model or Waterfall Method. This consists of the following activities.

   - System Information Engineering and Modeling.
   - Software Requirements Analysis.
   - System analysis and Design.
   - Code Generation.
   - Testing
   - Maintenance.

2. All information system must meet anticipated capacity requirements. is the responsibility of the system's development and operational teams to determine hardware requirements and capacity and monitor system performance .This includes, but is not limited to:

   - Disk usage and size
   - Network traffic and load
   - Load balancing
   - Necessary memory requirement.
   - Necessary processing power.

3. Requirement analysis shall be carried out by a joint team of development unit, user and external parties. SRS shall be documented and signed off by competent authorities.
4. System designed shall be done by project leader and shall be documented and signed off by competent authorities. The design must follow IREL's IT policy and business objectives.
5. With respect to the type of application ,the right programming language must be chosen. IREL shall prefer and promote open source and open formats. IREL shall prefer indigenous code, whenever possible. IREL shall retain rights and ownership of all source code written by in-house development teams or written by outsource companies for IREL exclusively IREL shall prefer escrow arrangements for third party closed source code.
6. Testing shall include debugging ,trail runs ,beta and full UTA according to IREL IT Quality control policies. Release versions shall be launched after extensive beta testing and reviews /feedbacks.
7. Changes in design, updates, upgradations and optimization/ tuning ,.after handling over the system for maintenance to maintenance units ,if any shall be managed by original installers and vendors, whenever possible
8. A changes request from or document, mentioning the nature, reason and purpose of a change shall be compulsorily submitted to the installer or system administrator. Changes shall be well documented and signed off by competent authorities.
9. Minor or configuration changes can be carried out by the user (maintenance staff),after necessary written approvals. such changes must be logged.
10. Where ever applicable, changes shall be applied to production site first and after ensuring satisfactory performance, some shall be applied to DR system.
11. Where ever applicable source code shall be maintained in a Subversion.
12. Frequent changes should be avoided.
13. Whenever there are major changes to be done or there are too many changes requests, providing a new system should be preferred instead of making those changes.

9.2 Acquisition process.

1. IREL shall acquire IT system through following methods.

   -Global Tenders

   -limited Tenders

-Quotations
-EOI
-Direct purchase orders

2. Global and limited tenders shall follow two bid system(technical and financial)
3. Standard tender process according to IREL procurements policy shall be followed for tendering.
4. Quotations shall be called in case of low value procurement or emergency procurements only. This will require approval from competent authority.
5. Direct Pos should be issued in case of emergency or when the product to be acquired is proprietary/specialized/no similar products are available in market. This will require approval from competent authority.
6. Payments shall be made as per tender conditions and IREL procurement policy.

9.3 IT Quality Control

1. All IT shall be accepted and commissioned after extensive testing.
2. AT procedures shall be approved by Head (IT) or the Head of the unit ,who are the owners of the system.
3. The test shall be conducted by trained staff in the unit. The results shall be reviewed by Head IT or the GM of the units, who are the owners of the system. The systems shall be taken over by the users, if the test results are found satisfactory.
4. In case of failure of one of the many tests, the vendor shall be responsible for correcting the problems and the same shall be re-offered for AT In case the problems remains unresolved, the vendor must offer an alternative solution which must be reviewed by AT team and approved by GM concerned. In case of there being no possible solution ,The AT team shall assess the criticality of the problem and may relax the test. This shall be approved by GM(IT) and IT users .If no relaxation is possible the entire system or parts of the system shall be rejected and new system shall be acquired.
5. The Testing shall be in line with IREL IT policy, IREL business objectives and IT best practices.
6. Benchmarking shall be done wherever applicable.
7. Load testing shall be done wherever applicable.
8. Failover tests, disaster recovery tests and redundancy checks shall be done when ever applicable.
9. Critical spare parts shall be ordered during the acquisition process.
10. Technical specification shall clearly define QoS parameters and the same shall be tested during AT.
11. Security probes shall be a part of ATP.
12. All systems shall be reviewed periodically and corrective measures shall be taken if found lacking in quality.

