REVISION HISTORY

No	Date	Name	Designation	Role	Description	Version
1.	01/02/2012	Hemant Nakti	IT Infra Manager	Creator	First Release	1.00
2.	01/03/2012	Vishal Doctor	Director	Approver	First Release	1.00
3.	05/05/2014	Dinesh Rao	VP – IT & OPS	Reviewer	Review & Changes (Details of changes in Appendix 'A')	2.00
4.	06/05/2014	Vishal Doctor	Director	Approver	Review & Changes (Details of changes in Appendix 'A')	2.00
5.	15/09/2015	Hemant Nakti	IT Infra Manager	Creator	Changes done in few policy (Details are mentioned in Appendix 'A')	2.01
6.	21/12/2015	Dinesh Rao	VP – IT & OPS	Reviewer	Review & Changes (Details of changes in Appendix 'A')	2.01
7.	23/12/2015	Vishal Doctor	Director	Approver	Review & Changes (Details of changes in Appendix 'A')	2.01
8.	16/08/2016	Bhavin Bheda	IT Infra Manager	Creator	Changes done in few policy (Details are mentioned in Appendix 'A')	3.00
9.	16/08/2016	Dinesh Rao	VP – IT & OPS	Reviewer	Review & Changes (Details of changes in Appendix 'A')	3.00
10.	16/08/2016	Viral Doctor	Director	Approver	Review & Changes (Details of changes in Appendix 'A')	3.00
11.	03/05/2018	Kamal Chatnani	Audit Manager	Reviewer	Review & Changes (Details of changes in Appendix 'A')	3.01
12.	03/05/2018	Sacchin Sharma	IT Manager	Reviewer	Review & Changes (Details of changes in Appendix 'A')	3.01
13.	03/05/2018	Dinesh Rao	VP – IT & OPS	Approver	Review & Changes (Details of changes in Appendix 'A')	3.01

Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of OEC. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for OEC to recover. This information security policy outlines OEC's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Company's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details. LSE is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the OEC is responsible. OEC is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001.

Objectives

The objectives of this policy are to:
1. Provide a framework for establishing suitable levels of information security for all OEC's information systems (including but not limited to all computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. a. This explicitly includes any ISO27001-certified Information Security Management Systems the Company may run.
b. The resources required to manage such systems will be made available
c. Continuous improvement of any ISMS will be undertaken in accordance with Plan Do Check Act principles
2. Make certain that users are aware of and comply with all current and relevant policy.
3. Provide the principles by which safe and secure information systems working environment can be established for staff and any other authorized users.
4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect OEC from liability or damage through the misuse of its IT facilities.
6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
7. Respond to changes in the context of the organization as appropriate, initiating a cycle of continuous improvement.

Responsibilities

All OEC staff and employees are expected to:
1. Understand the information classification levels defined in the Information Security Policy.
2. As appropriate, classify the information for which one is responsible accordingly.
3. Access information only as needed to meet legitimate business needs.
4. Not divulge copy, release, sell, and loan, alter or destroy any OEC's Information without a valid business purpose and/or authorization.
5. Protect the confidentiality, integrity and availability of OEC's Information in a manner consistent with the information's classification level and type.
6. Handle information in accordance with the OEC's Information Protection Standards and Procedures and any other applicable OEC's standard or policy.
7. Safeguard any physical key, ID card, computer account, or network account that allows one to access OEC's Information.
8. Discard media containing OEC's information in a manner consistent with the information's classification level, type, and any applicable OEC's requirement. This includes information contained in any hard copy document or report) or in any electronic, magnetic or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).

INDEX

Reference	Name of Procedures	Page
Ref: ISPOL-01	Acceptable Use Policy - Information Services	5
Ref: ISPOL-02	Information Backup Policy	6
Ref: ISPOL-03	Clear Desk Policy	7
Ref: ISPOL-04	Clear Screen Policy	8
Ref: ISPOL-05	Disposal of Company Sensitive Data	9
Ref: ISPOL-06	Electronics Device Policy	10
Ref: ISPOL-07	Laptop Policy	11
Ref: ISPOL-08	Operations Security	13
Ref: ISPOL-09	Password Policy	14
Ref: ISPOL-10	Patch Management Policy & Procedure	15
Ref: ISPOL-11	Physical Media in Transit	16
Ref: ISPOL-12	Access Card Policy	17
Ref: ISPOL-13	Removal of Access Policy	18
Ref: ISPOL-14	Server Room Restricted Access List	19
Ref: ISPOL-15	Training and Awareness Policy	20
Ref: ISPOL-16	Visitor's Policy	21
Ref: ISPOL-17	LAN Security Policy	22
Ref: ISPOL-18	Workstation Policy	27
Ref: ISPOL-19	Cryptographic Policy	28
Ref: ISPOL-20	OEC Infrastructure Policy	30
Ref: ISPOL-21	Coding Standards	34
Ref: ISPOL-21	Source Code Password Policy	35
Ref: ISPOL-22	Email Policy	36
Ref: ISPOL-23	Password Security Policy	39
Ref: ISPOL-24	Security Incident Management Policy	40
Ref: ISPOL-25	Owners and Custodians Policy	42
Ref: ISPOL-26	Data Privacy and Classification Policy	43
Ref: ISPOL-27	Data Purging Policy	45
Ref: ISPOL-28	Log collection and Retention Policy	46

Ref: ISPOL-29	Change Management Policy	47
Ref: ISPOL-30	User Access Management Policy	50
Ref: ISPOL-31	System & Application Access Control Policy	54
Ref: ISPOL-32	Information Processing Facilities Policy	55
Ref: ISPOL-33	Intellectual Property Rights Policy	56
Ref: ISPOL-34	Outsourced Development	58
Ref: ISPOL-35	Protection Of Test Data	60
Ref: ISPOL-36	Restriction On Changes To Software Packages	61
Ref: ISPOL-37	Secure Development Environment	62
Ref: ISPOL-38	Secure Development Policy	63
Ref: ISPOL-39	Secure System Engineering Principles	64
Ref: ISPOL-40	System Acceptance Testing	65
Ref: ISPOL-41	System Change Control Procedures	67
Ref: ISPOL-42	System Security Testing	68
Ref: ISPOL-43	Technical Review Of Applications After Operating Platform Changes	69
Appendix – A		70

Ref: ISPOL-01 Acceptable Use Policy - Information Services

1. I hereby acknowledge that I have read and understood all the security policies set by OEC i.e. - Digital Infrastructure Policy, Clean desk, Clear screen, Data backup, Electronic devices, Workstation Policy, Laptop policy, Operation policy, Password policy, Removal of access, Disposal of Sensitive Materials, Visitors policy, Workstation Data Backup Policy, etc.

2. I understand that the confidential data like client source code, database schemas, etc are the property of the company and I am not permitted to do an unauthorized transfer of the above mentioned data to the outside world by email, upload, download or any other way. I understand that it is my responsibility to safeguard this information from unauthorized use and will ensure that all copies are either destroyed or returned to The OEC, when I have finished. If engaged at a client site, I will apply this same practice there as well

3. I understand all the infrastructure resources, (networks, servers, workstations, etc) are continuously monitored for unauthorized activities.

4. I am aware my access privileges will be revoked upon any security compromise, (wilfully or unintentionally), to ensure the integrity of The OEC infrastructure. This access may be reinstated only with authorization from my manager or human resources.

5. I understand I am not allowed to Send/Receive non business/personal emails 'To & From' OEC account.

Penalties:

OEC may take any one or more of the following actions in response to complaints and/or violations of the IS Policies:

a. Issue warnings: written or verbal
b. Suspend account
c. Terminate account
d. Bring legal action to enjoin violations and/or to collect damages, if any, caused by violations.

OEC reserves the right to revise, amend, or modify these IS Policies at any time. Policy changes will be immediately published to the all employees

Full Name : _____

DOJ : _____

Signature : _____

Ref: ISPOL-02 Information Backup Policy

Purpose

The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. This document is intended to provide details on the stipulations of data backup and retrieval operations to the client.

Scope

The intended recipients of this policy are internal departments that house their hardware / software in the Cloud Enterprise Data Centre.

Policy

Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

Procedures

The backup server currently deployed has an LTO 3 backup tape device and a Virtual Tape Library attached to it. The type of backup varies with the model of the server and the volume of data to be backed up.

The backup software used to control the backup processes is online Ctrls Data Assurance 4.4.0 ®. The Systems Support team ensures that all backups are completed successfully and reviews the backup process on all servers daily. Logs are maintained to verify the amount of data backed up and the unsuccessful backup occurrences. There will be a daily incremental backup taken on Monday to Friday for the critical data of the company, a full weekly backup on every Saturday, full monthly backup on the last day of every Month, Quarterly backup every 90 days interval.

Backup Content

The content of data backed up varies from server-to-server. The primary data that will be backed up are: Data files designated by the respective owners of the servers and in some instances System Data (Applications files for the server and other selected software installed on the server). Data to be backed up will be listed by location and specified data sources. This will be stipulated in a separate document called “Data Sources Manifest”. Because it is impractical for the Systems Support to backup every bit of data stored on the servers, the only data that Systems accepts responsibility for is the data which is explicitly listed in the “Data Source Manifest”.

Ref: ISPOL-03 Clear Desk Policy

It is crucial to protect sensitive information from disclosure. Office space is frequently visited by visitors, consultants, vendors, cleaning crews, maintenance and fellow employees.

The work place should be kept neat & clean. If it is messy, it is very difficult to notice if anything goes missing.

Throughout the day:

1. Lock sensitive documents and computer media in drawers or filing cabinets
2. Ensure physical safety of laptops
3. Secure the Laptop/PC by locking it before leaving the workstation (Ctrl+Alt+Delete)
4. Do not post sensitive documents. Examples include:
    - 4.1 User IDs & Passwords
    - 4.2 IP addresses
    - 4.3 Contracts
    - 4.4 Account numbers
    - 4.5 Client lists
    - 4.6 Intellectual property
    - 4.7 Employee records
    - 4.8 Anything that is not to be disclosed

At the end of the day, take a moment to:

1. Keep the workstation tidy and secure sensitive material
2. Lock drawers, file cabinets and offices
3. Secure expensive equipments (laptops, PDAs, etc.)

Ref: ISPOL-04 Clear Screen Policy

With open planned offices becoming common, one could accidentally expose confidential material. Information can be read from the screen, especially when the workstation is logged on and one is away from the desk.

A Clear Screen Policy is an effective safeguard. If the screen is readable when one is absent from his/her desk or work area, this may result in sensitive information being read and 'leaked' to unauthorized persons.

When people can see when sensitive information is being accessed, it facilitates either pre-meditated or opportunistic attempts to read and copy the data when the PC is left unattended; even for a short period.

No sensitive file, shortcut to any sensitive file/application or diagram to be kept on the desktop - 'keep the desktop/screen clean'.

Ref: ISPOL-05 Disposal of Company Sensitive Data

Sensitive materials must be thoroughly sanitized before being discarded.

PAPER:
Paper containing sensitive information must be shredded. Cut papers into fine/small pieces and disposed properly.

Examples include:

1. Source codes
2. User IDs & Passwords
3. IP addresses
4. Contracts
5. Account numbers
6. Client lists
7. Intellectual property
8. Employee records
9. Anything you wouldn't want disclosed, etc...

IT ASSETS:
All IT assets as listed below must be disposed securely by approved prime third party vendor.

1. PC
2. Laptop
3. Server
4. Printer
5. Scanner
6. USB
7. Memory Stick
8. Hard Disk
9. CD/DVD
10. LTO tapes

The IT department is responsible for backing up and then wiping off company sensitive data from all IT assets slated for disposal; as well as removing off company tags and/or identifying labels.

The employees who are carrying the company IT assets should hand over the same back to IS Department on completion of the specified task.

Ref: ISPOL-06 Electronics Device Policy

Unauthorized devices pose a significant threat to security. The use of electronic devices must be strictly controlled to prevent information leaks.

With new devices being produced each year, it is difficult to specifically address each one.

I. Personally owned devices which fall into these categories are prohibited within company premises:

Computer systems: Computer systems can be used to store sensitive data and may introduce viruses into the network.

