INDIAN IMMUNOLOGICALS LIMITED
Rakshapuram, Gachibowli post, Hyderabad – 500032. India
Phone : 23000211, 23000212, 23000512, 23000213
Fax : +91-40-23000213, +91 -04-23001401

Information Security Policy

Issue No.: 04.0;Copy No.: 1
Issued to:
Issued by: K Veerabhadra Rao
Date of Issue: 03-Mar-2014

MANAGEMENT APPROVAL

NAME	Designation	Role	Signature and Date
K Veerabhadra Rao	Manager – IT	Author	3/3/14
M Prabhakar Rao	General Manager – IT & Commercial	Review	4/3/2014
M Kiran Kumar	Manager – Legal & CS	Review	21/Mar/2014
K V Balasubramaniam / Dr. K Anand Kumar	Managing Director / Deputy Managing Director	Approve	22/Mar/2014

Table of Contents

Note: The above policy documents can be approved by General Manager – IT & Commercial and Issued by Manager - IT

REVISION LIST

S.NO	TITLE	PAGE NO.	REVISION NO.	DATE OF ISSUE	REASONS FOR REVISION	REVISION APPROVED (SIGNATURE)

DISTRIBUTION LIST

This manual must be strictly controlled and maintained as an internal document. The responsibility for this document is entirely of the holder of the copy. This document would be available to all the employees on organization's Intranet site under their secure login.

Copy No.	Department / Section	Designation
1.0	All Employees	All Employees
2.0	Information Technology	Executive
3.0	Information Technology	Manager
4.0	Information Technology & Commercial	General Manager
5.0	-	DMD / M.D.

1.0 Introduction

Information Security Policy is intended to provide management direction and support for Information Security Management system. This indicates the clear policy direction and demonstrates support for, and commitment to, Information Security through the issue and maintenance of an Information Security policy across the organization.

IS Security Definition

"Information security protects business critical information from a wide range of threats in order to ensure business continuity, minimize business damage and maximise return on investments and business opportunities."

Information security is driven by the following control objectives:

- **Confidentiality** concerns the protection of sensitive information from unauthorized access.
- **Integrity** relates to safeguarding the accuracy and completeness of assets.
- **Availability** relates to information being available to an authorized entity.

Information Security Management System (ISMS) is a part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. ISO27001 standard provides a guideline to develop a framework to initiate, implement, maintain and manage information security within organization. This framework has been defined as Information security management System (ISMS) that helps IIL to determine the current status of their information security programs and, where necessary, establish a target for improvement.

Corporate Information Security Policy Statement of IIL

Information Security at IIL has the senior management mandate and the security policy has been signed off by Deputy Managing Director / Managing Director, IIL.

The Security Policy states:

"Information assets are critical to the success of business of IIL and its entities. Therefore, IIL is committed to security of Organizational Information Assets including data of all its business entities, business partners and customers associated with it. IIL IT Department shall ensure that information security controls, using the most appropriate technology and process, are applied and integrated to ensure information protection from threats to confidentiality, integrity and availability thereby enhancing confidence of and adding value to all its stakeholders. Information security shall be continually monitored to ensure legal, regulatory and contractual obligations compliance at the all levels."

This Information Security policy shall be communicated to all employees through training as well as by displaying it at prominent places such as all conference halls, working areas.

Responsibility for Information security

All employees and other third parties who require access to IIL's IT related information and associated assets are responsible for ensuring that this policy is adhered to. Management at all levels is responsible for ensuring that the information users are aware of, and adhere to, this policy.

Applicability of the Policy

This Policy is applicable to all employees, contractors and other individuals affiliated with Third Parties of IIL IT department who access the information resources of IIL. Throughout this document, the word "user" is used to collectively refer to all such individuals.

2.0 Classifying Information and Data

Policy Statement

All information and data must be classified depending on its confidentiality, integrity and availability.