IREL core team with the help of bidder’s technical team shall develop a test design document. Test design document will contain user acceptance testing (UAT) for each of the modules, functionalities and security features. IREL shall perform the testing of the application as under :-

- Module Testing

- **Functionalities**: individual transactions, programs, reports and standalone functions.
- **Security** : Content access and data access (The system should have proper security and maintenance facility which limits access to the system and its various functions to the users delegated with appropriate authority. It should provide log in, both by user and by terminal. The System should provide the date and time of all transaction with details of creation, read, change/ update, delete or print. Access should be restricted at different levels of data file, program, module, screen, record, field database table, row or column. Suitable firewall against unauthorized uses, interceptions, misuses by outside parties shall be provided.)
- **Usability** : Navigation, Captions

- **Integration Testing** :The integration testing will focus on end-to-end business scenario testing.
- **Systems Testing** Systems testing will focus on key system components. Carry out the performance and load test.
- **Cutover verification.**

This activity will be carried out in the production system in order to certify the system readiness to go live. This will involve key users representing the different functions.

9.4 Patch management

1. Patches shall be recommended by earlier system Administrator or vendors of the s/w. In all cases, the patches must be approved by OEM or application producers.
2. Where ever applicable patches should be first applied in a production site .After satisfactory performance of the system the same can be applied at DR site.
3. Critical patches should get high priority.
4. Systems that are not connected to Internet must have some arrangement of manual installation of patches.
5. Upgrades, Updates and patching must be logged by SA in a register.
6. Office PCs must be set to automatic updates, if connected to internet. Offline PCs must be updated manually at periodic intervals, except for critical patches, which must be installed immediately.
7. If the application of a patch or updates affects performance adversely, the same must be uninstalled or original files may be restored from backup. If DR is available, the sites should be switched over and vendor help may be called for.
8. Dependent processes/application owners must be informed before applying a major patch.
9. A full backup must be taken just before applying a patch.

9.5 Capacity planning

- Vendors responsible for AMC of a system shall be responsible for monitoring and review of performance of the system according to a suitable SLA.
- Such vendors shall advise about capacity planning to IT planning units.
- IREL shall appoint consultants for capacity planning of critical IT systems.

9.6 User access management.

1. Access rights and privileges of employees shall be granted depending on their roles. Limited rights must be given to all employees , except for system administrators.
2. Access to equipment not needed for an employee's job or role shall be denied. Access to network not needed for an employee's job or role shall be denied.
3. Access to s/w or applications or files or data not needed for an employee's job or role shall be denied .Access to computers/laptops not needed for an employee's job or role shall be denied. Access to internet/intranet can be denied depending on the location and criticality of system.
4. Security awareness training shall be conducted regularly for all IT staff.
5. Personnel Controls shall be reviewed regularly and shall be modified as and when necessary.

9.4.1 User Registration.

a) Network / information service access provided to user based request and approval from the respective head of divisions
b) User has to undertake conditions of access
c) Record is maintained for registration.
d) User is de-registered whenever he leaves the organization or not using the facility for a period of 3 months

9.4.2 Privilege management

Root account is super user and restricted privileged account is created for System Administration.

9.4.3 User Password management.

Initial password conveyed personally **Passwords** To decrease the chances of guessing password, user must select a hard-to-guess, or **strong** password. A strong password must:

- Be as long as possible
- Include mixed-case letters.
- Include digits and punctuation marks.
- Not be based on any personal information.
- Not be based on any dictionary word, in any language.

9.4.4 Review of user access rights.

Once in six months

9.5 User Responsibilities.

- Appropriate Software tools like Device Lock may be installed to disable USB Ports, Communication Ports, Floppy Drives and other removable drives. Such Ports / Drives may be enabled by the authorized user only when required. Soon after the requirement is met, the Ports / drives should be disabled. Record of such activity to be maintained.
- As a general rule, no computer utilized for classified application should be provided with Internal Combo Drives (CD / DVD Reader plus CD writer or CD / DVD writer). Only external combo drives / CD writer / DVD writer should be used on need basis , on specific authorization by the controlling officer in writing. Such drives should be kept in safe custody under lock and key, when not used.
- Access to the Servers should be restricted.
- The Network should have Firewall and Intrusion Detection System (IDS) to detect / prevent unauthorized access.
- Denial of access to unauthorized person Pen / Flash Drive etc.
- To share email accounts not permitted.
- Mass Mailing – only through IT

9.5.1 Password use.

- Servers should accept only secure passwords and the Life of password should be 3 months only.
- Every individual user should have separate user ID and Password. Two or more users should not share the same user and password.
- A password should have atleast 8 characters and be a combination of upper and lower case alphabets, numerals and special characters to make it complex.
- Screen Saver Password should be used.