Recording devices: Audio visual recording devices represent a threat for obvious reasons. Examples include digital cameras, PC cameras and video recorders.

Storage devices: Small storage devices and backup media can be used to transport large quantities of sensitive information. The IS department backs up files stored on networked personal drives. Employees do not need to make their own backups. Examples of specific prohibited devices are zip drives, CD RW drives, and USB storage devices.

Networking: Modems and wireless network devices must meet a business need and be approved, installed and maintained by the IS department. Do not use unapproved methods to remotely access company systems.

External hard drive/pen drive: Do not bring personal pen drive and external drive in the company work areas. If you need any data to be transferred, then contact IS department.

Consultants and visitors must be advised of these restrictions and monitored for compliance.

II. Company owned devices must be used responsibly:

1. Sensitive data on laptops and PDAs must be encrypted. If either is lost or stolen, report the incident to the Helpdesk immediately.
2. Be mindful of the background when using audio visual recording equipment. Protect tapes in accordance with the sensitivity of the information. Avoid recording meetings.
3. Store Company owned electronic equipment under lock and key.

Ref: ISPOL-07 Laptop Policy

Personal computers typically do not provide technical controls for user authentication, access control, or memory protection that differentiates between system memory and memory used for user applications. Due to lack of controls and the resultant freedom with which users can share and modify software, personal computers are more prone to attack by viruses, unauthorized users and related threats.

The loss of a laptop can cause irreparable harm to the organization. Laptops must be secured and used with responsibility to prevent compromise of sensitive information or unauthorized network access.

The IS department has taken measures to address the threats which laptop users face. Your active involvement is critical to complete the equation:

1. Laptop theft: When leaving a laptop unattended in a hotel room or office space, lock it to an unmovable or extremely heavy object using its security cable. Personal Laptops are strictly not allowed in the office.

2. System compromise: The operating system is hardened against attack.

3. Patches: The help desk will periodically recall your laptop to install security patches.

4. Network threats: Laptops are equipped and configured with software firewall to defend against hacking attempts on public networks and the Internet.

5. Data threat: USB Ports, CD/DVD, Admin privileges will be unavailable to protect the data. The user has to take the permission from IS Dept if He / She is carrying the laptop abroad & out of town.

6. Viruses: Anti-Virus definitions must be updated weekly to be effective. Keep your definitions current to avoid a system outage while you are travelling.

7. Theft of confidential files: The sensitive files must be stored using file encryption software to safeguard the data against stealing/loss of laptop.

8. Password compromise: Do not save passwords in files, web browsers, VPN clients or any other insecure software. Store passwords with encrypted password management software

9. Electrical surges: Protect your laptop from electrical spikes by plugging its power and modem connections into a surge protector.

Virus prevention in the PC environment must rely on continual user awareness to adequately detect potential threats and then to contain and recover from the damage. Personal computer users must practice their virus prevention management as a part of their general computing.

Personal computers generally do not contain auditing features, thus a user must be aware at all times of the computer's performance, i.e., what is normal or abnormal activity to understand some of the technical aspects of their computers in order to detect security problems, and to recover from those problems. Not all personal computer users are technically oriented, thus this poses some problems and places even more emphasis on user education and involvement in virus prevention. If you need assistance with updating virus definitions, using file encryption or any other security features, please contact the help desk.

Because of the dependence on user involvement, policies for LAN environments (and thus PC usage) are more difficult to implement than in a multi-user computer environment. However, emphasizing these policies as part of a user education program will help to ingrain them in users' behaviour.

The list of effective personal computer management practices specific to each personal computing environment is prepared. Creating such a list would save users the problem of determining how best to enact the policies, and would serve as a convenient checklist that users could reference as necessary.

The loss of a laptop is a serious security incident. In the event a laptop is lost or stolen, immediately contact help desk.

Ref: ISPOL-08 Operations Security

Operations security (OPSEC) addresses the confidentiality of internal business processes and sensitive information.

If OPSEC is breached, the compromise can be used to gain access, disrupt operations and/or for competitive advantage.

Adversaries may call many people throughout an organization, gathering small bits of internal information along the way (a name here, a term there). Before long, they have enough knowledge to impersonate an authorized user. Verify identity and distribute information based on a party's need-to-know. If someone is asking for internal information, verify his or her identity. If they don't have a need-to-know, the topic is none of their business (literally). Mention company policy as your reason for not disclosing the information.

Sensitive information can be deduced by gathering several pieces of public or uncontrolled information (aggregation and inference). For this reason, semi-sensitive information must be protected as well. Take a hard look at what outsiders can learn from public sources and observing your operations. Web sites frequently the source of information leaks. Do not post semi-sensitive information in areas that are accessible to the public or visitors (i.e. lobbies, reception areas, conference rooms and office space).

The examples of semi-sensitive information include:

1. Organization charts
2. Employee directories
3. Store numbers
4. Employee numbers
5. Site locations
6. Building blueprints
7. Names of vendors or suppliers
8. Approved processes for gaining access
9. Authorizing a visitor
10. Obtaining an ID access card
11. Obtaining a network, system or application account

Everyone throughout the organization must be aware of these threats and act accordingly to protect against them. Identify sensitive information in your area of responsibility (i.e. client lists or source code). Critically evaluate how it is protected.

Ref: ISPOL-09 Password Policy

Hackers use software and word lists to automate password submittals. Source materials include dictionary files and list of common names, characters, movies, etc. Using these methods, hackers can compromise weak passwords in less than an hour.

As per company policy, the password must meet complexity requirements as described below:

1. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
2. At least 8 characters in length
3. Contain characters from three of the following categories:
    - 3.1 English uppercase characters (A through Z)
    - 3.2 Base 10 digits (0 through 9)
    - 3.3 Non-alphabetic characters (for example,!, $, #, %)

The following password elements are prohibited:

1. Common elements (i.e. words, names, sports, movies & shows, groups, songs, etc.)
2. Elements relating to the user (i.e. user id, graduation, birthdays, phone numbers, pets, etc.)
3. Keyboard patterns (i.e. 1q2w3e4r)
4. Repeating patterns (i.e. ah*fJDS1, ah*fJDS2, etc.)

The following practices are prohibited:

1. Recording user ids or passwords on paper
2. Group accounts or shared passwords (passwords provide accountability, user to system)
3. Distribution of passwords by e-mail or other insecure methods (i.e. fax)
4. Use of the same password on multiple systems

Before distributing a password, positively identify the person and their need-to-know.

Change your password at least every 45 days and whenever you suspect it has been compromised.

Minimum pass

To change your password, Press (Ctrl+Alt+Delete) -> Click on Change password.

Ref: ISPOL-10 Patch Management Policy & Procedure

POLICY: The patch management is very important for our organization for information security in terms of data retrieves ability and availability and IS department is committed to provide it timely. All functional heads are advised to follow the procedure below.

Patch Management Standard Operating Procedure:

1. Subscribe for the Microsoft bulletin notifications on the Microsoft site.
2. Once the notification is received, it will be forwarded by the IS manager to the IS team.
3. The IS team will download the necessary patches.
4. The patches will be installed on one system belonging to each project and mail will be sent to all the TL's to check and confirm if they face any problems with the patch installation for 2 days.
5. If the TL's report of any problems faced with the patch installation it will be rolled back.
6. If the TL's confirm there is no problem with the patch installation, the patches will be rolled out for all the systems of the project.
7. An excel file will be maintained with the details of the monthly patch installation.

Ref: ISPOL-11 Physical Media in Transit

Confidential data may be exposed to unauthorized persons, threatening the confidentiality of sensitive information.

Equipment can be damaged in transit:

- The data should be encrypted before sending CD/DVD/ HDD.
- The data should be backed up before sending equipment
- The HDD should be removed before sending equipment (like Server/PC etc.)for replacement or Repair
- In case if hard drive needs to be sent to the vendor for data recovery, IS should take an approval from management about the confidentiality of data and the need for recovery of the data.

Ref: ISPOL-12 Access Card Policy

1. Keep Access card along with you while in office premises
2. In case of returning late after work, it might be required as identity proof for patrolling personnel
3. Please do not use any other employees Access Card
4. Resources travelling abroad on official work for long time period-please submit your Access card to Administration department
5. For abroad short visit, you may keep the access card with you
6. In case of loss of Access card please report to Administration dept. immediately to avoid misuse. One will be charged for the new access card as per admin policy.
7. In case of change in Emergency contact number, please inform the Administration department.

Ref: ISPOL-13 Removal of Access Policy

Unauthorized access can cause serious damage to the organization. Dissatisfied employees can use lingering accesses to enter systems or office space. Hackers can use inactive accounts to enter systems unnoticed. Potential damage includes theft of funds, equipment or intellectual property, disclosure of confidential information, and/or damage to property or personnel.

When an employee leaves their accesses must be immediately revoked. Admin Head should initiate systematic removal of accesses with the helpdesk and building security. When an employee leaves, their supervisor must ensure accesses are removed. Employees must only have the accesses as their position requires. When roles change, supervisors must withdraw accesses which are not needed.

The help desk goes to great lengths to track and rescind accesses. However, it is possible to overlook the extent of a user's accesses. The typical user has more than network and voice mail access. There are remote accesses, custom applications, development servers, etc. Please take a moment to drop an e-mail to the help desk if you notice a former employee in the network e-mail address book, on a development server or elsewhere.

Ref: ISPOL-14 Server Room Restricted Access List

Restricted Access

Policy:
All the servers are lying in the server room. The unauthorized person may steal the information from the server room.

Authorized Personnel:

1. Dinesh Rao | VP- IT & Ops
2. Bhavin Bheda| Manager- IT Infra
3. Satish Divekar | Asst. Manager - Tech
4. Yashpal Puthran | Manager- Software
5. Sweta Bhagat |Senior Programmer
6. Nilima Solaskar | Executive Programmer
7. Shyam Shivcharan| Jr. Sys Admin
8. Rohit Vishwakarma | Jr. Sys Admin
9. Pradeep Kolatheril | Sr. Manager- Security
10. Security Desk | Security Guard*

The above persons are allowed to enter the server room areas. Other than the above listed personnel, no other person should enter the server room.

As part of an audit exercise, an auditor or any other authorized person can enter the server room with due approval from VP – IT. However, in such scenarios, the auditor or that person will have to be escorted by the Manager – IT Infra or Jr. System Admin person.

If anyone notices any unauthorized person in the server room, then VP – IT / IT Head should be notified immediately.

* Any security guard can enter the server room at the time of duty/shift.

Ref: ISPOL-15 Training and Awareness Policy

OEC has made a policy to provide for the mandatory periodic training in computer security awareness and accepted computer practices for all the employees who are involved in the management, use, or operation of each computer

system within or under the supervision.
This policy provides a framework for identifying computer security training requirements for adversity of audiences who should receive some form of computer security training. It focuses on learning objectives based upon the extent to which computer security knowledge is required by an individual as it applies to his or her job function for detailed discussion and guidance for general computer security training. To maintain security in a LAN environment, training in certain areas of LAN operation and use, training should be imparted to LAN users. Security mechanisms, procedures, etc. may not be effective if they are used improperly. Training areas that should be considered are listed below for functional managers, LAN managers and general users.

The training area for functional managers focuses on:
(1) The need to understand the importance of the security policy
(2) How that policy needs to be implemented into the LAN for it to be effective.

The training area for LAN managers focuses on the need to understand how security is provided for the LAN operationally. It also directs attention on the need for effective incident response.

The training area for all users focuses on:
(1) Recognizing the user role in the security policy and the responsibilities assigned there
(2) Using the security services and mechanisms effectively to maintain security
(3) Understanding how to use the incident response procedures.

Functional Managers

1. Recognize the importance of the LAN security policy and how this policy drives the decisions made regarding LAN security. Recognize the importance of determining adequate security for different types of information that the functional manager owns (or has responsibility for).
2. Recognize the LAN as a valuable resource to the organization and the need for protecting that resource. Recognize the importance of providing for adequate protection (through funding, personnel, etc.).

LAN Management

1. Understand how the LAN operates in all aspects. Ability to recognize normal operating versus abnormal operating behaviour.
2. Understand LAN management's role in implementing the LAN security policy.
3. Understand how the security services and mechanisms work. Ability to recognize improper use of the security mechanisms by users.
4. Understand how to use the incident response capability effectively.