Explanatory Notes

Information handling procedures should be established in order to provide adequate level of security and control over information and protect from unauthorized disclosure or misuse. These procedures should be consistent with the information classification system of IIL IT department.

Policy Details

Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

2.1. Classifying Information

- All information assets must be classified under one of the following categories:
  - **Sensitive:** This classification applies to strategic business information, which is most critical and intended strictly for use within IIL. Its unauthorized disclosure could seriously and adversely impact IIL, its stockholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion.
    Examples: Merger and acquisition plans, Business plans, trade secrets, customer data, information security data, dealer pricing strategy, Strategy Documents.
  - **Confidential:** This classification applies to less sensitive business information, which is intended for use within IIL. Its unauthorized disclosure could adversely impact IIL, its stockholders, its business partners, its employees, and/or its customers. Information that some people would consider to be personal is included in this classification.
    Examples: Employee performance evaluations, CTC details, internal audit reports, short-term marketing plans, analysis of competitive products / services, designs and application

architecture documents and information capital of IIL which comprises the collective experience, knowledge, skill, and information of IIL and its people.

- **Internal Use:** This classification applies to all other information, which does not clearly fit into any of the other three classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact IIL's employees / customers stockholders & business partners.

  Examples: Information posted on intranet portals for employee usage, IIL training materials, and manuals.

  Public: This classification applies to information, which has been explicitly approved by IIL management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.

  Examples: Information posted on internet portals, Service brochures, advertisements, job opening announcements, and published press releases.

- It is the responsibility of the respective data owners to appropriately classify their data.
- All mailed data classification should be classified as per as per outlook data classification

IIL Data Classification as per Policy	IIL Data Classification mapped with Outlook
Sensitive	Private
Confidential	Confidential
Internal Use	Normal
Public	Normal / Personal

2.2. Accepting ownership for Classified Information

- IIL management must initiate measures for implementation of classification guidelines for all information assets of IIL. All IIL's critical & confidential application and data must have designated owners.
- Files created by individuals must be owned and classified by them.
- The nominated data owners will be responsible for:
  - Establishing the classification of information/data;

- Maintaining appropriate access controls to safeguard information/data;

- The data owner may delegate their security responsibilities to individual managers or the security team. However, the final accountability over resource integrity and security control resides with the owner.
- Each information asset owner is responsible for recording his asset details in the Asset Register.

2.3. Information labeling standards

- All information assets must be classified under one of the following categories:
  - Sensitive - This classification applies to strategic business information, which is most critical and intended strictly for use within IIL.
  - Confidential - This classification applies to less sensitive business information, which is intended for use within IIL.
  - Internal Use - This classification applies to all other information, which is internal to IIL.
  - Public - This classification applies to information, which has been explicitly approved by IIL management for release to the public

  Examples for respective category have been mentioned in section 2.1
- All information assets must be labeled accordingly, from the time it is created until the time it is destroyed or re-labeled. Such markings must appear on all manifestations of the information (hard copies, floppy disks, CD-ROMs, etc). All assets must be identified with a unique code number.
- For public information, the date when the owner declared the information public, must also be indicated.

2.4. Storing and Handling Classified Information

- Appropriate security classification must be clearly mentioned for all information assets of IIL. Based on the classification, the data owners will define the recipient list and handling procedures for the Information asset.
- All information must be processed and stored strictly according to the classification assigned to that information. Information processing and handling controls must be commensurate with the sensitivity of the information.

- Formal distribution lists must be used to ensure accurate distribution of restricted information. The Data Owner is responsible for reviewing the distribution lists and lists of authorized recipients at regular intervals.
- All information classified, as sensitive must specify a destruction date and recipients must destroy the document according to distribution instructions. Alternatively, information classified, as sensitive must specify a reclassification date i.e. the date when it will cease to have classification status.
- Handling Requirements, as defined in the procedure document, depending on the classified level must be adhered to.