9.5.2 Unattended user equipment.

a) Inactive session time out should be 10 minutes.
b) Password protected screen saver to be used for all the Desktops / Servers.

9.6 Network access Control

To prevent unauthorized access to information held in information systems following shall be ensured.

- To prevent intruders from hacking into systems via LAN / Internet connection UTM / Firewall shall be installed & configured. The following types of network traffic always shall be blocked:

1. Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
2. Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
3. Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks.
4. Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
5. Inbound traffic containing IP Source Routing information.
6. Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (local host).
7. Inbound or outbound network traffic containing a source or destination of 0.0.0.0.
8. Inbound or outbound traffic containing directed broadcast addresses

- The "intruder alert" facility, should be activated and all alerts should be acted upon.

- To detect unauthorised access of a system, Intrusion Detection System (IDS) shall be installed & configured

- Management access to networking equipments.

  Only from the console ports / from specified systems / using specific accounts

- Hardening of router and other equipments.
- Default passwords shall be changed and hardening done at the time of installation.

9.6.1 Policy on use of network services.

Access to network are approved by Competent Authority

9.6.2 Enforced path.

No Alternate routes from user PC to public data network (e.g. Internet)

9.6.3 User authentication for external connections.

a) No access allowed from outside to the servers except those in the respective DMZ. The authentication method is based on information classification.
b) No dial-in access permitted from outside
c) Dial-in access from internal only through ISDN.
d) Modems allowed only for specific use on approval.

9.6.4 Node authentication for remote computer.

a) User Id is required for sending mail
b) Authentication based on user Id / IP address / MAC address
c) Network Login should be based on user id.

9.6.5 Remote diagnostic port protection.

Dialup connectivity usually not provided for remote maintenance of equipments. Dialup connectivity provided for specific period on approval.

9.6.6 Segregation in networks.

9.6.7 Network connection control.

a) Type of firewalls used.

Stateful Identity based Inspection Firewall at Chavra unit

Make: Cyberoam CR50iNG UTM Box which also includes:

1. Gateway antivirus
2. Anti spam
3. IPS (Intrusion Prevention System)
4. Web/ Content/ Application filtering
5. On – application reporting
6. Bandwidth management
7. Routing & Load balancing

b) Traffic filtering policies of each firewalls (Explicitly permitted traffic)

<u>Secure Internet to Internet</u>: http, email.
<u>Internet to Secure Internet Segment</u>: Email
<u>Intranet to Secure Internet:</u> http, email, ftp.
<u>Secure Internet to Intranet</u>: Email, VPN Segments: Specific to VPN.
<u>Intranet to ANUNET Normal Channel</u>: http, email.
<u>ANUNET Normal Channel to Intranet</u>: Specific services through reverse proxy.

c) Traffic filtering policies of each firewalls (Explicitly blocked traffic)
d) Networks from which the access is permitted (indicate with or without authentication)
e) Networks from which the access is permitted to DMZs (indicate with or without authentication).
f) Services permitted on each of the above access
g) Authentication and authorization system used on each service
h) Usage of Virtual Private Networking (VPN).

9.6.8 Network routing control.

NAT implementation to hide internal address detail to external network
Hide internal from external

9.6.9 Security of network services.

Annexure attached.

9.6.10 Automatic terminal identification.

Terminal identification for connectivity to Servers and Firewall systems
Important server login is allowed from console or from a specified computer systems

9.6.11 Terminal log-on procedures.

a) All system banners are suppressed to external world.
b) Notice for unauthorised use given as per the rules of administration.
c) During logging, no help messages provided.
d) Un – successful log-on attempt should be maximum Five times.
e) There should be display of information about previous log-on, etc after successful log-on.