LAN Users

1. Understand the security policy and the user responsibilities dictated there. Understand why maintaining LAN security is important.
2. Understand how to use the security services and mechanisms provided by the LAN to maintain the security of the LAN and protect critical information.
3. Understand how to use the incident response capability, how to report and incident, etc.
4. Recognize normal workstation or PC behaviour versus abnormal behaviour.

Ref: ISPOL-16 Visitor's Policy

All un-escorted visitors within the company's premises are a serious threat to the security of the organization.

Upon arrival, visitors must present an ID card, and sign the visitor log. All items are subject to search. Laptops must be signed in and out.

Security will phone the concerned employee to inform him/her of a visitor's presence. Entry is not permitted until an escort arrives.

Provide the guard with your employee ID card and sign in the register meant for the visitor.

Visitors must be escorted at all times. Watch visitors closely. Smart devices can be used to take pictures and store large amounts of sensitive data. If you need to step away, ensure that someone else accepts responsibility for watching the visitor. This includes escorting visitors back to the security desk. Frequent visitors must not receive any special treatment.

Instruct visitors to wear their visitor badge so that they can be easily identified.

At no time will a visitor be given access to the company network without formal authorization from the security group.

Never let visitors (or anyone else) borrow your access card. Tours of restricted areas are absolutely prohibited.

Visits should be confined to normal business hours. If a visitor needs to come in early or leave late, the Admin /Security group must be notified. All other escort procedures apply.

Report any suspicious activity to building security immediately, followed by the Admin group.

Ref: ISPOL-17 LAN Security Policy

1.0 PURPOSE:

The information residing on the OEC local area r (LAN) is mission critical. The size and complexity of the LAN within OEC has increased and now processes sensitive information. Because of this specific security measures, procedures must be implemented to protect the information being processed on the OEC LAN. The OEC LAN facilitates sharing of information and programs by multiple users. This environment increases security risk and requires more stringent protection mechanisms than a standalone micro computer (PC) operation. These expanding security requirements in the OEC computing environment are recognized by this policy which addresses the use of the OEC LAN.

This policy statement has two purposes:

1. Emphasize for all OEC employees the importance of security in the OEC LAN environment and their role in maintaining that security.
2. Assign specific responsibilities for the provision of data and information security, and for the security of the OEC LAN itself.

2.0 SCOPE:

All automated information assets and services that are utilized by the OEC Agency Local Area Network (LAN) are covered by this policy. It applies equally to LAN servers, peripheral equipment, workstations, and personal computers (PCs) within the OEC LAN environment. OEC LAN resources include data, information, software, hardware, facilities, and telecommunications. The policy is applicable to all those associated with the OEC LAN, including all OEC employees, vendors, and contractors utilizing the OEC LAN.

3.0 GOALS:

The goals of the OEC information security program are to ensure the integrity, availability and confidentiality of data which are sufficiently complete, accurate, and timely to meet the needs of OEC without sacrificing the underlying principles described in this policy statement.

Specifically the goals are as follows:

3.1 Ensure that the OEC LAN environment has appropriate security commensurate with sensitivity, criticality, etc

3.2 Ensure that security is cost-effective based on a cost versus risk ratio, or that is necessary to meet with applicable mandates;

3.3 Ensure that appropriate support for the security of data in each functional area is provided for;

3.4 Ensure individual accountability for data, information, and other computing resources to which individuals have access;

3.5 Ensure that the OEC LAN environment is as per audit requirement

3.6 Ensure that employees are provided sufficient guidance for the discharge of responsibilities regarding automated information security;

3.7 Ensure that all critical functions of the OEC LAN have appropriate contingency plans or disaster recovery plans to provide continuity of operation;

3.8 Ensure that all applicable department and organizational policies, mandates, etc. are applied and adhered to.

RESPONSIBILITIES:

The following groups are responsible for implementing and maintaining security goals set forth in this policy. Detailed responsibilities are presented in Responsibilities for Ensuring OEC LAN Security.

4.1 Functional Managers (FM) - those employees who have a program or functional responsibility (Not in the area of computer security) within OEC. Functional Manager is responsible for informing staff about this policy, assuring that each person has a copy, and interacting with each employee on security issues.

4.2 LAN Management Division (LM) - employees who are involved with the daily management and operations of the OEC LAN. They are responsible for ensuring the continued operation of the LAN. The LAN Management Division is responsible for implementing appropriate LAN security measures in order to comply with the OEC LAN security policy.

4.3 Local Administrators (LA) - employees who are responsible for ensuring that end users have access to needed LAN resources that reside on their respective servers. Local administrators are responsible for ensuring that the security of their respective servers is in accordance with the OEC LAN security policy.

4.4 End Users (U) - are any employees who have access to the OEC LAN. They are responsible for using the LAN in accordance with the LAN security policy. All users of data are responsible for complying with security policy established by those with the primary responsibility for the security of the data, and for reporting to management any suspected breach of security.

5.0 ENFORCEMENT:

The failure to comply with this policy may expose OEC information to the unacceptable risk of the loss of confidentiality, integrity or availability while stored, processed or transmitted on the OEC LAN. Violations of standards, procedures or guidelines in support of this policy will be brought to the attention of the management for action and could result in disciplinary action up to and including termination of employment.

6.0 GENERAL POLICIES OF THE LAN:

6.1 Every personal computer should have an "owner" or "system manager" who is responsible for the maintenance and security of the computer, and for following all policies and procedures associated with the use of the computer. The primary user of the computer may fill this role. These users should be trained and given guidance so that they can adequately follow all policies and procedures.

6.2 In order to prevent unauthorized access to LAN data, software, and other resources residing on a LAN server, all security mechanisms of the LAN server must be under the exclusive control of the local administrator and the relevant personnel of the LAN Management Division.

6.3 In order to prevent the spread of malicious software and to help enforce program license agreements, users must ensure that their software is properly licensed and safe.

6.4 All software changes and backups on the servers will be the responsibility of the LAN Management Division.

6.5 Each user must be assigned a unique USERID and initial password (or other identification information and authentication data), only after the proper documentation has been completed. Users must not share their assigned USER IDs.

6.6 Users must be authenticated to the LAN before accessing LAN resources.

6.7 USER IDs must be suspended after a consecutive period of non-use.

6.8 Use of LAN hardware such as traffic monitors/recorders and routers must be authorized and monitored by the LAN Management Division.

6.9 Employees responsible for the management, operations and use of the OEC LAN must receive training in computer security awareness and acceptable computer practices. Computer security training should be implemented into existing training programs such as orientation programs for new employees, and training courses involved with information technology systems equipment and software packages.

6.10 Security reports must be generated and reviewed on a daily basis.

7.0 SPECIFIC RESPONSIBILITIES FOR ENSURING OEC LAN SECURITY:

7.1 Functional Managers:

Functional managers (and higher-level management) are responsible for the development and implementation of effective security policies that reflect specific OEC LAN objectives. They are ultimately responsible for ensuring that information and communications security is, and remains, a highly visible and critical objective of day-to-day operations. Specifically functional managers are responsible for the following:

- 7.1.1 Responsible for implementing effective risk management in order to provide a basis for the formulation of a meaningful policy. Risk management requires identifying the assets to be protected, assessing the vulnerabilities, analyzing risk of exploitation, and implementing cost-effective safeguards.
- 7.1.2 Responsible for ensuring that each user is trained/made aware of the security policy at a minimum, though handover of a copy of the security policy and site handbook (if any) is desired prior to creating an account for the user.
- 7.1.3 Responsible for implementing a security awareness program for users to ensure knowledge of the site security policy and expected practices.
- 7.1.4 Responsible for ensuring that all personnel within the operating unit are made aware of this policy and responsible for incorporating it into computer security briefings and training programs.
- 7.1.5 Responsible for informing the local administrator and the LAN Management Division of the change in status of any employee who utilizes the OEC LAN. This status change includes an interagency position change, interdivision position change, or a termination from OEC employment.
- 7.1.6 Responsible for ensuring that users understand the nature of malicious software, how it is generally spread, and the technical controls to use for protection.

7.2 Local Area Network (LAN) Management Division:

The LAN Management Division (or designated personnel) is expected to enforce (to the extent possible) local security policies as they relate to technical controls in hardware and software, to archive critical programs and data, and to control access and protect LAN physical facilities. Specifically, LAN management is responsible for the following:

- 7.2.1 Responsible for rigorously applying available security mechanisms for enforcement of local security policies.
- 7.2.2 Responsible for advising management on the workability of the existing policies and any technical considerations that might lead to improved practices.
- 7.2.3 Responsible for securing the LAN environment within the site and interfaces to outside networks.
- 7.2.4 Responsible for responding to emergency events in a timely and effective manner.
  - 7.2.4.1 Notify local administrators if a penetration is in progress, assist other local administrators in responding to security violations.
  - 7.2.4.2 Cooperate with local administrators in locating violators and assist in enforcement efforts.
- 7.2.5 Responsible for employing generally approved and available auditing tools to aid in the detection of security violations.
- 7.2.6 Responsible for conducting timely audits of LAN server logs.
- 7.2.7 Responsible for remaining informed on outside policies and recommended practices as and when appropriate, informing local users and advising management of changes or new developments.

7.2.8 Responsible for judiciously exercising the extraordinary powers and privileges that are inherent in their duties. Privacy of users should always be a major consideration.

7.2.9 Responsible for developing appropriate procedures and issuing instructions for the prevention, detection, and removal of malicious software consistent with the guidelines contained herein.

7.2.10 Responsible for backing up all data and software on the LAN servers on a timely basis.

7.2.11 Responsible for identifying and recommending software packages for the detection and removal of malicious software.

7.2.12 Responsible for developing procedures that allow users to report computer viruses and other incidents and then responsible for notifying potentially affected parties of the possible threat.

7.2.13 Responsible for promptly notifying the appropriate security or incident response personnel of all computer security incidents including malicious software.

7.2.14 Responsible for providing assistance in determining the source of malicious software and the extent of contamination.

7.2.15 Responsible for providing assistance for the removal of malicious software.

7.2.16 Responsible for conducting periodic reviews to ensure that proper security procedures are followed, including those designed to protect against malicious software.

7.3 Local Administrators:

Local administrators (or designated personnel) are expected to utilize, on their assigned server, the available LAN security services and mechanisms to support and enforce applicable security policies and procedures. Specifically local administrators are responsible for the following:

7.3.1 Responsible for managing all users' access privileges to data, programs and functions.

7.3.2 Responsible for monitoring all security-related events and the following-up on any actual or suspected violations where appropriate. When appropriate, responsible for notifying and coordinating with the LAN Management Division the monitoring or investigation of security relevant events.

7.3.3 Responsible for maintaining and protecting LAN server software and relevant files using available security mechanisms and procedures.

7.3.4 Responsible for scanning the LAN server with anti-virus software at regular intervals to ensure that no virus becomes resident on the LAN server.

7.3.5 Responsible for assigning a unique USERID and initial password (or other identification information or authentication data) to each user only after proper documentation has been completed.

7.3.6 Responsible for promptly notifying the appropriate security or incident response personnel of all computer security incidents, including malicious software;

7.3.6.1 Notify the LAN Management Division if a penetration is in progress; assist other local administrators in responding to security violations.

7.3.6.2 Cooperate with other local administrators and the LAN Management Division in finding violators and assisting in enforcement efforts.

7.3.7 Responsible for providing assistance in determining the source of malicious software and the extent of contamination.

7.4 User:

Users are expected to be knowledgeable about and adhere to OEC Agency security policies, and other applicable laws, policies, mandates and procedures. Users are ultimately responsible for their own behaviour. Specifically users are responsible for the following:

7.4.1 Responsible for understanding and respecting relevant Federal laws, Department policies and procedures, OEC policies and procedures, and other applicable security policies and associated practices for the OEC LAN.

7.4.2 Responsible for employing available security mechanisms for protecting the confidentiality and integrity of their own information when required.

7.4.3 Follow site procedures for security of sensitive data as well as for the OEC LAN itself. Use file protection mechanisms to maintain appropriate file access control.

