aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

# Standard Information Security Policy

## Guideline Document

Second Edition

Initiated by TRA هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority
www.tra.gov.ae

www.aecert.ae

ae
CERT
فريـق الاستجـابة لطـوارئ الحاسـب الآلـي

Computer
Emergency
Response
Team

Initiated by TRA هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority
www.tra.gov.ae

P.O. BOX: 26662 Abu Dhabi, United Arab Emirates | Tel: +971 2 6269999 | Fax: +971 2 6118209
P.O. BOX: 116688 Dubai, United Arab Emirates | Tel: +971 4 2208888 | Fax: +971 4 2300100
aecert@aecert.ae

## Table of Contents

1. Creation and Issuance: 2

Table of Contents 3

2. Introduction 7

Scope 8
Organization's Information Security Mission Statement 8
Objectives 8
Responsibilities and Undertaking 8
Compliance 9
Definitions 9

3. Sub-Policies 16

3.1 Anti-Virus Policy 19
3.2 Password Management Policy 23
3.3 Internet Usage Policy 27
3.4 E-mail Usage Policy 31
3.5 Information Handling and Classification Policy 35
3.6 Encryption Policy 39
3.7 Desktop & Laptop Usage Policy 43
3.8 Software Compliance Policy 47
3.9 Backup and Restoration Policy 49
3.10 Remote Access Policy 53
3.11 Wireless Communication Policy 57
3.12 Mobile Phone Policy 61
3.13 Disposable of Media Policy 65
3.14 Visitor Premises Policy 67
3.15 Physical Access for Data Center Policy 69
3.16 Patch Management Policy 71
3.17 Physical Access for Operation Center Policy 75
3.18 Change Management Policy 77
3.19 User Access Management Policy 81
3.20 Information Security and Business Continuity Incident Management Policy 85
3.21 Acceptable Use of IT Equipment Policy 89
3.22 Clear Desk and Clear Screen Policy 93
3.23 Data Centre Document Management Policy 95
3.24 Log Management Policy 97
3.25 Physical Access for organization office Policy 101

# Introduction

Computer
Security
Protected!
Antivirus
Firewall
Email Scan
Passwords

# Introduction

Standard Information Security Policy (SISP) is defined as a set of standards, guidelines and procedures that specify in more or less detail the expectations in regard to the appropriate use of information and/or information assets and network infrastructure. SISP is a policy approved and supported by the senior management. The intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to the organization's established culture of openness, trust and integrity, however, it is the Information Security Department's commitment to protect the organization and its users from illegal or damaging actions by individuals, either intentionally or unintentionally.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, applications, data storage media, network accounts providing electronic mail, Internet browsing, and FTP, are the property of the organization. These systems are to be used for business purposes in serving the interests of the organization, and of our users in the course of their normal business operations.

Effective security is a team effort involving the participation and support of every employee in the organization and affiliate who deals with information and/or information systems. It is the responsibility of every user using the organization's resources to know these standards, guidelines and procedures and conduct their activities in compliance to this policy.

The SISP contains and is not limited to the following sub-policies to be adhered by all users:

- Anti-Virus Policy
- Password Management Policy
- Internet Usage Policy
- E-mail Usage Policy
- Information Handling and Classification Policy
- Encryption Policy
- Desktop & Laptop Usage Policy
- Software Compliance Policy
- Backup and Restoration Policy
- Remote Access Policy
- Wireless Communication Policy
- Mobile Phone Policy
- Disposable of Media Policy
- Visitor Premises Policy
- Physical Access for Data Center Policy
- Patch Management Policy
- Physical Access for Operation Center Policy
- Change Management Policy
- User Access Management Policy
- Information Security and Business Continuity Incident Management Policy
- Acceptable Use of IT Equipment Policy
- Clear Desk and Clear Screen Policy
- Data Centre Document Management Policy
- Log Management Policy
- Physical Access for organization office Policy

Adapting these policies will assist in complying with Information Security Management standard (ISO 27001:2005) and Business Continuity (BS 25999-2:2007).

## Scope

This policy applies to the organization employees, contractors, consultants, temporaries, and any other entity that works at the organization's premises, including all personnel affiliated with third parties all referred in here as the term "Users".

This policy applies to all equipments that is owned or leased by the organization.

## Organization's Information Security Mission Statement

"Ensure the Confidentiality, Integrity and Availability of organization's information, information systems and the entire network infrastructure against unauthorized disclosure, modification and/or downtime."