9.6.12 User identification and authentication.

a) Authentication procedure
b) Unique user Id, shared account not allowed.

9.6.13 Password management System.

a) Password management
b) Storage of password in server systems ---- Shadow File / SHA – 1.
c) Default system passwords are changed immediately on installation.

9.6.14 Use of system utilities.

a) User area and system area should be mounted on separate partition.
b) Limited utilities are provided to the user by restricted shell
c) Only required software are installed on critical servers

While installing the operating System (OS), only the Utilities / Components required by the user should be installed / enabled. Some of the utilities listed below, which are enabled by default with the bundled Software must be either disabled or configured on need basis.

a. Default Password
b. Sample Networking Programme
c. File Sharing Tools
d. Ports enabled by default.

9.6.15 Duress alarm to safeguard users.

(Duress alarms shall be provided for users who might be the target of coercion).

9.6.16 Terminal time-out

Five Min with clear screen

9.6.17 Limitation of connection time

Connectivity to Important servers are allowed in only working hours. Idle time lock out is implemented.

9.7 Application Access control

9.7.1 Disabling unwanted services and protocols

Only required network services should be installed in the server. There are many default services with the standard OS software. Depending upon the role of server one should load only required network services, like on a mail server DNS service is not required.

9.7.2 Information access restriction.

Controlling access rights of the users based on read/write/delete etc

9.7.3 Sensitive system isolation.

Sensitive systems are not connected to any networks

9.8 Monitoring system access and use.

Server shall be regularly audited and log files scanned for knowing any attacks and intrusions, preferably daily. For small organizations separate logging server with hardened OS should be implemented. Server to logging server communication should also take place over a secure i.e. encrypted channel. Additionally the logs must also be encrypted & access to it should be highly restricted. For very high threat exposure IDS should be installed.

Incident detection tools

Appropriate Tools for Incident Detection shall be installed on the server. The reports generated by the tools should be monitored regularly to check any change in the system, unauthorized access, DoS attacks etc. The alarms and event notifications should also be set appropriately.

Some of the tools are

Windows based servers	SamSpade, Retina, Fport, NBTScan
Unix based server	NMAP, SAINT, SARA, THC-Amap, THC-Hydra

These tools are very helpful in detecting server compromise and similar attacks.

9.8.1 Event logging.

Logging is a cornerstone of a sound security posture. Logging the correct data and then monitoring those logs is critical. Reviews should take place on a daily to weekly basis and when a suspicious activity has been noted or a threat warning has been issued. Automated Log File Analysis Tools can be used for analysis.

a) Syslogs shall be enabled on all servers. To capture User id with dates & time of Successful / rejected logins.

b) Ten Years Security Logs to be preserved on backup media.

9.8.2 Monitoring system use

a) Date & time of events
b) Use of super user a/c
c) System start & stop
d) Un authorized access attempts
e) Console alerts or messages
f) Audit tools used for log reviewing (analysis of logs)
g) Nobody is allowed to modify the log files.

9.8.3 Clock Synchronization.

1. All system clocks, PC clocks and network devices must be synchronized to a Central timeserver in IREL.
2. The timeserver shall provide the time via NTP.
3. The time server must be synchronized to a national or international atomic clock or to GPS satellites through a GPS antenna.
4. The time server must have a hot standby to prevent clock drifts in case of server failure.
   The standby server must be preferably installed at a distant location.
5. Users should be forbidden from changing the system clocks or time Synchronization settings. Users should be forbidden from changing the system date and time zone settings.

All NTP communications between routers and switches are statistically configured and authenticated using MD5.

9.9 Mobile computing and teleworking

9.9.1 Mobile computing.

Security of Laptop.

- **Physical security.**
  - Lock down laptops with physical cable lock wherever possible especially in public places.
  - Keep record of computer asset number (equipment capital / serial / model / year of manufacturing / hard disk serial number / MAC address of LAN and WIFI connection). This may help in recovering lost laptops.
  - As far as possible, do not leave laptop unattended. If leaving the laptop unattended, logout or turn off.
  - Do not leave laptops in vehicles they are prime attraction to car thieves. Other places one has to be careful about the Check-in counters, while waiting for baggage in airports (do not leave laptops on trolley, always carry them.),RMs etc
  - If a laptop is lost or stolen, report it immediately to local Police Station and Chief Information Security Officer (CISO) of IREL. The CISO shall inform CISAG and DAE.
  - Asset tags with physical engraving on laptop body will help prevent thieves selling the laptops.