7.4.4 Select and maintain good passwords. Usage for guidance on good password selection. Do not write passwords down, or disclose them to others. Do not share accounts.

7.4.5 Responsible for advising others who fail to properly employ available security mechanisms and help to protect the property of other individuals. Notify them of resources (e.g. files, accounts) left unprotected.

7.4.6 Responsible for notifying the local administrator or management if a security violation or failure is observed or detected.

7.4.7 Responsible for not exploiting system weaknesses.

7.4.7.1 Do not intentionally modify, destroy, read or transfer information in an unauthorized manner: do not intentionally deny others authorized access to or use of LAN resources and information.

7.4.7.2 Provide the correct identity and authentication information when requested and not attempt to assume another party's identity.

7.4.8 Responsible for ensuring that backups of the data and software on their own workstation's fixed disk drive are performed.

7.4.9 Responsible for being familiar with how malicious software operates, methods by which it is introduced and spread, and the vulnerabilities that are exploited by malicious software and unauthorized users.

7.4.10 Responsible for knowing and utilizing appropriate policies and procedures for the prevention, detection, and removal of malicious software.

7.4.11 Responsible for knowing how to monitor specific systems and software to detect signs of abnormal activity, and what to do or whom to contact for more information.

7.4.12 Responsible for utilizing the technical controls that have been made available to protect systems from malicious software.

7.4.13 Responsible for knowing and utilizing contingency procedures for containing and recovering from potential incidents.

Ref: ISPOL-18 Workstation Policy

An unlocked workstation is a violation of security policy:

1. Please configure a password-protected screen saver to lock after 5 minutes of inactivity:
   1.1 Start > Settings > Control Panel > Display
   1.2 From the Display window, click on the Screen Saver tab
   1.3 From the screen saver drop down menu, choose a screen saver
   1.4 In the Wait window, choose 5 minutes
   1.5 Select "On resume, password protect" > Click OK

2. You should also lock your workstation before leaving your desk:
   Press Ctrl + Alt + Del > Click on "Lock Computer"

Both methods eliminate a period of vulnerability while the system is left unattended. The system can be unlocked by supplying your login ID and password.

3. When you leave for the day, log off your workstation. This would enable helpdesk to perform periodic inventory, maintenance and patch update activities.
4. In case, employee who needs to engage (unlock) their machines during non-office hours should send an email to techsupport@oecrecords.com stating reason for not logging off.
5. Never turn off your computer, unless instructed to do so.
6. The user should take the responsibility of his/her workstation that it should not contain any unwanted stuff/garbage data like, CD Dumps, Personal Photos, Literature, junk jpg files, mp3 files, video files. In case you find anything unusual report to helpdesk immediately. Helpdesk have rights to delete the above stuffs without prior notice.
7. Do not shift or change a location of the PC's. It should be done by admin group subject to approval from helpdesk.
8. User is not allowed to install, un-install and repair of any software. You should send an email request to techsupport@oecrecords.comwith prior approval from your project manager/leader.

Ref: ISPOL-19 Cryptographic Policy

1. When developing a cryptographic policy the following should be considered:
   - **3.1** The management approach towards the use of cryptographic controls across the Organization, including the general principles under which business information should be protected.
   - **3.2** Based on a risk assessment, the required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm required;
   - **3.3** The use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines;
   - **3.4** The approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;
   - **3.5** Roles and responsibilities, e.g. who is responsible for:
     - **3.5.1** The implementation of the policy;
     - **3.5.2** The key management, including key generation
   - **3.6** The standards to be adopted for the effective implementation throughout the organization\(Which solution is used for which business processes);
   - **3.7** The impact of using encrypted information on controls that rely upon content inspection e.g. virus detection.

2. Cryptographic controls can be used to achieve different security objectives, e.g.:
   - 2.1 Confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
   - 2.2 Integrity /authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
   - 2.3 Non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

Other information:

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A procedure on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. When using digital signatures, consideration should be given to any relevant legislation, in particular legislation describing the conditions under which a digital signature is legally binding. Specialist advice should be sought to identify the appropriate level of protection and to define suitable specifications that will provide the required protection and support the implementation of a secure key management system.

Key management Control:

Key management should be in place to support the organization's use of cryptographic techniques, implementation guidance. All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures, and secure methods for:

1. Generating keys for different cryptographic systems and different applications;
2. Generating and obtaining public key certificates;
3. Distributing keys to intended users, including how keys should be activated when received;
4. Storing keys, including how authorized users obtain access to keys;
5. Changing or updating keys including rules on when keys should be changed and how this will be done;
6. Dealing with compromised keys;
7. Revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);
8. Recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;
    8.1 Archiving keys, e.g. for information archived or backed up;
    8.2 Destroying keys;
9. Logging and auditing of key management related activities. In order to reduce the likelihood of compromise, activation, and deactivation dates for keys should be. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust. The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

Other information:

1. Secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information; this key has to be kept secret since anyone having access to the key is able to decrypt all information being encrypted with that key, or to introduce unauthorized information using the key;
2. Public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret); public key techniques can be used for encryption and to produce digital signatures.

There is a threat of forging a digital signature by replacing a user's public key. This problem is addressed by the use of a public key certificate. Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

Ref: ISPOL-20 OEC Infrastructure Policy

1.0 Overview:

OEC's intentions for publishing an Infrastructure Policy are not to impose restrictions that are contrary to OEC Established culture of openness, trust and integrity. OEC is committed to protecting OEC's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing, and FTP, are the property of OEC. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every OEC employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at OEC. These rules are in place to protect the employee and OEC. Inappropriate use exposes OEC to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope:

This policy applies to employees, contractors, consultants, temporaries, and other workers at OEC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by OEC.

4.0 Policy:

4.0.1 General Use and Ownership:

4.0.1.1 While OEC's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of OEC. Because of the need to protect OEC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to OEC.

4.0.1.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.0.1.3 For security and network maintenance purposes, authorized individuals within OEC may monitor equipment, systems and network traffic at any time, per OEC's Audit Policy.

4.0.1.4 OEC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.0.1.5 IP Messenger is the only program allowed for the official internal communication and no other messaging programs e.g.: yahoo messenger, AOL etc.

4.0.1.6 Image Editing application like MS-paint will be used as it is our business requirement.

4.0.1.7 Any kind of large printouts (>10 pages) should not be printed without prior permission by PM/Team Leads. Take printouts only when absolutely necessary and maintain register.

4.0.2 Security and Proprietary Information:

4.0.2.1 The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

4.0.2.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords should be changed every 45 days. If you have not changed your login password yet, please change it immediately. "**Press Ctrl Alt Del key and Change Password."**

4.0.2.3 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging-off(control-alt-delete for Windows users)

4.0.2.4 Personal Laptop is strictly prohibited in the premise. Please do not try to connect laptop, Bluetooth, pen drive or any electronic device to this network. The Employee should not carry external media like floppies, CD/DVD's in the Premise.

4.0.2.5 All hosts used by the employee that are connected to the OEC Internet/Intranet/Extranet shall be continually executing approved virus- scanning software with a current virus database. Unless overridden by departmental or group Policy.

4.0.2.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.0.2.7 All users must Log off before they leave the office. If there is a reason as to why they must stay logged in, then the person MUST keep up an away message explaining why they should not be logged out

4.0.2.8 By any reason DO NOT

a) Try to change computer name
b) Shifting exchange of computers
c) Loading or installation of software's

4.0.2.9 All kind of hardware and software requests should be email to techsupport@oecrecords.com

4.0.2.10 Any kind of unwanted files /garbage data like, CD Dumps, Personal Photos, literature, study materials, unwanted jpg files,mp3 files, video files, installable tools found on the workstation/server/emails will be deleted without notice and the user will be excluded from the backup list.

4.0.2.11 The home folder (H :) is available in an explorer; you should keep your important data in home folder more security and safety.

4.0.2.12 Email signature format should be same as per company format.

4.0.2.13 Please do not put shutter/any object in front of projector while it is in running state, doing so the bulb will get fused which is a very expensive component of the projector. Also, use the projector when more than three people are involved in Conference. Do not forget to power off the projector once your conference gets over.

4.0.3 Unacceptable Use:

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of OEC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing OEC-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.0.3.1 **System and Network Activities:**

The following activities are strictly prohibited, with no exceptions:

4.0.3.1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that aren't appropriately licensed for use by OEC.

4.0.3.1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which OEC or the end user does not have an active license is strictly prohibited.

4.0.3.1.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.0.3.1.4 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.0.3.1.5 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.0.3.1.6 Using an OEC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.0.3.1.7 Making fraudulent offers of products, items, or services originating from any OEC account.

4.0.3.1.8 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.0.3.1.9 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.0.3.1.10 Port scanning or security scanning is expressly prohibited unless prior notification to OEC is made.

4.0.3.1.11 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

4.0.3.1.12 Circumventing user authentication or security of any host, network or account.

4.0.3.1.13 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.0.3.1.14 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.0.3.1.15 Providing information about, or lists of, OEC employees to parties outside OEC.

4.0.3.2 **Email and Communications Activities:**

4.0.3.2.1 Do not send/receive non business personal emails from OEC account.

4.0.3.2.2 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.0.3.2.3 Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4.0.3.2.4 Unauthorized use, or forging, of email header information.

4.0.3.2.5 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.0.3.2.6 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.0.3.2.7 Use of unsolicited email originating from within OEC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by OEC or connected via OEC's network.

4.0.3.2.8 Posting the same or similar non-business-related messages to large numbers of Usenet news groups (newsgroup spam). Sending mass or group emails is strictly reserved for Admin & HR only. If you want to circulate message to a group, please contact these persons.

4.0.3.2.9 Sending mass/group emails are only permitted for PM/HR/Admin/OPS/IT.

5.0 Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Ref: ISPOL-21 Coding Standards

1. Use Option Explicit
2. Do not use option base
3. Declare variables and constants at the top of the procedure. Don't put anywhere in the procedure even though it is allowed.
4. Don't declare variable with variant type.
5. Don't use an object type when the true type of the object is known.
6. Declare error handling in very procedure.
7. Use common error trapping label names.
8. Use debug. Print statements for immediate results.
9. Keep module to manageable size. Each modules should be less than 1000 lines
10. Don't put general procedure in form modules. Form module should contain only the event procedure of form.
11. Make practice of putting comments on each procedure for easy understand.
12. Avoid line longer than 80 characters.
13. Write comment block at the top of each module. This name of module, description.
14. Begin each procedure with comment block.
15. Declare variable with comment.
16. Module name and procedure name should be meaningful words or phrases that describe the abstraction of the module. Use nouns for object abstractions and verbs for functional abstractions. Modules names should be without spaces, in mixed case, with the first letter uppercase, and the first letter of each subsequent word capitalized. The file name of the module should match the internal name of the module.
17. Variable and parameter names should be meaningful noun or noun phrases, without spaces, with the first letter lowercase and the first letter of any subsequent words capitalized. The first few letters of the variables name define the type of the variable. The remainder of the name should describe the role that the variable plays.
18. Global variables should have prefix "g_" before the name of the variable.
19. Module level variables should have prefix "m_" before the name of the variable.

Ref: ISPOL-21 Source Code Password Policy

Overview:
All personnel that have access to source code must adhere to the password policies defined below in order to protect the source code of the co.

Purpose:
The purpose of the policy is to establish a standard for creation of strong password, the protection of that password, and the frequency of change.

Scope:
This policy applies to any and all personnel who have access to the source code.

Password Protection:

1. Never writes down the passwords
2. Never send password through email
3. Never tell password to anybody
4. Never reveal password over the telephone
5. Never use company network and corporate password.
6. Please refer Manager –Software for creation of new account.
7. Be careful about letting someone see you type your password
8. Passwords are case sensitive and the user name or login Id is not case sensitive.

Enforcement:
Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

Other considerations:
Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

Ref: ISPOL-22 Email Policy

The purpose of this policy is to ensure the proper use of OEC's email system and make users aware of what OEC deems as acceptable and unacceptable use of its email system. OEC reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

All emails will follow the following nomenclature :

1. firstname.lastname@oecrecords.com
2. In case there are 2 persons with the same first and last name, then the same will be suffixed with 1, 2, 3 & so on.