## Objectives

Information and information systems are considered the foremost important factor in continuing the day to day business functions effectively. Supporting the above the organization is committed to securing the information, the information systems and the network infrastructure by adapting to the following principles:

- Protect the information and the network infrastructure against external or internal threats.
- Provide minimum level of access between information systems and the users on a "Need-to-know" basis.
- Classify the information according to its criticality to protect it against unauthorized modifications or disclosure.
- Adopt set of leading industry standards, guidelines and procedures to ensure the security of information, the information systems and the network infrastructure.
- Conduct security awareness campaigns within the organization about the security policy (i.e. standards, guidelines and procedures) to educate the users of the best security practices when working with information and information systems.
- Conduct continuous risk assessment, risk analysis and risk management procedures to information and information systems.
- Monitor the logs and audit trails to ensure that information and information systems are protected against unauthorized violations.
- Ensure that users comply with all UAE federal, local and cyber laws, ethical responsibilities & regulations and information security policy pertaining to information and information systems.
- Protect the users and the organization from any inappropriate use that would expose the organization to risks including virus attack, compromise of network systems & services and any other legal issues.

## Responsibilities and Undertaking

It is the responsibility of the users, who have been provided with the IT services and privileges (such as: Internet Access, Domain Login Accounts, Desktop and/or Laptop, E-mail Account, etc.) to make themselves aware of the SISP and the sub-policies statements and their responsibilities towards complying with it. Users will be accountable for their actions.

Each employee who has been provided with the service will have to sign a written undertaking indicating that they have understood and are bound by the organization's Information Security Policy.

External users such as Consultants and Contract employees using the organization's IT services and privileges are also required to read, understand the SISP, their responsibilities and sign an undertaking.

## Compliance

Compliance with the organization's Information Security Policy is Mandatory for all users. Compliance checks will be performed on a regular basis by the Information Security team of the organization.

Any breaches or alleged breaches of this Policy will be investigated in accordance with the current Human Resources and Legal Department procedures and directly reported to the Head of the concerned department to take the Disciplinary actions. Accordingly, User must sign the Adherence to aeCERT Information Security Policy document.

## Definitions

### Back Up

The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

### Archive

The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing online storage space.

### Restore

The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server, database server, mail server and web server etc.

### Visitor

A visitor is any person, who is not an employee that enters the organizations premises. An example of a visitor could be a contractor who needs to perform a certain job. A visitor could also be a guest who needs to attend a meeting.

### Strictly Confidential

Information that, if made public, or even shared around the organization could seriously impede or collapse the organization's operations or result in human Loss. Information would include business plans, strategy, or Intellectual Property.

### Confidential

Any Client Information or aeCERT information if made public may result in loss of business or reputation. Information would include Inventory details, Client Contracts, Customer sensitive information, Employee Data.

### Internal Use Only

Any Information shared within aeCERT which if leaked, doesn't pose a major risk to aeCERT or its clients business. Such information would include internal communications etc.

### Public

Information or facts available to be disseminated to the external world.

## IT

Stands for "Information Technology," and is pronounced "I.T." It refers to anything related to computing technology, such as networking, hardware, software, the Internet, or the people that work with these technologies.

## Protection

The activity of protecting someone or something.

## Two-Factor Authentication

(TFA) means using any independent two of these authentication methods (e.g. password + value from token) to increase the assurance that the bearer has been authorized to access secure systems.

## Computer Contaminant

Means any set of computer instructions that are unauthorized to modify, destroy, record, transmit data or programs residing within a computer, computer system or computer network; or by any means to take control of the normal operation of the computer, computer system, or computer network by an unauthorized person or action.

## Malicious Software

Means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.

## Database

A database is a collection of data for one or more multiple uses. One way of classifying databases involves the type of content, for example: bibliographic, full-text, numeric, and image. Other classification methods start from examining database models or database architectures: see below. Software organizes the data in a database according to a database model. As of 2010 the relational model occurs most commonly. Other models such as the hierarchical model and the network model use a more explicit representation of relationships.

## Active Directory

Active Directory stores information and settings in a central database. Active Directory networks can vary from a small installation with a few computers, users and printers to tens of thousands of users, many different domains and large server farms spanning many geographical locations.