- **Operating System Security**
  - Enable BIOS setup and user level passwords.
  - Disable boot-up capabilities of other drives in the BIOS. Make sure that select "Boot from Harddisk " only and deselected the boot from other devices such as CD, USB, Network etc.
  - Use Genuine OS (Licensed copy of OS) with latest patch and enable auto update of OS patch. Note down the OS license number for future reference
  - Admin / Administrator account may be used for administrative actions. It should not be used for normal working. Disable Guest account.
  - Create ordinary user accounts (with administrative privileges) in OS (e.g Windows) for general usage / normal working

- **Network Security**
  - Make sure to "turn off" all wireless connections like Wi-fi, Infra-red and Bluetooth in the laptop when not in use. It will increase battery backup time as well as unauthorized and unknown outside access.
  - Turn Off network services or programs which are not used like WWW, FTP services etc)

  - **<u>Wireless Network Security</u>**

1. The SSID(service Set Identifier)or ESSID(Extended Service Set Identifier)must be changed to something unique and not easily guessable before commissioning a device.
2. Identifier Broadcasting must be disabled.
3. WEP(Wired Equivalent Privacy)and WAP(Wi-fi PROTECTED Access) encryption or better must be enabled.
4. All default passwords for wireless devices must be changed to a strong password before commissioning.
5. MAC address filtering must be enabled.
6. Auto connections to open wireless networks must be disabled.
7. .Access points, hot spots and wireless routers must be installed in a way to minimize leakage of the signal to areas outside the building. Power levels must be enough to cover the required area only.
8. The network may be powered off when not needed ,e.g. after hours.

- **Data Security.**
    - Take regular back up of important data on CD or USB.

9.9.2 Teleworking

(Remote working allowed from fixed location outside the organization through VPN.)

10 SYSTEM DEVELOPMENT AND MAINTENANCE

IREL shall adopt system Development Life Cycle (SDLC) Model ,also known as Classic Life Cycle Model or linear Sequential Model or Waterfall Method. This consists of the following activities.

1. System Information Engineering and Modeling.
2. Software Requirements Analysis.
3. System analysis and Design.
4. Code Generation.
5. Testing
6. Maintenance.

All information system must meet anticipated capacity requirements. It is the responsibility of the system's development and operational teams to determine hardware requirements and capacity and monitor system performance .This includes, but is not limited to:

-Disk usage and size
-Network traffic and load
-Load balancing
-Necessary memory requirement.

-Necessary processing power.

Requirement analysis shall be carried out by a joint team of development unit, user and external parties. SRS shall be documented and signed off by competent authorities.

System designed shall be done by project leader and shall be documented and signed off by competent authorities. The design must follow IREL's IT policy and business objectives.

With respect to the type of application ,the right programming language must be chosen. IREL shall prefer and promote open source and open formats. shall prefer indigenous code, whenever possible. IREL shall retain rights and ownership of all source code written by in-house development teams or written by outsource companies for IREL exclusively IREL shall prefer escrow arrangements for third party closed source code.

Testing shall include debugging ,trail runs ,beta and full UTA according to IREL IT Quality control policies. Release versions shall be launched after extensive beta testing and reviews /feedbacks.

Changes in design, updates, upgradations and optimization/ tuning, after handling over the system for maintenance to maintenance units ,if any shall be managed by original installers and vendors, whenever possible

A changes request from or document, mentioning the nature, reason and purpose of a change shall be compulsorily submitted to the installer or system administrator. Changes shall be well documented and signed off by competent authorities.

Minor or configuration changes can be carried out by the user (maintenance staff),after necessary written approvals. Such changes must be logged.

Where ever applicable, changes shall be applied to production site first and after ensuring satisfactory performance, some shall be applied to DR system.

where ever applicable source code shall be maintained in a Subversion SVN

Frequent changes should be avoided.
Whenever there are major changes to be done or there are too many changes requests, providing a new system should be preferred instead of making those changes.