2.5. Disclosure of Information

- Any information including data or applications held on shared equipment or stored on removable media (e.g., tapes, cartridges, diskettes, CD-ROM's, etc.) must not be disclosed to unauthorized people, business associates or third parties, without obtaining specific approvals from the owner of the data.

2.6. Security of media in transit

- Controls should be in place to protect information during physical transport. Only IIL's authorized reliable courier and delivery channels must be used.
- It must be ensured that packaging for information is sufficient to protect contents from physical damage or tampering.
- For sensitive information, special controls should be used including, but not limited to:
    - Tamper resistant packaging
    - Delivery by hand
    - The use of more than one delivery and dispatch by different routes.

2.7. Isolating Highly Sensitive Information

- All information in sensitive category must be isolated and handled in strict compliance to the Information security procedures. Refer to the Classifying Information and Data procedures.

3.0 Computer Virus Control

Policy Statement

All PC's, Laptops, workstations, servers and other information processing equipment must be adequately protected against viruses

Explanatory Notes

Computer viruses may affect the stability of a system and may cause damage or loss of valuable business information. Adequate protection from viruses would ensure that information, data, and software are protected.

Policy Details

3.1. Protection against Malicious Software

- IT department has taken initiatives to detect and prevent software and information processing facilities from malicious software.
- Users shall not disable anti-virus and shall not stop auto scan. The anti-virus software will be updated by obtaining the latest updates from the anti-virus vendor and distributed promptly across the organization.
- Bypassing the in-built scanning process is strictly prohibited.
- All software that is being used shall be procured only from authorised vendors.
- Users shall not download freeware or shareware from internet without proper authorization from IT Manager. All open source software's shall be thoroughly tested and evaluated before being used to prevent Information leakage.
- Users shall scan any electronic information being brought into IIL's environment e.g. diskettes, tapes etc prior to use.
- If a virus attack is suspected, User shall immediately remove the suspect personal computer from the network; and the immediate higher authority and System Administrator must be informed who must in turn inform various escalation points depending upon the priority of the situation.

4.0 Computing Usage Policy

Policy Statement

Every user has certain responsibilities to ensure security of the computing resources used and the data that they contain.

Explanatory Notes

Employees who have been provided with laptop/desktop and other computing resources shall ensure that security of these computing resources and data is maintained.

Policy Details

4.1. User Access to Information, Data and Application

- IIL users must be granted access to information, data and applications strictly on a "need to know" basis.
- The allocation of computing resources like Desktop/Laptop, printer, storage media, etc. to the employees will be given based on the computing requirement of the employee. The decision related to the configuration of the resource (e.g. computer or printer, etc.) and whether the resource is exclusive or shared will be decided by Manager-IT considering the job requirement of the employee.
- Access to information services will be controlled though unique userids, wherever possible, so that each user can be made accountable for their actions.
- User access rights to applications and data shall be assigned only by the application administrator, on receipt of a documented approval from his own supervisor as well as from IT Manager of the entity. All access requests must include the purpose for request of access and nature of access.
- If for any reason, a user's access rights need to be modified or revoked, the concerned IT manager/Head of the entity shall send an intimation of the same in writing to the Application administrator. The application administrator shall then accordingly modify/revoke the access rights after approval from management.

- Users will be required to re-authenticate themselves after a specific period of inactivity. All applications wherever possible will use session timeout for sensitive applications.
- All users shall be granted, "Read" access to all information classified as "public". Other rights to such information must be strictly reserved with the owner of such information.

4.2. Password Management

Access to a majority of the computing resources shall be controlled using User-Ids and passwords for identification and authentication. Hence, it is necessary that all users adhere to the following guidelines relating to passwords:

- The minimum length of passwords must be set as 6-8 alphanumeric characters.
- Password shall not be created from personnel information like family names or pet names or birthdays or dictionary words.
- A password expiration period of 90 days (or less) shall be set, so that users will be forced to change their passwords at regular intervals.
- Users shall change the password at the time of the initial logon.
- System will maintain a password history of last 5 passwords.
- System will lock the account after 3 unsuccessful attempts during logon.
- No user shall disclose passwords even to any system administrator or Helpdesk.
- If passwords have been compromised, the user shall inform the system administrator immediately and change the password.
- Passwords must never be displayed in clear text or stored in readable form in batch files in automatic login scripts or in other locations.
- Exceptions to the password management policies may be granted for certain applications only after proper management authorization.