## Information Resources (IR)

Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, Mobile Phones, pagers, distributed processing systems and network attached, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

## Owner

The manager or agent responsible for the function which is supported by the resourcethe individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

## Custodian

Guardia or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For applications Information Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

## Change Management

The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

## Change means :

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

## Scheduled Change

Formal notification received, reviewed, and approved by the review process in advance of the change being made.

## Unscheduled Change

Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.

## Emergency Change

When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

## VPN

A virtual private network (VPN) is a computer network that is layered on top of an underlying computer network. The private nature of a VPN means that the data travelling over the VPN is not generally visible to, or is encapsulated from, the underlying network traffic. This is done with strong encryption, as VPN's are commonly deployed to be high-security "network tunnels". Similarly, the traffic within the VPN appears to the underlying network as just another traffic stream to be passed. If you can envision secured "pipe" within the wire that is your connection, you would be well on your way to picturing a VPN deployment, if perhaps oversimplified.

## Authentication

Is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the subject are true. This might involve confirming the identity of a person, tracing the origins of an artefact, ensuring that a product is what it's packaging and labelling claims to be, or assuring that a computer program is a trusted one.

## Security Incident

In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system.  It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. It also includes violations to the security policy enforced by the organization and unauthorized access to restricted areas in the organization.

## Business Continuity Incident

Any situation that might be, or could lead to, a business disruption, loss, emergency or crisis Examples of business continuity incidents are: disasters of any kind, unavailability of more than 33% of the employees in aeCERT, or downtime of email for more than half an hour.

## Information Security Incident Response Team (ISIRT)

Personnel who are responsible for coordinating the response to information security incidents in an organization.

## Primary Roles are:

- Focal point for analysing the security incidents
- Helps in finding the root cause of the security incidents
- Observing new technologies and security threats (in respected area)
- Suggesting the recommendations and improvements to protect the assets

## Resident Vendor

External company which supplies services (Implementation and maintenance of software, Hardware, Turn-key solutions), to aeCERT and referred to as supplier.

## Resident Consultant

Organization or individual, who provides support or help in implementation and management for aeCERT for short time project/services.

## Chain Email or Letter

Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

## Clean Desk

Can produce a positive image when our customers visit the company

## Filling Papers

Preservation and methodical arrangement as of documents and papers

## Access

The Infrastructure and some enterprise security staff shall have full access to all network documentation. The Infrastructure team shall have the ability to read and modify network documentation. Designated enterprise security staff shall have access to read and change network documentation but those not designated with change access cannot change it.

## Storage Locations

Documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the IT infrastructure. Information in both facilities should be updated annually basis at the time of the documentation review.

## Internet

A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange

## Download

Transfer a file or program from a central computer of any Web Site to a internal computer or to a computer at a remote location.

## Logs

Are records of events that occur within the information systems of an organization.

## Application Logs

Have the ability to generate an audit trail of past transactions with time stamps, user names and object access details

## Mobile

A hand-held mobile radiotelephone for use in an area divided into small sections (cells), each with its own short-range transmitter/receiver

## Device

Something in an artistic work designed to achieve a particular effect

# Sub-Policies

POLICY
COMMUNICATIONS
CREDITS
QUOTATION
VISION
CALL CENTER
PURCHASE
PROMOTION
RESEARCH
FINANCE
MEETING
CHANNEL
PERFORM
EXPORT
MANAGEMENT
SERVICES
LOANS
PROFIT
QUALTY CONTROL
PRESENTATION
LOGISTIC
PACKAGING
MARKETING
HUMAN RESOURCE
DEVELOPMENT
INVOICE
FEASIBILITY
BONUS
PRICING
PRODUCT

VIRUS

# Anti-Virus Policy

## Objectives

### The objectives of this sub-policy are:

- To detect, prevent and minimize the impact of Virus outbreaks in the organization's systems such as, servers and user-end desktops & laptops.
- To protect the systems against the spread of malicious viruses.
- To define appropriate control measures for users in order to protect the systems against virus attacks.
- To ensure the protective and optimum performance of the users when using the systems without any considerable delays.

The organization will follow the below preventive and detective control measures to protect against malicious software and virus attacks.

### Scanning for Viruses

- Users are allowed to use only authorized/licensed software in the organization. Use of any other software without the written permission of the Head of the concerned department is prohibited.
- All files and software downloaded/received either from or via external networks, e-mail, or on any other medium such as data storage media should be first scanned for viruses/ malicious code prior its use.
- Database/file servers where critical data is stored will be scanned for viruses on a regular basis.
- Any data storage media brought into the organization must be scanned for virus before being used by the user or to be given to the Information Security Team for scanning.
- Organization's Laptops of users will have to be first updated with the Anti-virus software in use at the information security division and scanned for viruses by the information security team and approved, before connecting to the organization's network.