Hosting: As OEC is not an email service provider, the service will be licensed from a third party service, the third party will have to adhere to all IT policies of OEC.

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail:

1. If you send emails with any libellous, defamatory, offensive, racist or obscene remarks, you and OEC can be held liable.
2. If you forward emails with any libellous, defamatory, offensive, racist or obscene remarks, you and OEC can be held liable.
3. If you unlawfully forward confidential information, you and OEC can be held liable.
4. If you unlawfully forward or copy messages without permission, you and OEC can be held liable for copyright infringement.
5. If you send an attachment that contains a virus, you and OEC can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and OEC will disassociate itself from the user as far as legally possible.

The following rules are required by law and are to be strictly adhered to:

1. It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.
2. Do not forward a message without acquiring permission from the sender first.
3. Do not send unsolicited email messages.
4. Do not forge or attempt to forge email messages.
5. Do not send email messages using another person's email account.
6. Do not copy a message or attachment belonging to another user without permission of the originator.
7. Do not disguise or attempt to disguise your identity when sending mail.

OEC considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service.
Therefore OEC wishes users to adhere to the following guidelines:

1. Writing emails:
   1.1 Write well-structured emails and use short, descriptive subjects.
   1.2 OEC's email style is informal. This means that sentences can be short and to the point. You can start your e-mail with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards' or 'With Regards'. The use of Internet abbreviations and characters such as smiley, however, is not encouraged.

1.3 Signatures must include your name, job title and company name. A disclaimer will be added underneath your signature (see Disclaimer). (Signature must include your First Name & Last Name, Designation & Company Name, Mobile & Telephone Number)

1.4 Signature must have as per company standard .e.g

With Regards,	[font Name: Calibri, Font Size: 11, Color: Black]
Name | Designation	[font Name: Calibri only Name in bold, Font Size: 11, Color: Black]
OEC Records Management Co Pvt Ltd	[font Name: Calibri with bold, Font Size: 11, Color: RGB Decimal Value: 0, 125,190 [Code:#007DBE])
Tel: 0000000000 | Mob: 00000000000	[font Name: Calibri, Font Size: 11]

1.5 Use the spell checker before you send out an email.

1.6 Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.

1.7 Do not write emails in capitals.

1.8 Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.

1.9 If you forward mails, state clearly what action you expect the recipient to take.

1.10 Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).

1.11 Only mark emails as important if they really are important.

2 Replying to emails:

2.1 Emails should be answered within at least 2 working hours, but users must endeavour to answer priority emails within 1 hour.

2.2 Priority emails are emails from existing customers and business partners.

2.3 Auto revert facility to be activated if user is not expected to be on their desk for the day so the sender should know who to get in touch with in absence of the recipient.

3 Newsgroups: Users need to request permission from their supervisor before subscribing to a newsletter or news group.

4 Maintenance: Delete any email messages that you do not need to have a copy of, and set your mail client to automatically empty your 'deleted items' on closing.

Disclaimer:

The following disclaimer will be added to each outgoing email:

This message is confidential and is intended only for the use of the individual to whom it is addressed. If you have erroneously received this message, please immediately delete it and notify the sender. Also, if you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this message or any accompanying document is strictly prohibited and is unlawful. Internet communications cannot be guaranteed to be timely, secure, error or virus-free. OEC accept no responsibility for any loss or damage arising from the use of this email message or its attachment(s).

Although OEC's email system is meant for business use, OEC allows the reasonable use of email for personal use if certain guidelines are adhered to:

1 Personal use of email should not interfere with work.
2 Personal emails must also adhere to the guidelines in this policy.
3 Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be deleted weekly so as not to clog up the system.
4 The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
5 On average, users are not allowed to send more than 2 personal emails a day.
6 Do not send mass mailings.
7 All messages distributed via the company's email system, even personal emails, are OEC's property.

Avoid sending confidential information by e-mail. If you do, you must secure the information by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone.

You must have no expectation of privacy in anything you create, store, send or receive on the company's computer system. Your emails can be monitored without prior notification if OEC deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the OEC reserves the right to take disciplinary action, including termination and/or legal action.

All email accounts maintained on our email systems are property of OEC. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.

Ref: ISPOL-23 Password Security Policy

All the privileged ids passwords are sealed in an envelope and handed over to Senior Management.

Whenever a password of privileged id is changed, the corresponding sealed is replaced.

For retrieving the passwords in emergency situations these sealed envelopes will be opened after taking written permission of the Department Head Technology

Any part of Logon name cannot be used as password. Employees are instructed not store or transmit password in clear text or in any easily reversible form.

Default passwords are changed after first login. If an account or password is suspected to have been compromised, employee reports the incident to IT department which post enquiry changes the password immediately.

The user shall immediately change the password on first logon.

Wherever feasible the system should ensure the change of password on the first logon.

Ref: ISPOL-24 Security Incident Management Policy

The Incident Management Policy is intended to communicate what is expected of personnel when confronted with an incident pertaining to information resource confidentiality, integrity, and/or availability.
The policy provides the vital framework necessary to develop incident response procedures.

Types of Incidents:

1. Data hack
2. Hardware Failure
3. Software Failures
4. Natural Disaster

Data Hack:
As per company policy 3 levels of data hack have been defined

- Malicious script/Virus
- Data Stolen
- System Down

Malicious script/viruses are dealt with up to date software which is built deployed across systems.
Data Stolen – Data is cross referenced on a daily basis using logs, if data files are missing, the same is reported to the cyber-crime department and necessary action is taken.

If the System is brought down by an external threat, the same is rebooted immediately, refer to backup policy as required. In parallel the cyber-crime team is involved to assess the situation and action as required

Hardware Failure:
Servers to be procured refer to procurement policy, backup devices basis the last 24 hours to be used to deploy new instance on the server.

Software Failure:
Evaluate failure basis OS or Critical software, if OS is corrupt then re-install using the key assign to the OS of particular machine, in case of software failure branch head to inform system admin and redeployment of software to happen – data loss avoided basis all data feed captured on the DB server.

Natural Disaster:
IT Head and Manager's evaluate nature of damage and implement procurement and restoration of data – refer to backup policy basis the same

Level 1	Level 2	Level 3	Level 4
Compromised System Compromised User Credentials Individual Virus and Malware Phishing Software Error	Multiple system Failures Multiple Virus and Malware Attacks UPS Failure Software not accessible	Network Attacks SVN Data Loss Software not accessible	Lost Equipment/Theft Physical Break-in Software Corrupt Natural Disaster

Level 1	Level 2	Level 3	Level 4
2-8 Hours	1-2 Days	4-6 Days	6.10 Days
			6.11

- Employees and contract employees Document security incidents via email or call
- IT dept makes an initial assessment.
- Communicate the incident as per escalation matrix
- IT dept contains the damage and minimizes the risk.
- IT dept Identify the type and severity of the compromise.
- IT dept stores evidence; logs/reports
- Notify external agencies if appropriate.
- Recover systems.
- IT dept compiles and organizes incident documentation.
- IT dept assesses incident damage and cost.
- Review the response and update policies.

Level 1	Junior Programmer/Jr. Sys Admin
Level 2	Manager Infra / Manger Software
Level 3	VP IT
Level 4	Board

1. Employees and contract employees documents IT security incidents via email
2. Employees and contract employees send notifications to unit IT workers identifying the type of incident
3. IT dept acknowledges the notification
4. IT dept contain the incident as soon as possible
5. IT dept investigates and update the tracking system
6. IT dept determines incident severity
7. IT dept reviews incidents in the tracking system and closes request via mail.

Ref: ISPOL-25 Owners and Custodians Policy

To provide a clear definition of responsibility for the management of information that will ensure that access to information is both controlled and authorized.

1. **Information Owner: Directors, HODs**
   1.1 Information Owners will be Management, HODs and Branch managers, who have been given the authority to collect, create, retain and maintain information and information systems within their assigned area of control. The Information Owner may delegate some operational responsibilities, but will retain accountability

2 **Information Custodian: Sys Admin**
   2.1 Information Custodians are those individuals who control information systems regardless of physical or logical location, storage medium, technology used, in the case of OEC these are Management, HODs and Branch Managers.

   2.2 The Information Custodian will be responsible for the administration of controls as specified by the Management.

3. **Information User: Supervisors and below**
   3.1 Information Users are individuals who have been granted explicit authorization by the relevant HODs &Branch heads to access, alter, destroy, or use information within OEC. An Information User will be responsible for: using the information only for the purpose intended by the company; complying with all controls established by the owner and custodian; ensuring that classified or sensitive information is not disclosed to anyone without permission of the owner.

Ref: ISPOL-26 Data Privacy and Classification Policy

Data Privacy and Classification Policy is to provide a system for protecting information that is critical to the organization, and its customers. In order to provide more appropriate levels of protection to the information assets entrusted to OEC, data must be classified according to the risks associated with its storage, processing, and transmission. Consistent use of this data classification policy will facilitate more efficient business activities.

Data Privacy and Classification Policy apply equally to any individual, or process that interacts with OEC Information Resources in any tangible manner. All personnel who may come in contact with confidential information are expected to familiarize themselves with this Data Classification Policy and consistently use it.

1. Classifications:

Three types of classification followed by OEC

1.1 Confidential:

Confidential Data is information protected organizational policies or contractual language. Confidential Data is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis only.

Disclosure to parties outside of the organization must be authorized by executive management, approved by a Technology Head, or covered by a binding confidentiality agreement. Examples of Confidential Data include:

1. Medical records
2. Credit card numbers
3. Personnel and/or payroll records
4. Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction

OEC HOD and above have access to confidential data, this is further segregated via departments example, Customer Service, Logistics etc

1.2 Internal:

Internal Data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. Internal Data is information that is restricted to personnel designated by OEC who have a legitimate business purpose for accessing such data.

Examples of Internal Data include:

1. Employment data
2. Business partner information where no more restrictive confidentiality agreement exists
3. Internal directories and organization charts
4. Planning documents
5. Contracts

1.3 Public:

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to organizational disclosure rules, is available to all OEC employees and all individuals or entities external to the corporation.

Examples of Public Data include:

1.3.1.1 Publicly sent emails

1.3.1.2 Publicly available marketing materials

2. Publicly posted job announcements
Disclosure of public data must not violate any pre-existing, signed non-disclosure agreements

3. Data Type:

3.1 Restricted Data:

Restricted data is the most sensitive information and requires the highest level of protection. This information is usually described as "non-public information" about people and under the purview of a Data Custodian.

OEC – Personnel responsible for the same
Directors
Head Technology
HOD

3.2 Sensitive Data:

Sensitive data is information that business units may decide to share with other units outside their administrative control for the purpose of collaboration. This information is not information that meets the requirements of "non-pubic" information. Examples include data created by the department, research data, and project data.

3.3 Public Data:

Most OEC information is suitable for public dissemination and is accessible to anyone in the world. Examples include public web pages, services, press releases, marketing brochures, etc. While the requirements for protection of public data are less than that of Restricted and Sensitive, sufficient controls must be maintained to protect unauthorized modification of data.

Employee Classification and Access:

Currently data classification is done via bands. Following is an overview basis the same:

- Confidential and Restricted: Directors
- Confidential: HOD
- Sensitive: Branch Managers
- Public: Anyone below Branch Manager

Ref: ISPOL-27 Data Purging Policy

Data Purging Policy is to safeguard information that is critical to the organization, and its customers. In order to provide more appropriate levels of protection to the information assets entrusted to OEC, data must be classified according to the risks associated with its storage, processing, and transmission. Consistent use of this data purging policy will facilitate more efficient business activities.

1. **Scanned images:**

   All client's data / document which is being scanned & converted into images should not be saved in any of local / shared / Network folders beyond the agreed number of days with the respective client. In the absence of any such agreement with the client, by default the frequency for data purging of scanned images will be 7 days.

2. **Scanned images on Android / Hand held devices:**

   All client's data / document which is being scanned from Android / Handheld devices should be purged once the images are successfully transferred and the task is completed.
   Frequency for data purging of scanned images on Android / Hand held Devices will be two days

3. **Scanned Imaged Email attachments:**

   Customer data (All scanned Images) should be encrypted / compressed with password protected before sending through email as attachments, once the email has been send to the customer, all the scanned imaged email attachments should be purged as per the agreed number of days with the respective client. In the absence of any such agreement with the client, by default the frequency for data purging of scanned images will be 7 days.