4.3. Ensuring Logical Security on Laptops and Desktops

4.3.1. Securing information on Laptops and Desktops

- All desktops and laptops shall have a login/power-on password;

- All desktops and Laptops must have up-to-date anti-virus software installed. The System Administrator or Help Desk must ensure that updated anti-virus software is installed in all desktops and laptops;
- The folders or disk drives in individual desktops or laptops must not be shared unless appropriate access controls have been enabled on the folder or the disk drive. Sharing of any information classified as restricted or confidential is not permitted;
- Laptop users shall take necessary precautions to ensure privacy and confidentiality of IIL's data contained in laptop hard disk.

4.3.2. Security of Unattended User Equipment

- It is the responsibility of the user to ensure that it is not logged in before leaving any equipment unattended;
- Whenever a user leaves equipment unattended, it shall be secured with a screen saver with password protection, wherever available auto log out/ off settings (say after 5 minutes) shall be used. Other locking mechanisms available shall also be utilized to protect any resources when they are unattended during or beyond working hours;
- All active sessions should be terminated, when finished.

4.4. Mobile Computing

Mobile Computing consists of carrying IIL's computing resources out of the facility on a temporary basis to enable productivity while traveling in the normal course of business. Modularity and large-capacity portable drives make it easy to transport stolen data for access on another computer system. When using mobile computing facilities, special care must be taken to ensure that business information is not compromised.

Depending upon business requirements, employees may be provided with laptops to enable them to work from any locations. The decision in this accord is taken by management, i.e. Manager – IT and General Manager - IT. It is responsibility of all employees who have been provided laptop as per Laptop policy to take care of security of laptop and information stored in it.

The ownership and responsibility of all such equipment shall be clearly established to ensure accountability and maintenance.

4.5. Reporting Security Incidents and Security weaknesses

- A formal reporting procedure shall be established to enable the users to report the security incidents immediately. All employees and contractors should be aware of the procedure for reporting security incidents.
- Users should report any incident or weaknesses in systems threatening information security as per the specification. Users must report to his/her supervisor or Manager IT Officer depending on the nature of the incident/weakness. As part of the reporting, users will be required to note any symptoms, error messages, or failures.
- The user shall not attempt to perform any investigations, which could unintentionally compromise the investigation or contaminate evidence. The user shall not attempt to 'clean- up' until directed to do so by helpdesk or system administrator. A key aspect of incident investigation is preservation of evidence, destruction or cleanup of evidence will attract penalty or disciplinary action.
- The respective departments or units must notify the IT Manager if the security incident is in any way suspected or indicative of security vulnerability.

4.6. Reporting Software Malfunctions

- Users should report any software malfunctions, software not functioning correctly i.e. as per the specification (suspected malicious software, such as virus infection).
- Software malfunctions or errors must be reported to the system administrators or the help desk. As part of the reporting, users will be required to note any symptoms, error messages, or failures.
- The respective departments must notify the IT Manager if the software malfunction is in any way suspected or indicative of security vulnerability.
- The users, in the case of software malfunction are expected to follow the following procedures:
  - Note the symptom of problem and any messages appearing on the screen; and

- If a security breach is suspected (e.g. suspicious mail client behavior), the user should inform the system administrator immediately for appropriate remedial action.
- The computer should not be used until such time a clearance is obtained from the system administrators for usage of the computer. Also, the data/diskettes will not be transferred to other computers.

- In case the system administrators suspect a security breach after the preliminary assessment of the incident, they should report the matter immediately to the Chief Information Security Officer.
- The users should be warned not to attempt to remove malfunctioning software, without the support of IT department.