### User and Information Security Team Responsibilities

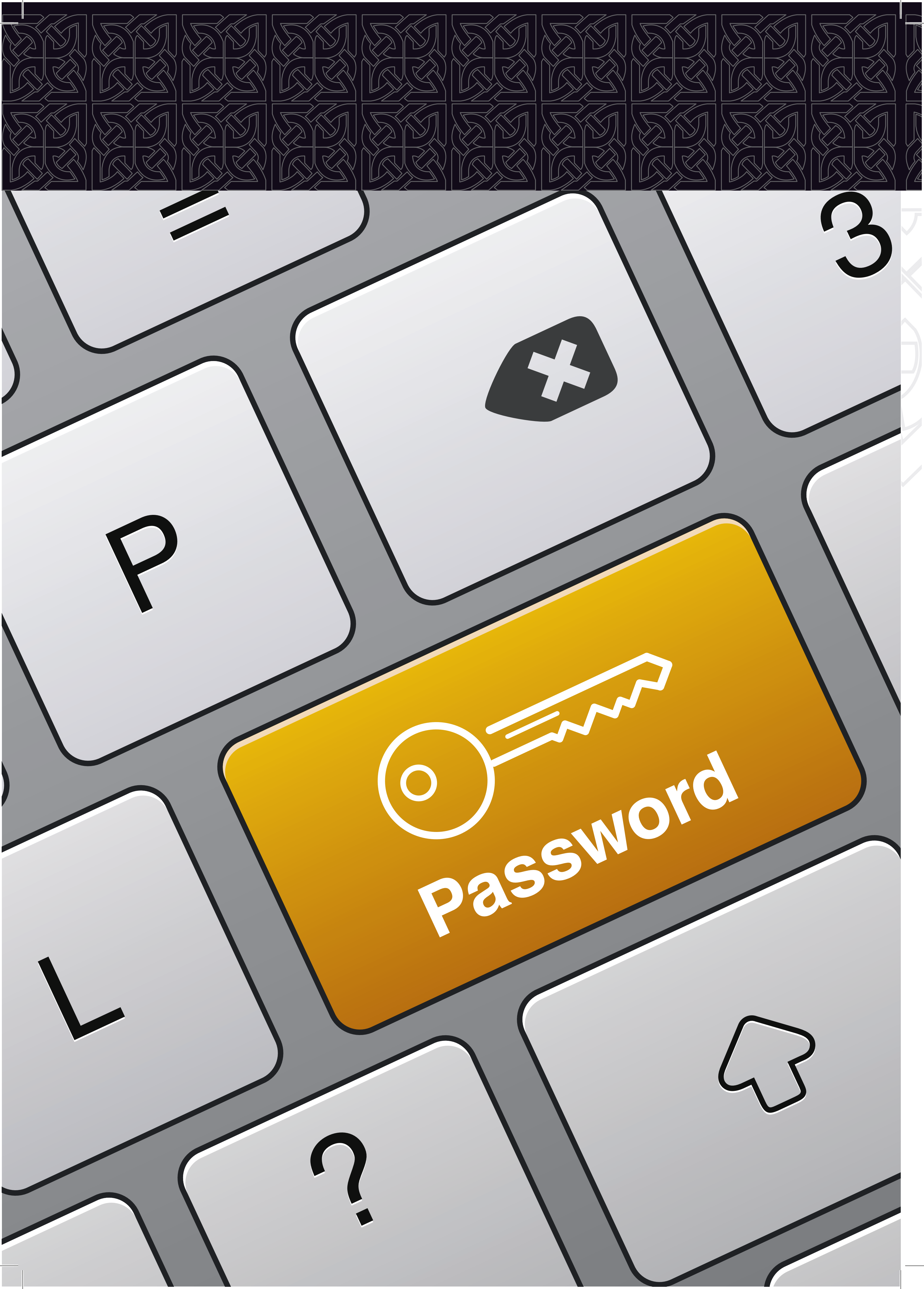
- Anti-virus software will be configured to clearly instruct the user to either disinfect or erase the file if a virus is found and users are advised not to disable, remove or change the configuration of the Anti-virus software installed on their desktops and laptops.
- All users are advised to report virus attacks if any detected to service desk along with the necessary details like name of the virus, the action taken and the results thereon.
- All users are prohibited from opening any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and then empty the Recycle Bin.
- All users must delete spam, chain, and other junk email without forwarding, in keeping with organization's Acceptable Use Policy.
- On sighting a virus alert or suspicious activity, users are advised to immediately disconnect their systems from the network and contact the information security team for immediate support.