10.1 Security requirement of systems.

10.1.1 Security requirements analysis and specification

(Business requirements for new systems, or enhancements to existing systems shall specify the requirements for automate and manual controls).

10.2 Security in application systems

(To prevent loss, modification or misuse of user data in application systems).

a. Security and business continuity measures built into design of information systems.
b. Security and business continuity measures built into design of control and instrumentation systems.

10.2.1 Input data validation

Applicable for all applications

10.2.2 Control of internal processing

(Validation checks shall be incorporated into systems to detect any corruption of the data processed).
All critical applications tested are for software reliability aspects

10.2.3 Message authentication

Message Integrity protected

10.2.4 Output data validation

Applicable for all applications

10.3 Cryptographic controls

10.3.1 Policy on the use of cryptographic controls.

a) Usage of link level or network level encryption Permission for application level / Transport level encryption
b) On ANUNET Secure channel and on VPN SSL on Intranet

10.3.2 Encryption

Cryptographic Control : A suitable encryption package for storing Top Secret Data in CSM may be identified and used, as necessary.

a) Any restriction of use of encryption algorithm
b) Type of encryption used (Symmetric / Asymmetric)
c) As per the Govt. Of. India's Encryption policy Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

10.3.3 Digital signatures.

PKI infrastructure status and Legal standing of Digital signatures in the organization As per the Govt. Of. India's Encryption policy

10.3.4 Non-repudiation services.

As per the Govt. Of. India's Encryption policy

10.3.5 Key Management

a) Generation of keys
b) Obtaining certificates
c) Distribution of keys to users
d) Storing keys
e) Revoking of keys / certificates
f) Archiving keys / destroying keys

As per the Govt. Of. India's Encryption policy

10.4 Security of system files

(To ensure that IT projects and support activities are conducted in a secure manner).

10.4.1 Control of operational software

During development & testing the previous version retained as contingency measure

10.4.2 Protection of system test data

(Test data shall be protected and controlled)

10.4.3 Access control to program source library.

For protecting source code from corruption.

a) Is any restriction / authorization for accessing the source code
b) Log record for accesses to the source code Archiving of old versions with date & time Software development control

10.5 Security in development and support process

10.5.1 Change control procedures.

a) Identify the area where the changes are affecting
b) Formal approval for the proposal
c) Documentation upgrade for changes
   i. Version updates
   ii. Software development control

10.5.2 Technical review of operating system changes.

(Application systems shall be reviewed and tested when changes occur)

10.5.3 Restrictions on changes to software packages.

Modification to software packages are allowed with proper impact analysis

1. Patches shall be recommended by earlier system Admins or vendors of the s/w.In all cases, the patches must be approved by OEM or application producers.
2. Where ever applicable patches should be first applied in a production site .After satisfactory performance of the system the same can be applied at DR site.
3. Critical patches should get high priority.
4. Systems that are not connected to Internet must have some arrangement of manual installation of patches.
5. Upgrades,Updates and patching must be logged by SA in a register.
6. office PCs must be set to automatic updates, if connected to internet. offline PCs must be updated manually at periodic intervals, except for critical patches, which must be installed immediately.
7. If the application of a patch or updates affects performance adversely, the same must be uninstalled or original files may be restored from backup. If DR is available ,the sites should be switched over and vendor help may be called for.
8. Dependent processes/application owners must be informed before applying a major patch.
9. A full backup must be taken just before applying a patch.

10.5.4 Covert channels and Trojan code.

a) Is buying program from reputable vendors
b) Is source code available?

Verification of source code
Critical software from external vendor based on availability of source code and impact analysis.

10.5.5 Outsourced software development.

a) Code ownership and IPR
b) Security in Development of Outsourced Software development
c) Verification of quality and accuracy

Testing before installation
Designated departmental official verify the entire code.