5.0 Personnel Security

Policy Statement

The personnel security policy specifies the information security requirements that need to be integrated in the processes including recruitment, during employment and separation

Explanatory Notes

- Ensure that security roles and responsibilities are included in the job description.
- Reduce the risks due to human error, theft or misuse of information assets or facilities.
- Minimize the damage from the security incidents by restricting access when separated.

Policy Details

5.1. Prior To Employment

- The Background verification checks shall be carried out for all employees for employment and all personal information should be maintained confidential.
- All users should sign a confidentiality agreement which will hold them liable for any unauthorized disclosure of organization information.

5.2. During Employment

- Adequate level of awareness, education and training on information security shall be provided to all employees.
- Any third party organization who access the information assets of IIL shall sign a Non-Disclosure Agreement.

5.3. Termination or Change of Employment

- Formal termination process which includes return of all information assets issued such as software, documents, equipment that is the property of IIL.
- Physical and logical access to IIL or its information assets shall be restricted.

6.0 EMAIL SECURITY

Policy Statement

The use of official e-mail should be only for IIL's business purposes and advancement of IIL's Business Interests.

Explanatory Notes

IIL has an e-mail system for all employees to facilitate better communication. The purpose of E-mail Security Policy is to define necessary standards with respect to approved use of IIL's e-mail system.

Policy Details

6.1. Authorized use

- The e-mail systems are intended for use in the conduct of IIL's business. Though limited personal usage has been allowed, employees shall use the email facility with responsibility and prudence. All e-mail messages will be considered as IIL records. The company retains all rights to read the contents of any message sent from IIL network.
- Unauthorized use of e-mail will include, but is not limited to:
  - Transmitting or storing offensive material like pornography;
  - Soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user's employment and the user's responsibilities to IIL;
  - "Spamming" - sending unsolicited messages, promotions, sending or forwarding chain letters;
  - 'Letter bombing' (re-sending the same e-mail repeatedly to one or more recipients)
  - Creating, sending, receiving or storing materials that infringe the copyright or other intellectual property right of any third parties.
  - Sending, transmitting or distributing proprietary information, data or other confidential IIL information to unauthorized recipients.

- No advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about IIL may be issued unless it has first been approved by the Marketing/ Public Relation Departments.
- There can be limited personal usage of IIL's email system and it should not compromise its official usage.

6.2. Awareness and Undertaking

- It is the responsibility of the users, who have been provided with the electronic mail facility, to make themselves aware of the usage norms and their responsibilities towards it.

6.3. Access to external Email Systems (like Hotmail, Rediffmail, yahoo etc)

- IIL provides Corporate Emailing facility to all authorized and approved users for official and business usage. All employees are encouraged to send mails using the official email facility provided.
- IIL will not provide access for external webmail portals like Hotmail, Rediff Mail, Yahoo Mail, Gmail etc. Since Email functionality is being provided by corporate email system, employees would be prohibited from using the above for any official communication.

6.4. Access to IIL's E-mail System

- IIL will reserve the right to inspect and review any data maintained in its e-mail system without prior consent of, or notification to, the employee.
- IIL may disclose contents of e-mail either internally or to external parties, where necessary, for a legitimate business reason, without any permission of the employee.

6.5. Approved Users

- E-mail facility shall be granted to users only after receiving approval from the immediate supervisory authority or after approval from HR.
- Users shall not allow anyone else to send email using their Email accounts. This includes their supervisors, secretaries, assistants and any other subordinates. Though, Users shall make

suitable arrangements during their absence to ensure that company's interest is not affected because of inaccessibility of their e-mail facility.

- All e-mail users (including contractors) shall sign non-disclosure agreement / terms of usage of information security policy confirming that they shall abide by policy to follow usage norms for email rights provided to them.

6.6. Transmission of Sensitive Information

- Users are prohibited from sending highly sensitive information or data via e-mail, unless strong encryption or similar approved technologies are used.