- Users are not allowed to disable the anti-virus software residing on their desktop and/or laptops.
- The information security team will inform the users regularly of the latest viruses and the precautions to be taken by the users to mitigate the virus risk.
- E-mail will be used by information security team to communicate to the users about the virus alerts and the guidelines to follow as a security precaution. It is Mandatory for users to follow those guidelines.
- The information security team will refer to qualified resources, such as reliable antivirus software suppliers, CERT advisories, etc. to identify the potential viruses and differentiate between hoaxes and real viruses.
- Latest signature updates will be downloaded on to a central server and the updates will be pushed automatically on to the desktops and servers with little or no user intervention. This must be scheduled to occur automatically on a daily basis.
- Information security team will routinely check the Laptops and Desktops for the presence of Anti Virus software and the signature level, and if required will install/update the latest signature updates before it gets connected to the organization's network.
- The information security team will regularly check the Anti-virus server logs to see if all the desktops and servers are running with the latest updates, if not they will manually push the updates.
- Information security team will continuously monitor the vendor sites for signature updates.
- All updates, as soon as received from the vendors, will be rolled out to the various desktops, laptops and servers on a high priority basis.

## Audit and Review

The information security team may conduct review on a regular basis to ensure:

- Presence of the anti-virus software on the user desktops and laptops.
- Anti-virus software is not disabled on the users systems.
- Setting of the anti-virus software is configured correctly.
- Number of virus related incidents are recorded and action taken.


=
3
P
Password
L
?

# Password Management Policy

Passwords are a common form of verification and are considered the only barrier between a user and his/her personal information.

## Objectives

### The objectives of this policy are:

- Enforce adequate password controls in systems and user level.
- Protect information and information assets related to the user.
- Ensure that only authorized users can access certain information, applications, services and systems.
- Protect the Confidentiality, Integrity and Availability of information, systems, services, and applications within the organization's network.

### Password Allocation

Every user is given a username and a password to access the systems, applications, servers, services, domain, etc. on a "need-to-know" basis after the approval/authorization from the Manager of the concerned department.

The access will be withdrawn when the employee leaves the organization and/or if a user's contract comes to an end or upon a request from the Manager of the concerned department.

### Creating Strong Passwords

- User passwords should remain confidential and not shared, posted or otherwise revealed in any manner.
- The minimum length of a password is 8 characters
- User passwords must not be based on personal information that can be easily guessed or accessed (such as: name of wife, name of husband, date of birth, mobile number, etc.)
- User passwords must not be a word in any language, dictionary, slang, dialect, jargon, etc. (such as: password, julie, 123456789, qwerty, etc.)
- The password must be a combination of Alpha Numeric characters. (such as password like: TaM*55*F where you have upper case, lower case alphabets, numbers, and characters such as *, %, $, #)

### Password Expiration

- Passwords will expire after a minimum period of 60 days. (Expiry)
- A given password will not be repeated within a cycle of 6 password changes. (History)

### First time Use of Initial Passwords

If a user is given with an initial password by the Administrator, the user must change this password immediately after the first time he/she logs into the system.

### Password Reset

- For security reasons, user account password should be changed at least once every two months.

- User password resets will be performed when requested by the user, after verification of identity.
- Only the user to whom the USER-ID is assigned will request for user password reset. The Information Security Manager will be informed whenever a password is reset for a particular user.

## Screen Saver Password

Every user will use the organization screen saver set by information security team with a password, which be activated within 5 minutes of inactivity.

## Password Protection

- Do not reveal your password over phone to anyone, in an email message, to the manager, to information security team, or in front of others.
- Do not hint at the format of the password
- Do not share a password with co-workers, friends, or family members
- Do not reveal a password in questionnaires and/or Internet.
- Do not use the "Remember Password" feature of applications (e.g. Outlook, Web-mail, etc.)
- If you feel that your password is suspected to be compromised, change it immediately.
- Always lock your account before leaving your workstation/laptop, even for few minutes (use the key combination CTRL+ALT+DEL then lock computer or the windows key with the letter L)

## Password Maintenance

Information security team reserves the right to run password cracking or guessing tools on periodic basis against user passwords and any easy passwords detected during the scans, the user will be required to change the password. Such checks will be approved, scheduled and audited by senior management.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the password is enforced.