Ref: ISPOL-28 Log collection and Retention Policy

Establish and control the records that provide evidence for analyze usage pattern and diagnose system.

1. **Collection of Logs:**
   OEC should enable log collection services on all applications including Operating Systems log, application logs, firewall logs, CCTV logs, biometric logs etc. Before reach to maximum size OEC should archive the logs and remove the logs manually.

2. **Retention Logs:**
   OEC is responsible for keeping the logs for a period minimum of 8 years also subject to client's requirements and its legal commitment. During the retention period, data can only be available to clients on a written request which should be further approved by VP IT.

3. **Use of logs**
   Logs can be used to investigate any suspicious / fraudulent activity and / or client's requirements.

Ref: ISPOL-29 Change Management Policy

Purpose:

Monitor and initiate changes across OEC basis Software & IT-Infrastructure. Define as anything—hardware, software, system components, services, documents, or processes—that is deliberately introduced into the production environment and which may affect a service level agreement (SLA) or otherwise affect the functioning of the environment or one of its components

Scope:

Workflow:

Design and Implementation Requirements: After Initial Approval specific requirements for the change to be successfully implemented are completed. The Design and Implementation process includes a complete Impact Analysis and Risk Assessment basis current OEC requirement. The Change is classified as High, Medium, or Low impact. To arrive at this assessment we identify who and what will be potentially affected by the change including Departments, systems, configuration items, procedures, costs, schedules, and resources.

Test Plan Development: This phase focuses on developing the plan for conducting testing and quality assurance to ensure reliability and performance of all components of the organization's technology infrastructure.

Approval Matrix:

Approval Type	Personnel	Description
Level 1	Tech Support	Mail Ids, Deletion of backup files, updating machines, relocation of machines
Level 2	Manager IT Infra /Manager – Software	Changes to database, changes in the software cycle, backup changes,
Level 3	Manager – IT Infra, Manager – Software, VP-IT	Procurement basis software and Hardware, Updates to existing software, development of modules, changes to network

Implementation:

Request for change:

A request for change can be initiated from a Service Call, Request for Service via email. The change may be initiated by a staff member or a client. Request is determined to be either In Scope or Out of Scope for Change Management. The scope evaluation is done by a joint meeting between concerned personnel from the respective department and Tech If it is within scope, change initiation continues through the process

Preliminary Planning and Requirements Analysis:

Preliminary information regarding the change is gathered. This includes describing the change and its objectives, identifying the benefits to the customer and internal teams, and identifying the systems and the type of change. Sys Admin and Senior Programmer are responsible for the same.

Impact Analysis and Risk Assessment:

An initial impact and risk analysis is conducted to determine who and what may be affected and the degree of impact. An assessment of impact for not doing the change is also included. VP Tech is responsible for the same

Review and Approval:
The change request is reviewed by the tech team depending upon the impact classification and scope of the change. Approval is granted/denied by VP Tech and auctioned as required

In scope:
The primary functional components covered in the Change Management process include:

- Changes handled through the formal or informal software development life cycle.
- Installation, modification, removal or relocation of computing equipment of medium or high.
- Installation, patching, upgrade or removal of software products including operating systems and access
- Database – Changes to databases or files such as additions, reorganizations and major maintenance.
- Application – Application changes being moved to production as well as the integration of new application systems and the removal of obsolete elements.
- MACs – Moves, Adds, Changes and Deletes to system configuration.
- Schedule Changes: Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the I.S. Department.
- Desktop – Any medium or high impact modification or relocation of desktop equipment and services.
- Generic and Miscellaneous Changes: Any medium or high impact changes that are required to complete tasks associated with normal job requirements, i.e. cabling, environmental changes, etc.

Out of Scope:
Changes made within the daily administrative process. Examples of daily administrative tasks are:

- Password resets
- User adds/deletes
- User modifications
- Adding, deleting or revising security groups
- Rebooting workstations when there is no change to the configuration of the system
- File permission changes
- Desktop telephony moves, adds, changes

Change Type:
Hardware changes:
Additions, deletions, reconfigurations, relocations, or preventative or emergency maintenance

Software:
Product releases, versions, table changes, tuning, alterations to libraries, catalogs, monitors, service packs, security patches, configuration changes, and new installations.

Network Systems:
Additions, modifications, lines, modems routers, network access, controllers, servers, protocol converters. Software components either distributed or centralized, tables, router software, servers.

Operating Procedures:
Changes in equipment downtime schedules, planned system outages, changes in delivering services, or changes to service levels.

Workstations and Public Clusters:
Changes in hours of availability, hardware configurations, operating systems, utilities, applications including versions, installations or de-installations of systems, servers

Change Classification Methods:
Changes at OEC are classified basis the Normal Changes & Emergency Changes:

Normal Changes:
Change request sent into IT have to be approved by the department head and then by VP Tech, if procurement is required then Admin is involved basis negotiation on a case to case basis, all normal changes have a turnaround time, this basis type of request – Daily operations request will be considered in the same

Emergency Changes:
These changes require from VP tech only. The change can be a solution or a stop gap. Once the change is made, the log is presented into management to ensure the change is signed off as required. Emergency tech budgets are handled via emergency budget allocations which have been assigned to the VP Tech – System, Network and Product failures resulting in stoppage of work will be treated as emergency changes.

Tracking:
All changes will be tracked using a tracker at OEC the same is an XL sheet, Senior Programmers, Sys Admin, Infra Manager Tech and VP Tech have access to the same

Change Communication:
Communication to process to employees via email broadcast via Tech Support and HR department

Ref: ISPOL-30 User Access Management Policy

PURPOSE:

The purpose of this policy is to prevent unauthorised access to OEC IT-Infrastructure information systems. The policy describes the registration and de-registration process for all information systems and services to ensure that only authorized users have access to information systems.

SCOPE:

In accordance with the ISO 27001: 2013, formal procedures should be in place to control the allocation of access rights to information systems and services.
The procedures developed to support this standard will cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. In addition, the procedures, where appropriate, will address the need to control the allocation of privileged access rights, which will allow users to override system controls.

DESCRIPTION OF ACTIVITIES

1. User registration :

1.1 New Users

Access to OEC IT-Infrastructure information systems is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out (i.e. Training).

There is a standard level of access (Tobas, Email, files & folders and database), other services can be accessed when specifically authorised by HR/line management.
A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR.

The request is free format, but must state:

- Name of person making request
- Job title of the newcomers and workgroup
- Start date
- Services required (default services are: Windows login, Tobas login, Email and Internet access)

Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure.

The user signs the form indicating that they understand the conditions of access. Access to all systems is provided by IT and can only be started after proper procedures are completed.

A new user will be set up on receipt of written notification but not made available, by issue of password, until the individual's start date.IT will maintain a record of all requests in a folder named "new users" in the Helpdesk, mailbox and will file email paper copies in the user access file.

a. **Change of user requirements**

Changed requirements will normally relate to an alteration to the applications used but may also involve network access. Requests must be in writing (e-mail or hard copy) and must be directed to the Helpdesk.

Changes will be made on receipt of a properly completed request, the same details as shown above are required and requests will be filed under "access change requests" in the Helpdesk.

b. **Change of password**

Where a user has forgotten his/her password, the helpdesk is authorised to issue a replacement.
Upon receipt of such a request the Helpdesk will

1. Ensure the request is logged.
2. Confirm the identity of the user by question about existing services/access or by reference to a work colleague
3. Issue a temporary, single use, password which will require the user to set up a formal password.

2. User De-registration :

As soon as an individual leaves the organisation, all his/her system logons will be revoked.

As part of the employee termination process, HR (or line managers in the case of contractors) will inform IT Tech Team of all leavers and their date of leaving.

All notification will be filed & updated in a file called "ID Creation_Deletion Form V 2 1".

Additionally, IT Tech Team will positively confirm leavers with HR; IT tech team will deactivate all network access for all leavers on leaving date & block the email id, passwords will change & auto forwarding rules will be set to his id for one month. Old user ID's are removed and will not be re-issued.

The organisation expects all leavers to hand over current files within their workgroup; however IT Tech Team can move a leavers files to specific areas if requested. Normally a leaver's data will be left in its existing directory for one month and then archived off system (but can be recovered if required).

3. User Access Provisioning:

A user role, also termed a business role or positional role, is used to represent a group of users with a particular meaning in a business model, such as a classification of users who share a business function.

User roles can be modelled with an organizational role and used to support role-based provisioning. A user role can be mapped to a set of access entitlements in the provisioning policy so that the access to IT resources is automatically provisioned for the users that belong to the role.

User roles are often modelled to help with user management for the business, and user roles can also be used to support role-based access control and role-based provisioning. Access to IT resources might be managed by the following systems:

Central access control system:
A role-based access control model grants access to resources based on a user role, such as the user's job title or work responsibility.

Distributed system for a specific resource
A role-based provisioning model automates the access entitlement provisioning process for a specific managed resource, based on the roles to which the user belongs.

We have considered the following items while designing provisioning policies:

- The target services to manage
- The number of groups on each service
- The number of user roles in the organization
- The pattern of user roles and access entitlement mappings to the target services.

An access entitlement can be simply mapped to an account on a service or to specific group members on a service. A provisioning policy allows a user role to map to multiple entitlements for different services, and it allows multiple roles to have the same set of access entitlements. On the other hand, it is also possible to have multiple provisioning policies for the same role, each granting a set of accesses for the role.

An organizational role in Active Directory is used to represent access to IT resources. The access can be mapped to one or multiple services that represent aggregated access to the resources.

This type of organizational role can be directly exposed to the user for access requests, and can be categorized based on its access type, such as access to an application or a shared folder.

4. Privilege Access Rights :

"Special privileges" are those allowed to the system manager or systems programmers, allowing access to sensitive area (for example, passwords). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached

Privileged access must be authorised by the VP of IT Dept, using the request form shown in Ref Appendix A-2. All requests for access outside normal services must be supported by a completed and authorised Privilege Access form Ref Appendix A-2.

The IT Head of organisation will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the Audit Team on a three monthly basis. The list will identify all separate logons for each system and service.

5. Review of user access rights:

The IT team will review all of network access rights at least six month basis, which is designed to positively confirm all users. Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed.

Annually, the IT Team will review all access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. All other logons will be deleted.

The review will be conducted as follows:

- The IT team will generate a list of users, by application.
- The appropriate list will be sent to each Application owner who will be asked to confirm that all users identified are authorised to use the system.
- The IT team will ensure a response.
- Any user not confirmed will have his/her access to the system removed.
- The IT Team will maintain a file of -
    - Lists sent over
    - Application owner responses
    - A record of action taken
    - The review will normally be conducted in periodic basis (Monthly Review)

Ref: ISPOL-31 System & Application Access Control Policy

PURPOSE:

The purpose of this policy is to prevent unauthorised access to system & application information systems. The policy describes the access control process for all information systems and services.

SCOPE:

In accordance with the ISO 27001: 2013, formal procedures should be in place to control the access rights to information systems and services to prevent unauthorized access to systems and applications. It is applicable to all systems and applications where applications meant for OEC are hosted.

DESCRIPTION OF ACTIVITIES

Information access restriction:

All applications developed in house which contain information, have incorporated a uniform access control mechanism, which provides users with the required level of access. Additional privileges are given based on proper authorization from the information owner.

Secure log- on procedures:

All user machines are accessible through a user name and password. These are assigned to each authorized user and are unique in nature. Unauthorized access is not permitted.

Password management system:

This has been well defined in our password policy and kindly Refer to 'Ref: ISPOL-09 Password Policy'

Use of privileged utility programs:

All system utility programs, which impact the operations of the systems, are installed with controlled access to administrative accounts. Use of system utilities is controlled & maintained via our standard Software Installation Policy, Kindly refer to Information Security Procedure

'Ref: ISPOL-07 Desktop Computer and Laptop Installation'

Access control to program source code

Only the project development team has access to the program source code in the project.
Kindly refer to our Information security Policy 'Ref: ISPOL-21 Source Code Password Policy'

Ref: ISPOL-32 Information Processing Facilities Policy

Users of Organization information processing facilities will utilize these facilities for only management-authorized business purposes. Organization reserves the right to legally monitor facilities for compliance. The purpose of this policy is to protect the availability and integrity of the organization's information processing facilities as well as protect the organization against legal sanction against the misuse of assests /data / information's etc...