6.7. Email attachments

- All e-mail attachments must be scanned for viruses before opening it.
- User should not open e-mail attachments unless they are sure about its contents and know their senders.

6.8. Distribution list management

- Mails to a larger group should always be sent using the distribution lists.
- Individual owners would be defined for the purposes of authorizing additions and deletions to the distribution lists.
- Posting to BLOGs or Discussion Forums is strictly prohibited unless authorized by employee's supervisor and IT Department.

6.9. Mailbox and E- Mail Size Limitations

- Size of the e-mail should be kept as small as possible as defined by IT Dept., from time to time. For sharing large files within the office, shared folders on the network resource should be preferred over sending e-mail;
- Every individual should be assigned a limit on the size of Mailbox. This will vary as per the job requirement of the user. Maximum size of e-mail with attachment permissible is 5 MB. In case of absolute necessity, the mails with bigger attachment sizes can be requested through itcommunication@indimmune.com , which will be maintained by the IT-Department;

- An automatic warning should be given by email administrator to user once the mail box is reached 80% of mailbox limit ;
- Users shall be trained to periodically archive their mails on the local systems and the manner in which the personal folders need to be protected;
- Users are encouraged to send all attachments to mails in a compressed mode/ zipped format;

6.10. Logging and Auditing

- Server Log will be enabled on the Email Server. Authentication logs shall be logged. Individual Email Databases will keep a track of access to the database.
- Logs will be reviewed periodically and relevant action will be taken based on the findings.
- The log audit will be carried out by the Nominated personnel, and the reports will be submitted to Manager IT.

6.11. Email retention period

- The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.
- E-mail Retention Categories: E-mail information is categorized into four main classifications with retention guidelines.

Category	Retention Period
Administrative Correspondence	4 Years
Fiscal Correspondence	4 Years
General Correspondence	1 Year
Ephemeral Correspondence	Retain until read, destroy

- E-mail Retention Categories Definitions:
- Administrative Correspondence

  Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and

any legal issues such as intellectual property violations. All e-mail with the information sensitivity label "Management only" shall be treated as Administrative Correspondence.

- Fiscal Correspondence

  Fiscal Correspondence is all information related to revenue and expense for the company.

  As per Information security policy of IIL, to ensure Fiscal Correspondence is retained.

- General Correspondence

  General Correspondence covers information that relates to customer interaction and the operational decisions of the business.

  As per Information security policy of IIL, the individual employee is responsible for e-mail retention of General Correspondence.

- Ephemeral Correspondence

  As per Information security policy of IIL, Ephemeral Correspondence is by far the largest category and includes personal e-mail, requests for recommendations or review, product development, updates and status reports related emails.

6.12.Exceptions and Third Party ID Creation

- Exceptions to the security Policy shall be documented and approved.
- Creation of temporary IDs for use of IIL resources is against security policy. Such cases shall be treated as exceptions based on business need for a temporary id.
- It shall be created only if the following conditions are met
  - Request is approved by Senior manager or the entity
  - Start and End date for the account is specified.
  - Only one user has access to the account and the user shall be specified in form.
  - The user must sign the security policy or the NDA should exist between IIL and the third party.

- In case of a business need for granting access to Internal Email systems of IIL for Third Party personnel, External Parties Policy needs to be referred and the External Parties Procedure needs to be followed.

6.13.Enforcement

- Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment and if warranted, appropriate legal action.

7.0 Internet Usage and Security

Policy Statement

The Internet Usage & Security Policy shall define a coherent information security policy that shall help to enable disciplined usage of Internet and to protect information systems from attacks through the Internet.

Explanatory Notes

The Internet is a world wide public network, that is changing the way organizations and individuals communicate and do business. Internet provides a number of services including e-mail, file transfer, login from remote systems, data storage, news groups and the World Wide Web.

However, use of the Internet presents new and heightened risks. The Internet suffers from significant and a widespread security problem that makes organizations open to intruders.