11 BUSINESS CONTINUITY MANAGEMENT

11.1 Aspects of business continuity management.

11.1.1 Business continuity management process

1. Risk Management practices must be put in place so that Departmental heads can weigh the losses that may be expected to occur in the absence of an effective security control against the costs of implementing the control. Risk management is addressed through risk assessment, risk reduction and risk monitoring.
2. Risks must be assessed under three categories –confidentiality, integrity and availability .The objectives of risk analysis should be to reduce the impact of system failure or security breaches on the business.
3. Control measures may be suggested based on such assessments.
4. IT procurements policies may be reviewed in the light of risk analysis.
5. Risk and threat monitoring must be done continuously and security measures may be taken as per the need.
6. Business Continuity Policy may be formulated and implemented to ensure uninterrupted service .
7. Services may be classified based on their level of criticality and importance.
8. Disaster recovery measures may be suggested at the planning stage itself.

    a) Critical System, Critical business support systems shall have disaster recovery sites. Such sites shall be exactly mirrored and shall be located far away distances from main sites.
    b) DR site operate in hot standby mode. Data from main site shall be replicate to DR site periodically.
    c) Periodic switch over to DR shall be carried out
    d) .Suitable staff be posted at DR site and in case of emergency switch over , main site staff shall be moved to DR site.

9. Systems shall have provisions of hot standby or load-shared systems.
10. Networks shall have redundant connectivity and diversities.
11. Fail over procedures shall be documented and committed to system.
12. Periodic switch over to stand by systems shall be done and a record of the same shall be maintained.
13. All IT resources, assets and properties shall be under Insurance according to IREL's insurance.

11.1.2 Writing and implementing continuity plans.

a) Documentation of emergency procedure
b) Training of emergency procedure to staff Testing & updating of the plans

11.1.3 Business continuity planning framework.

a) Emergency procedure plan
b) Resumption procedure for returning to normal operation

11.1.4 Testing, maintaining and re-assessing business continuity plans.

Effective of disaster recovery plan is tested once in six month.

12. COMPLIANCE

The objective of this section is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. It is concerned with legal and IPR compliance.

12.1 Compliance with legal requirements.

All laws, regulations, and contractual obligations related to information security shall be complied

12.1.1 Identification of applicable legislation
12.1.2 Information Technology Act 2000, Right to Information Act.

12.1.3 Intellectual property rights (IPR)

a) Legislation for copy right
b) Any checks for software (products) installed on PC
c) **Maintaining assets register**

Intellectual property Right (IPR) of the source code and documentation and design specifically developed for IREL shall rest with the IREL. The bidder will have to submit source code and required documentation to the IREL. Any modification in the source code or documentation will be provided time to time to IREL. The IPRs will remain with their respective owners.

12.1.4 Safeguarding of organizational records.
(Important records of an organization shall be protected from loss, destruction and falsification).

a) Classification of records
Storage of records

12.1.5 Data protection and privacy of personal information.
(Controls shall be applied to protect personal information in accordance with relevant legislation).

12.1.6 Prevention of misuse of information processing facilities
Disciplinary action for misuse of computer misuse / information processing facilities

12.1.7 Regulation of cryptographic controls
Country specific

12.1.8 Collection of evidence to support action against a person / organization.

12.2 Reviews of security policy and technical compliance

(To ensure compliance of systems with organizational security policies and standards).

12.2.1 Compliance with security policy.

Responsibility of policy conformance

12.2.2 Technical compliance checking

(Information systems shall be regularly checked for compliance with security implementation standards)

12.3 System audit considerations

12.3.1 System audit controls

a) Internal auditing policy

1. Information Security Committee (ISC) shall conduct period audits of all IT systems in IREL. The internal audits shall be conducted every 3 months.
2. The auditors shall be highly trained and qualified.
3. Various audit procedures shall be clearly documented.
4. The auditors shall report their findings to CISO who in turn shall report to CISAG, DAE.
5. In case of major security issues , the matter must be referred to vigilance dept. In case of gross violation of procedures, penalty or disciplinary actions are to be taken according to the organization rules.
6. All units shall take suggested actions and report their compliance . Critical issues shall be given priority and target dates shall be fixed by the concerned units.
7. Comprehensive reports shall be communicated to IT PLANNING UNITS so that measures can be taken while planning future projects based on current experience .

b) External auditing policy

a. IREL shall also appoint independent external auditors to conduct yearly audits of all IT systems.

12.3.2 Protection of system audit tools

(Access to system audit tools shall be protected to prevent any possible misuse or compromise).