BUSINESS NEWS
Home
News
Business
Markets
Industries
Technology
Travel
Jobs
Opinions
Growth Picks Up
Real estate market review
World Econom
for ene
Oil prices hit two-year high

# 3.3 Internet Usage Policy

Internet Access is vital to assist the users to conduct their daily business needs and functions within and across other departments in the organization in a secure manner (without endangering the security of the organization's Information and Information Assets) with a uniform code of conduct.

## Objective

### The objectives of this Policy are:

- Ensure that the Internet is used for business purposes only.
- Protect the Information and Information Assets even when users access the Internet.
- Communicate within and across organization network and other departments in a secure manner.
- Manage user productivity and optimize the use of IT Infrastructure through control of Internet Access.
- Ensure having an efficient Internet Access within a secure networked environment to all users.

### Internet Access

Internet Access will be provided to the user only after the approval/authorization by the Manager of the concerned department.

The service will be withdrawn when the employee leaves the organization and/or if a user's contract comes to an end or upon a valid request from the Manager of the concerned department.

### Statements

- Users are permitted for the use of the Internet service that supports the business needs/ functions and for furthering their knowledge in their areas of expertise in the organization.
- Users are permitted to limited personal use of the Internet as long as:
- It does not delay the business operations and functions.
- It does not violate the applicable laws or company policy, and;
- It does not degrade the organization's network performance.
- Users are prohibited from sharing their Internet User Identification and password.
- Accessing, contributing and downloading from offensive sites are prohibited. Offensive sites include sites that support racism, derogatory religious sentiments, offensive language, defamation or derogatory/abusive attacks on any individual or group and sites having pornographic content.
- Users are prohibited from using any automated tools or any other means for gaining unauthorized entry into any third party systems or any resource over the Internet to which they do not have authorized access rights.
- Users are further prohibited from engaging in any activity that will result in the disruption in operations of either the organization's or any third party computer systems.

- Users are not permitted to post company specific/ proprietary/ confidential information pertaining to the company on the Internet including on forums, groups, Anonymous FTP servers, or any other such open facility. Users are not authorized to make personal statements that could be misconstrued to the official position of the organization.
- Users are prohibited to use any Chat channels (such as: MSN messenger, Yahoo messenger, or web based chat, etc.)
- Users are prohibited from downloading and/or uploading and installing software from the Internet. Any such requests will have to be routed to IT division after approval from the concerned Head of Department.
- Users must not open any attachment via the Internet from any non – organization e-mail system, such as (hotmail, yahoo, etc.)
- Users are prohibited from changing and removing the browsers settings configured to use the proxy and any direct dial up connection from a system connected to the network is strictly prohibited.
- The organization has all the right to enforce URL filtering to block access to certain sites that are considered offensive and/or not relevant to the business.

NOTES

## Please note the following:

- All activity on the Internet is monitored and logged.
- All material viewed is scanned for viruses.
- All the content viewed is scanned for offensive material.