Policy Details

7.1. Access to Internet

Employees shall be provided with Internet access on a need basis.

7.2. Authorized and Unauthorized use of Internet

- Internet usage must be restricted to serve business requirements. Though Internet facility has been provided to employees for official purposes only, they may use it for limited personal usage. They shall use Internet facility with responsibility and prudence.
- Unauthorized use of Internet will include, but is not limited to:
  - Using for personal entertainment, personal business or profit, and publishing personal opinions.
  - Attempting to gain or gaining unauthorized access to any computer system of IIL or any other organization.
  - Sending/receiving/viewing racial, sexually threatening, defamatory or harassing messages.

- Sending, transmitting or distributing proprietary information, data or other confidential IIL information.
- Using Internet for non-business purposes and wasting computer resources like uploading and downloading large files not related to business, accessing streamline audio and/or video files, playing games on the Internet and engaging in online chat groups, not related to business.
- Introducing computer viruses, worms, or Trojan horses.
- Downloading obscene written material or pornography.

7.3. Downloading and Uploading of Software

- The users are not allowed to download or upload any software from/to Internet without prior approval from the System Administrator as well as from their reporting manager. Any software download or upload should be based on business requirement.
- If it requires downloading software for business reasons, the downloaded software must be tested on a stand-alone non-production machine that has been recently backed-up. (clause: tested by IT representative)
- There will be periodic review of all desktops by system administrators to ensure that no unauthorized software is installed.

8.0 Physical Security at work place

Policy Statement

Work environment must be secured from unauthorized access, damage or interference. Physical security measures must be in place to ensure the security and integrity of information processing facilities and the information assets located within.

Explanatory Notes

The Physical and Environmental Security Policy defines the physical security standards and the environmental controls at work places that shall be followed in order to maintain a minimum level of protection to information systems. Users shall also need to follow certain guidelines to ensure physical security of information and information processing systems in their work environments.

Policy Details

8.1. Securing the premises from visitors and third parties

- The date and time of entry and departure of visitors and third parties and the purpose of visit must be recorded in a visitor's log.
- No employee is authorized to take any visitor near user workstations. He should keep his entry restricted to the discussion rooms or reception area.
- Visitors and third parties shall be allowed entry to work places for authorized and specific purposes only. They must not be permitted unsupervised access to IIL's computer/laptops.

8.2. Identification Badges

- All employees, visitors and third parties are required to wear badges within IIL premises.
- Identification badges and access cards shall not be shared with other users.
- The visitor badges must be returned to security personnel or receptionist.
- IIL personnel must question unescorted strangers or those not wearing visible identification.

- Identification badges must be returned by employees, when retired or transferred/terminated and by personnel of outsourcing agencies at the end of the contract.

8.3. Issue of duplicate identification badges

- It will be the responsibility of each employee or third parties, who has been issued an identification badge to immediately report lost or stolen badges to Administration department.
- The original identification badge will be taken back while issuing a duplicate badge in case of damaged badges.

8.4. Clear Desk and clear screen policy

- Computer terminals must not be left logged on, when unattended. Key locks, power-on and screensaver passwords, or other controls shall be used to protect them when not in use.
- Computer media, like Floppy diskettes, CDs, tapes, external hard-disks etc. containing confidential information or otherwise shall not be left unattended. They shall be stored in suitable locked cabinets when not in use, especially after working hours.
- Computer terminals should be switched off when not in use and should be protected by key locks, passwords, screensavers or equivalent controls to ensure sensitive information are not easily available to an unauthorized user.
- Files and other papers (non-electronic format) that contain sensitive or confidential information must be protected from unauthorized access. Users shall not leave such papers unattended on printer trays, photocopiers, fax machines or on their desks.
- Incoming and outgoing mail points and unattended fax and telex machines must be protected from unauthorized use outside normal working hours.
- 'Sensitive' and 'Confidential' information and storage media must be locked (ideally in a fire-resistant safe or cabinet), when not required.