The IT Head Officer shall provide managers with guidelines for the legal monitoring of computer facilities. Managers of information processing facilities shall monitor the use of such facilities.

If misuse is detected, it shall be brought to the attention of the person's manager for disciplinary action.

An acceptable use policy will be communicated to users. This policy will be included in the acceptance of policy letter that employees will sign during orientation. The acceptable use policy will govern permitted and forbidden activities for their location. In all cases, any activity not expressly permitted is forbidden.

At logon, a message shall appear to warn users that they are entering a private system and that unauthorized access is not permitted.

Ref: ISPOL-33 Intellectual Property Rights Policy

All users will comply with the legal aspects of intellectual property protection and the rights and limitations of license agreements associated with proprietary software products.

The purpose of the policy is to ensure that users are aware of and comply with such restrictions as copyrights, trademarks, and design rights. Users are responsible for not violating applicable copyright, intellectual property, or other licensing rights of electronic media or software that is not the property of organisation. Furthermore, users are responsible for not using organisation intellectual property outside the limits of company policy or licensing.

Failure to abide by these policies will subject the user to disciplinary actions up to and including termination or criminal/civil charges.

Intellectual Property Standards and Training:

IT will publish the organization's standards for software acquisition (see Ref: ISPOL 20).

Intellectual Property Rights Protection policies shall be included in all security awareness training (see Ref: ISPOL 15).

The Chief IT Officer shall establish, document and educate applicable users on:

- Maintaining appropriate asset registries
- Maintaining proof of ownership or licenses
- Implementing controls to restrict the amount of users to the appropriate licensed amount
- Implementing controls and checks to ensure that only licensed software is installed
- Policies and controls to assure that license conditions are met
- Policies and controls for disposing of or transferring software to others
- Use of appropriate audit tools

Using Software from Outside Sources:

IT will publish the organization's policies and procedures for obtaining software from public networks.

Users will not download or install any third party pirated software on Organisation systems.

Users will not download or install any non-approved software from the Internet. The IT Head Officer will approve specific software for use from the Internet if there is a business need.

Copyrighted Material and Peer-To-Peer File Sharing at Organization

Organization respects the copyrights of those involved in creating and distributing copyrighted material, including music, movies, software and other literary and artistic works. It is the policy of Organization to fully comply with all copyright laws.

Organization provides its employees access to computer systems and the Internet to allow them to do their jobs on behalf of Organisation. Employees may make occasional use of the Company's computer systems and network for personal use.

When Organization employees need to use copyrighted materials to do their jobs, Organisation acquires appropriate licenses.

Organization employees may not:

- store or otherwise make unauthorized copies of copyrighted material on or using Organization computer systems, networks or storage media;
- download, upload, transmit, make available or otherwise distribute copyrighted material using Organization computer systems, networks or storage media without authorization; or
- use or operate any unlicensed peer-to-peer file transfer service using Organization's computer systems or networks or take other actions likely to promote or lead to copyright infringement.

Please note – this is not a policy against MP3 files, or electronic music and video files as such. Rather, the policy is targeted at unauthorized – that is, unlicensed – electronic music and video files. If you downloaded the files from an unlicensed peer-to-peer site (i.e., Morpheus, Grokster, KaZaA, etc.) or other source, then those files are almost certainly not authorized and most likely violate the copyright laws.

Organization reserves the right to:

- Monitor its computer systems, networks and storage media for compliance with this and other Company policies at any time, without notice and with or without cause; and Delete from its computer systems and storage media, or restrict access to, any unauthorized copies of copyrighted materials it may find, at any time and with or without notice.

Ref: ISPOL-34 Outsourced Development

OBJECTIVE

To specify controls to reduce the information security risks associated with outsourcing.

SCOPE

The policy applies to all in the organisation namely outsource providers including hardware and software support and maintenance staff, external consultant and contractors, IT or business process outsourcing firms and temporary staff.

RESPONSIBILITY

The system development team is responsible for monitoring and supervising the activity of outsourced software development.

Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

POLICY STATEMENTS

1. Choosing an outsourcing Partner

1.1. Criteria for selecting an outsourcing Partner shall be defined and documented by taking following points:

- Company's reputation and history
- Quality of services provided to other customers
- Number and competence of staff and managers
- Financial stability of the company and commercial record.

2. Assessing outsourcing risks

2.1. The software development team is the owner for each business functions/processes outsourced. The owner shall assess the risks before the functions/processes are outsourced

2.2. In relation to outsourcing, the owner shall take due account of the sensitivity, volume and value of any information assets involved.

2.3. The result of the risk assessment shall be presented to the management for approval prior to signing the outsourcing contract.

3. Contracts and confidentially agreements

3.1. The formal contract between organisation and the outsourcer shall exit to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing.

3.2. Any information received by organisation from the outsourcer which is bound by the contract or confidentially agreement shall be protected by appropriate classification and labelling

3.3. Upon termination of contract, the confidentially arrangements shall be revisited to determine whether confidentially has to be extended beyond the tenure of the contract.

4. Hiring and training of employees

4.1. Outsource employees, contractors and consultants working on behalf of organisation shall be subjected to background checks equivalent to those performed on organisation employees.

4.2. Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to organization information security policies, standards, procedures and guidelines (*e.g.* privacy policy, acceptable use policy, procedure for reporting information security incidents *etc.*) and all relevant obligations defined in the contract

Ref: ISPOL-35 Protection Of Test Data

PURPOSE

To ensure that the test data helps in assuring the quality of the product and also in managing and streamlining the Quality Assurance of the product that has to be released to the customers - both internal and external as applicable.

SCOPE

The test data is to be used within the test environment. The test data may be any kind of input to application. The software development team will have right to access the test data in testing environment. Each tester will try to manipulate the data according to his/her own needs. In some cases, the test data may be reused. Most of the times in regression testing the test data is reused, it is always to verify the test data before re-using it in any kind of test.

REFERENCE

NONE

RESPONSIBILITY

All members of technical team will be responsible for the protection of test data in all scenarios.

POINTS TO BE NOTED WHILE SELECTING THE TEST DATA

1. Analysis Data

Generally test data is constructed based on the test cases to be executed. For example in a System testing team, the end to end test scenario needs to be identified based on which the test data is designed. This could involve one or more applications to work. A thorough analysis of all the different kinds of data that maybe required has to be made to ensure effective management

2. Data setup to mirror the production environment

This is generally an extension from the previous step and enables to understand what the end user or production scenario will be and what data is required for the same. Use that data and compare that data with the data that currently exists in the current test environment. Based on this new data may need to be created or modified

3. Determination of the test data cleanup

Based on the testing requirement in the current release cycle (where a release cycle can span over a long time), the test data may need to be altered or created as stated in the above point. This test data although not immediately relevant, maybe required at a later point.

4. Identify sensitive data and protect it

Many times in order to properly test applications, there may be large amount of very sensitive data that is required. For example, a cloud based test environment is a popular choice because it renders on demand testing of different products. However, something as basic as guaranteeing user privacy in a cloud is a cause of concern. So especially in cases where we will need to replicate the user environment, the mechanism to shield sensitive data must be identified. The mechanism is largely governed by volume of the test data used.

5. Automation

Just as we adopt automation for running repetitive tests or for running the same tests with different kinds of data, it's also possible to automate the creation of test data. This would help in exposing any errors that may occur with respect to data during testing

6. Effective data refresh using a central repository

A lot of effort in creating test data can be saved by maintaining a central repository which contains all kinds of data that maybe required for various kinds of testing.

Ref: ISPOL-36 Restriction On Changes To Software Packages

PURPOSE

To provide guidelines for restriction on changes to software packages. Once the software packages are released, there should be minimal changes in coding. Executable code must be prevented from users accessing it other than members of the software team. No changes should be taken up if these changes are going to have adverse impact on the organization.

SCOPE

The use of this policy document applies to all the technical personnel who are working in IT-software Department. All the changes to the software should be routed through proper channel with a change request form.

RESPONSIBILITY

All members of the technical team are responsible.

GUIDELINES FOR RESTRICTION ON CHANGES TO THE SOFTWARE PACKAGES

1. Modifications to the executable code must be prevented unless provided by the respective vendor/user in the form of a patch or upgrade.

2. Modifications to the vendor supplied software packages that are provided via 'open source' resources should not be allowed on the in-house systems unless specifically supported and supplied by the original vendor.

3. Where it is essential to change the software package due to un-avoidable circumstances, then the following points must be considered:

- o Evaluate the risks of built-in controls and ensure that the integrity processes are not compromised
- o The consent of the vendor/user should be obtained where applicable
- o The possibility of obtaining the required changes from the vendor/user as a standard program update should be explored
- o Study the impact in case the organization becomes responsible for the future maintenance of the software as a result of the changes
- o The possibility of undetected security compromises existing in the new code

Ref: ISPOL-37 Secure Development Environment

PURPOSE

To improve practices of the software development lifecycle stages on software security and integrity across applicable diverse environments. Also to examin vendor practices reinforcement and assertion that software assurance is addressed throughout the software development lifecycle is effective and not treated as a one-time event or single box on check list.

SCOPE

The guidelines in this policy are applicable to software development, testing and safe storage of source codes.

RESPONSIBILITY

The system development team is responsible for creating a secure development Environment.

KEYS TO CREATING A SECURE DEVELOPMENT ENVIRONMENT

ISOLATE DEVELOPMENT FROM PRODUCTION:
There will be separate environments for development, test and production. It keeps untested code changes from deleting or corrupting production data, and it keeps developers from having access to test and production systems. There will be separate sandboxes for separate activities. Those sandboxes are for Development, Project integration, Demo, Pre-production and production.

SECURE THE ENDPOINTS
External storage media will be prohibited from connecting to the development environment. Only development team has a right to use external media in case of any need.

KEEP CODE IN THE ENVIRONMENT
Programming codes should be kept in separate server and not to be kept in external media. Backup of code will be kept in secured place and retrieving the information from non-secure environment could be open invitation for malware.

AUDIT ALL THE TIME
Code will be reviewed thoroughly before the system put into production. In addition to auditing code, run periodic security checks on all programmers, designers, and others who work in the web application development pipeline.

USE SECURED FEATURES
Before developing the product, proper design documents will be prepared and coding standards, secure coding requirements, code review process with roles and responsibilities and enforcement mechanisms will be pre-defined. Release management should also include proper source code control and versioning will be implemented.

Ref: ISPOL-38 Secure Development Policy

PURPOSE

To provide guidance on specifying, designing/selecting and implementing information security controls through a set of **process** integrated throughout an organisation's System Development Life Cycle/s (SDLC). It is process- oriented. It

addresses all aspects from determining information security requirements, to protect information accessed by an application as well as preventing unauthorised use and/ or actions of an application.

SCOPE

The use of this policy documents applies to all technical personnel who are developing, managing new systems or making modification or enhancements to existing systems.

REFERENCE

NONE

RESPONSIBILITY

The Manager- Software will ensure that security rules to be applied while developing the software and system which will be used in the organization.

RULES OF SECURE SOFTWARE DEVELOPMENT

The developer will be under pressure, if there is urgency from client/user end for any software product. This could mean sacrificing quality of the product and dependability for speed. This may leads to release of poor quality product and also in poor development techniques. In all cases, developer has to maintain the product in all respects. To meet those demands, developers need to institute server rules.

Rule 1. : Make proper code review and repeat testing a priority

Codes should be properly aligned and reviewed at the time of development. Co-ordination should be required among developers.

Rule 2: Software assurance is more critical than ever.

Update happens continuously and will often be pushed, perhaps multiple times a day. If the software is not continuously monitored and the code gets evaluated, this almost certainly guarantees failure.

Rule 3: Management must take responsibility for software risk.

One way to evaluate issues like reliability, security, or performance at a high level is through analytics that loop business leaders into where the vulnerabilities lie, in order to protect customers and meet the company's fiduciary responsibility to shareholders. Another way is through benchmarking. Knowing the baseline starting point and comparing it to industry performance provides fact-based insight.