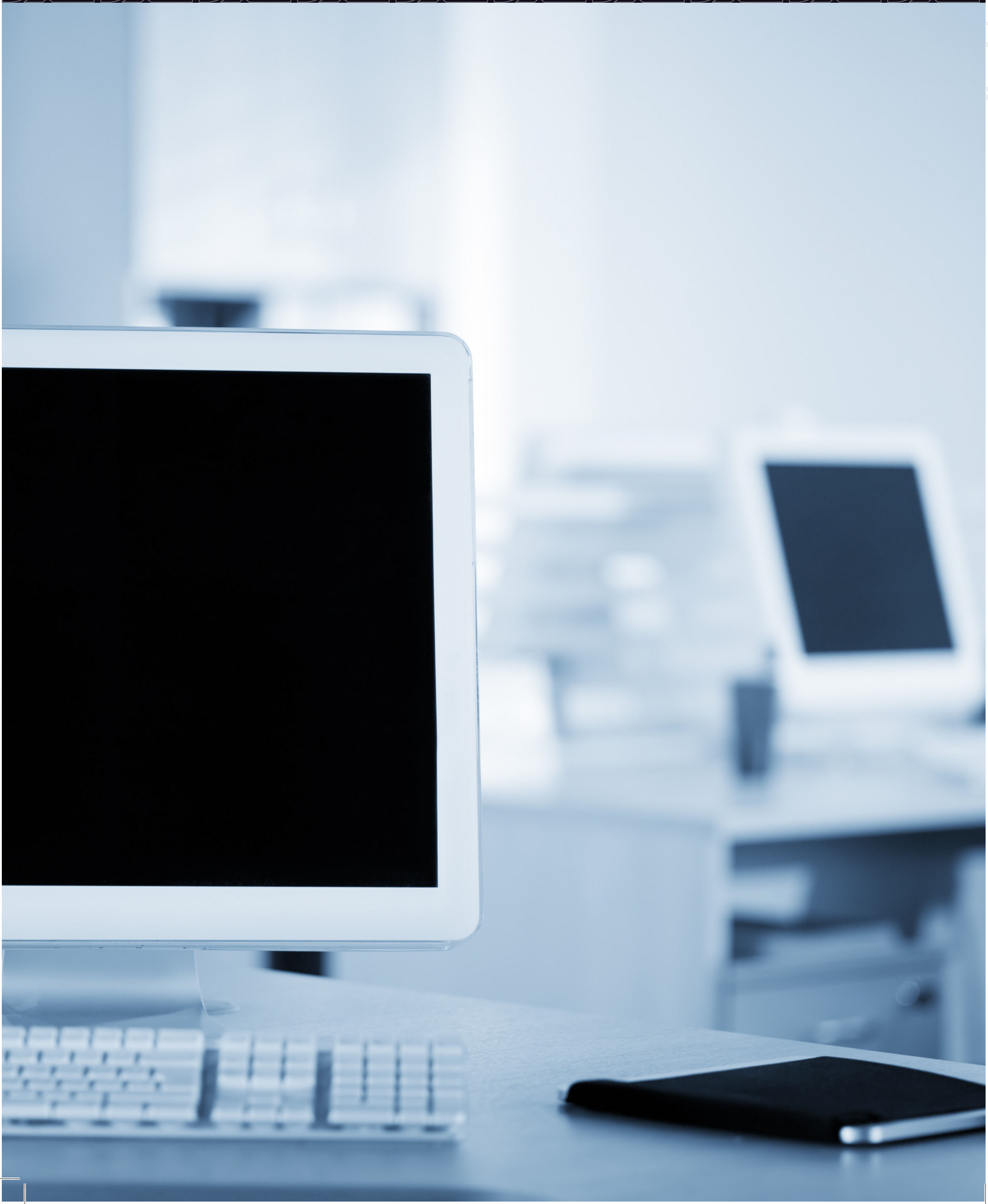
If you are in any doubt about an issue affecting Internet Access you should consult the Head of IT Security Department. Any breach of the Organisation's Internet Acceptable Use Policy may lead to disciplinary action.

## Use of Internet in Special Case

Where Incident Handling Team wants to investigate any website they should be allowed to do it with the approval of Head of IT Security Department.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.



# 3.4 E-mail Usage Policy

Electronic mail (e-mail) is an important communication tool used widely in the organization to correspond internally within and/or externally with customers, business partners, suppliers and others in a fast and efficient way.

## Objective

### The objectives of this policy are to:

- Ensure the appropriate method to use e-mail within and across other departments in the organization.
- Ensure that risk exposures of information and information assets are minimized.

### Email Access

Organization's e-mail access will be provided to the user only prior approval/authorization by the Manager of the concerned department.

The service will be withdrawn when the employee leaves the organization and/or if a user's contract comes to an end.

### Statements

- Organization's e-mail will be used only for the conduct of the organization's business needs and functions.
- Ensure that when sending email with the organization's Business Information with business attachments that the email recipient is the intended person to receive it.
- Use of e-mail services for purposes constituting clear conflict of the organization's business functions or in violation of the organization's e-mail usage policy is expressly prohibited.
- Users are not permitted to use the organization's email to participate in chain letters/e-mails or forwards internally or externally.
- Users are not permitted to send large attachments containing graphics/pictures/objects/video files that can result in disruption of the organization's e-mail services unless if work related.
- No user is permitted to send sensitive and confidential data through the organization's email without the use of encryption software.
- Encryption may be used to send confidential or proprietary information via e-mail, so that it is only readable by the intended recipient. (Refer to the Encryption Policy)
- All users must scan and verify that the files to be sent via e-mail as attachments contain no viruses or malicious codes.
- Unsolicited e-mail/Junk email is to be treated with caution and not responded to.
- Usage of profanity, obscenities, or derogatory remarks in any e-mail message is prohibited.
- No user is permitted to read or send e-mails from another user's e-mail account without that user's explicit permission and written authorization.
- Automatically an E-mail Security Disclaimer will be added at the Mail Gateway to all users when sending any e-mail externally.