Rule 4: Up the game for structural quality analysis.

For some enterprise IT developers, this might be a familiar environment, especially if they are running mission-critical systems, like a utilities provider or a bank. But, ordinary app and device software developers could suddenly find themselves needing to take much more rigid precautions, such as the same degree of structural quality analysis and code review required by software engineers for airline autopilot systems.

Rule 5: Make software quality and security education a priority

We all need to evangelize the fact that security vulnerabilities caused by poor coding or system architectural decisions can be some of the most expensive problems to correct.

Ref: ISPOL-39 Secure System Engineering Principles

PURPOSE

To aid in designing secured information systems and organization complied set of engineering principles for system security. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. Design, develop and operate information systems using security engineering principles.

SCOPE

The guideline in this policy is applicable to all the developers who develops the software.

RESPONSIBILITY

The system development team is responsible for applying the secured system engineering principles while designing, developing the system.

GUIDELINES

1. Establish a sound security policy as the "foundation" for design
2. Treat security as an integral part of the overall system design
3. Ensure that developers are trained in how to develop secure software
4. Reduce risk to an acceptable level
5. Assume that external systems are insecure
6. Implement tailored system security measures to meet organizational security Goals
7. Protect information while being processed, in transit, and in storage
8. Consider custom products to achieve adequate security
9. Protect against all likely classes of "attacks."
10. Use common language in developing security requirements
11. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process
12. Implement layered security
13. Design and operate an IT system to limit damage and to be resilient in response
14. Provide assurance that the system is, and continues to be, resilient in the face of Expected threats
15. Limit or contain vulnerabilities
16. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
17. Use boundary mechanisms to separate computing systems and network infrastructures.
18. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations
19. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability
20. Strive for simplicity
21. Minimize the system elements to be trusted
22. Implement least privilege
23. Do not implement unnecessary security mechanisms
24. Ensure proper security in the shutdown or disposal of a system
25. Identify and prevent common errors and vulnerabilities

Ref: ISPOL-40 System Acceptance Testing

PURPOSE

To verify that the functionality of the software meets the requirements as documented in the Preliminary Design

Document. In order to minimize the time required to test the completed software, the System Test and Acceptance Test documents and activities are tested together.

SCOPE

The system acceptance testing will use cases in testing to find out if there are any errors. It cannot establish that the product functions properly under all conditions. It will not help in finding the root causes. The system acceptance testing will be done by testing team.

RESPONSIBILITY

The system development team is responsible for verifying the functionalities of the software based the change request form.

DOCUMENT ORGANIZATION

The remainder of this document defines the plan for conducting the combined System and Acceptance Tests in the following areas:

- **Test Objectives**: identifies the categories of tests that are to be included in or excluded from the System Test.
- **Procedures**: describes the procedures to be followed in preparing test cases, preparing test data, running tests and verifying test results.
- **Test Acceptance Criteria**: identifies the criteria for successful completion of the System and Acceptance Test.
- **Resources**: identifies the people and their responsibilities as well as hardware and software requirements.
- **Schedule**: a list of high-level activities and tasks together with expected start and completion dates

1. TEST OBJECTIVES

The combined System and Acceptance Test will provide a formal approach to testing THE PROJECT ADVISOR in the following areas:

- **Functional Testing**: to exercise the processing logic of the system to expose errors in data base updates, calculations and edits and to ensure that the system delivers all functionality described in the Preliminary Design.
- **Security Testing**: to ensure that the system security meets the specifications.
- **Human Interface Testing**: to ensure that the human interface (screens and reports) is usable and consistent. Ensuring adherence to standards is the responsibility of the quality assurance officer (in this case the Director of Methodology).

2. PROCEDURES

2.1 Test Preparation

One or more test cases will be prepared for each process in the Preliminary Design. Each command on the file pull-down menu for each screen will be tested. Data will be entered into every field; edits will be tested on selected fields only. Test cases will be designed to test multi-user access.

2.2 Test Environment

The Test environment will be set up on the Systems Development Environment Platform as per the Project Plan and will simulate a production environment. Access to the Test environment will be restricted to the Acceptance Test Team.

2.3 Test Execution and Evaluation

The test scripts will be executed in the sequence. This will allow the valid data generated by one test to be used as input to the next test, thus resulting in end-to-end testing of the full application

3. TEST ACCEPTANCE CRITERIA

Integration Methods will accept the application software when all test scripts specified have been executed and the expected results have been achieved on the initial run.

4. SCHEDULE

Before performing the system acceptance testing, user should schedule the tasks as per the requirement.

Ref: ISPOL-41 System Change Control Procedures

PURPOSE

To specify a procedure to regulate the changes to applications which are maintained by the technical team. The system change will be done on the basis of Change Request Form. The software team will review the Change Request Form accordingly makes the changes in system. The software team will also review the System Change Control Procedure in

terms of improving the process and dealing with systemic exceptions.

SCOPE

The software problems can be reported at any stage in the lifecycle. Problems can fall into a number of categories according to the degree of regression in the life cycle. i.e. how for back you need to go to fix the problem. Problem categories include: operations error, code does not conform to design, design does not conform to requirements and new or changed requirements.

1. DIAGNOSE PROBLEM

1.1 Identification of problem

1. If any problem in application or changes to be required in existing system, user has to fill the change request form

The developer will be under pressure, if there is urgency from client/user end for any software product. This could mean sacrificing quality of the product and dependability for speed. This may leads to release of poor quality product and also in poor development techniques. In all cases, developer has to maintain the product in all respects. To meet those demands, developers need to institute server rules.

Rule 1. : Make proper code review and repeat testing a priority

Codes should be properly aligned and reviewed at the time of development. Co-ordination should be required among developers.

Rule 2: Software assurance is more critical than ever.

Update will occur non-stop and will often be pushed, perhaps multiple times a day. If the software is not continuously monitored and the code evaluated, this almost certainly guarantees failure.

Rule 3: Management must take responsibility for software risk.

One way to evaluate issues like reliability, security, or performance at a high level is through analytics that loop business leaders into where the vulnerabilities lie, in order to protect customers and meet the company's fiduciary responsibility to shareholders. Another way is through benchmarking. Knowing the baseline starting point and comparing it to industry performance provides fact-based insight.

Rule 4: Up the game for structural quality analysis.

For some enterprise IT developers, this might be a familiar environment, especially if they are running mission-critical systems, like a utilities provider or a bank. But, ordinary app and device software developers could suddenly find themselves needing to take much more rigid precautions, such as the same degree of structural quality analysis and code review required by software engineers for airline autopilot systems.

Rule 5: Make software quality and security education a priority

We all need to evangelize the fact that security vulnerabilities caused by poor coding or system architectural decisions can be some of the most expensive problems to correct.

Ref: ISPOL-42 System Security Testing

OBJECTIVE

The purpose of this document is to provide guidelines for organizations on planning, conducting technical information security testing, carry out assessments, analyze findings and developing mitigation strategies. It provides practical recommendations for designing, implementing, maintaining technical information relating to security testing,

assessment of processes and procedures, which can be used for several purposes.

SCOPE

The use of this policy documents applies to all technical personnel who are working in IT-software team.

RESPONSIBILITY

The system development team is responsible for testing the security functionality during software development based on the security testing techniques.

SYSTEM SECURITY TESTING TECHNIQUES TO ADOPT DURING SOFTWARE DEVELOPMENT

5. Risk Analysis

To review security requirements and to identify security risks, risk analysis is carried out during the design phase of the development. Threat modelling is a methodical process that is used to identify threats and vulnerabilities in the software. It helps system designers to analyze and think about the security threats that their system might face. It is recommended that all applications have a threat model developed and documented. Threat models should be created as early as possible in the SDLC and should be revisited as the application evolves and development progresses.

6. Code Review

Source code review is carried out by static analysis. It is the process of manually checking source code for security vulnerability. Many serious security weaknesses cannot be detected with any other procedure of analysis or testing. Operational procedures need to be reviewed as well, since the source code being deployed might not be the same as the one which is being analyzed.

7. Automated Static analysis

Automated static analysis is an analysis that examines the software without executing it, and it involves the use of a static analysis tool. The main objective of static analysis is to find out security flaws and to identify their potential fixes.

8. Fuzz Testing

Fuzzing is a technique for finding security-critical flaws in any software in a very less computational cost and time. Fuzz testing takes random invalid data to the software under test through its environment or another software component. Fuzzing means a random character generator for testing applications by injecting random data at their interfaces.

9. Vulnerability Scanning

Application vulnerability scanners are a very important software security testing technique. These tools scan the executing application software for input and output of known patterns that are associated with known vulnerabilities. In application level software, automated vulnerability scanning is used.

10. Penetration testing

The alternate name of Penetration testing is ethical hacking. It is a very common technique for testing network security. While penetration testing has proven to be effective in network security, the technique does not naturally translate to applications.

Ref: ISPOL-43 Technical Review Of Applications After Operating Platform Changes

PURPOSE

To provide guidance to the technical team about the points to be reviewed from technical end when the operating

system changes takes place. This guidance is to help the technical team to protect the data loss, application setup errors, application incompatibilities and performance problems. New features might be added which were not available in the older version of the software and these features may affect to application which are developed in older version. Changing operating system from the old version to the new version might affect the current application which is installed might be un-trusted and unreliable.

SCOPE

The use of this policy documents applies to all technical personnel who are working in IT-software team.

REFERENCE

NONE

RESPONSIBILITY

All members of technical team will technically review the applications when the operating system changes.

POINTS TO BE REVIEWED

1. Application incompatibilities

If any operating system changes or upgrades, there might be chance that the user may not run some applications. In some cases, you can get an uncooperative application to work by running it in compatibility mode.

2. Application setup errors

There are possibilities of errors in application setup when the operating system changes. There may be compatibility issues. In this case, user has to update the patch/s which is/are compatibility with new operating system.

3. Data loss

The data is the most precious thing. The operating system and applications can be reinstalled. But data is often unique and you might not be able to re-create it. Changing or upgrading operating system should leave data intact. It's best, as matter of course, to store user data on a different partition from one on which the operating system is installed.

4. Performance issues

Your upgrade installation proceeded without problems, but when you reboot and start using the system, you discover that the new OS runs much more slowly than the old one did. Usually the problem comes down to insufficient hardware, the wrong drivers, application incompatibility etc.

Appendix – A

#	Date	Policy Name	Brief description about the changes incorporated
1	22-Jan-2016	Information Security Policy	1. Consolidated individual policies listed in Ver. 2.00 into an integrated policy version 3.00

2	22-Jan-2016	Format Changed	1. Document Format changed as per ISO Standard
3	22-Jan-2016	Revision History	2. Approver name changed from Mr. Vishal to Mr. Viral
4	22-Jan-2016	Email Policy	3. Standardize email signature, changes done

Appendix A - 1 Data Source Manifest

Date:		Server Name:	

Type of Backup Agent Needed

☐	Windows	Version:		Type:	
☐	Windows	Version:		Type:	
☐	Linux	Version:		Type:	

List of Files/Folders to be Backed Up

Backup Client and Policy

Backup Client Installed On Client Server:	☐													
Backup Policy for Client Server:	☒ ☐ ☐	MON	☐ ☐ ☐	TUE	☐ ☐ ☐	WED	☐ ☐ ☐	THU	☐ ☐ ☐	FRI	☐ ☐ ☐	SAT	☐ ☐ ☐	SUN
Run Schedule for Policy:	AM:		PM:											

Only One Full(F) followed by either a Differential(D) or an Incremental(I)

Retention and Offsite

Retention Period for Backup:	☐	☐	☐	☐
Offsite Storage:	☐		☒	

Signatures

Requestor's Signature:		Date:	
System/Backup Administrator Signature:		Date:	

Appendix A - 2 Authorised Privilege Access form

Name of Applicant :		**Type**	**Permanent**
Job Title :			**Temporary**

Access Requested For :

Systems	Login Name	Access Level	Reasons

Access required: From date: _____
To date : _____

Applicant signature: _____

System owner name: _____

System owner's comments: _____

System owner's authorization: _____

Approved by: VP-IT

_____