- Users are not allowed to send sensitive information to personal email accounts.
- It is strictly prohibited the use of auto forwarding of corporate emails to personal email accounts.
- Organization's email service access over the public channel (outlook web access using Internet or mobile ActiveSync) shall have encrypted communication channel.

## Virus Protection

- All Incoming/Outgoing e-mails will be scanned for viruses and other malicious content.
- Gateway Anti Virus software will be installed on the e-mail server and periodically updated with the latest signatures as and when received from the vendor.
- The e-mail server will be periodically updated with the latest service packs/patches.
- Any virus infected e-mail, as detected by the Anti Virus software and which cannot be cleaned will be quarantined.
- The sender/recipient will be notified if any viruses are detected in any e-mail and the nature of action taken.

## Mailbox and E- Mail Size Limitations

- Size of external (incoming/outgoing) email attachments is not restricted.
- Mailbox size for the organization users will be limited to 1GB.
- Requirement of a larger mailbox size will need to go through an authorization process, and will require the approval of the Head of Department.
- Users will be trained to periodically archive their emails on the user folders that are created on the File Server and the manner in which the personal folders (PST) need to be protected.
- Users are encouraged to send all attachments to e-mails in a compressed mode/zipped format.

## Monitoring and Maintenance

- The organization’s information security team reserves the right to monitor E-mail Access against this Policy. The e-mail server will be monitored for:

1 Uptime

2 Disk space

3 CPU & Memory usage

4 Mail Flow / Mail Queues

5 The e-mail server will be monitored for any spamming and relaying attempts.

6 The e-mail server will be backed up daily.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

# 3.5 Information Handling and Classification Policy

Electronic mail (e-mail) is an important communication tool used widely in the organization to correspond internally within and/or externally with customers, business partners, suppliers and others in a fast and efficient way.

## Objective

### The objective of this policy is to:

- Classify the organization's information assets based on its criticality.
- Ensure that adequate level of protection is applied and adhered in line with asset classification.
- Information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

### Information Classification practices

- The organization shall maintain and update a database of all its information assets of all locations and related to Infrastructure processing facility.
- Assets shall be classified in accordance with business needs, level of confidentiality, value and the impacts associated. The responsibility for classifying assets is with the originator or nominated owner of the asset.

### Information Categorization

a. Organization shall follow a Four scale grade for classifying its asset

I. Strictly Confidential
II. Confidential
III. Internal Use Only
IV. Public

b. The classification category must be marked in the top left header of every printed page.

c. Information which resides in the electronic form also part of same classification requirements.

d. Electronic data, whether stored or in transit, that is classified as confidential and strictly confidential must be kept encrypted.

## Security requirements for the Classified Information

a. All Classified Information shall have the following Security requirements

## PHYSICAL DOCUMENTS

| Action | Strictly Confidential | Confidential | Internal Use | Public |
|---|---|---|---|---|
| Labeling of Documents | Must not Copy without the permission of Information Owner | Must not Copy without the permission of Information Owner/custodians | Must not be Copied without Business requirement | No Special Requirement |
| Storage of Documents | Stored in Secured Location in Fire Proof Cabinets | Stored out of sight | Stored out of Sight | No Special Requirement. |
| Disposal of Documents | Physical destruction beyond ability to recover | Physical destruction beyond ability to recover | No Special Requirements | No Special Requirements |
| Dissemination of Information | Not Applicable | Not Applicable | Not Applicable | Approval Needed |
| Transportation of Documents | Sealed envelope marked "Strictly Confidential" and delivered by hand to addressee only. | Sealed envelope marked "confidential" and delivered by hand. | Sealed envelope marked " private" | No Special Requirement |

b. Materials such as tapes used to record or store classified information, shall be treated with same level of the highest classification of data residing on the tapes.

c. Sensitive or classified information shall not be recorded on Answering Machine / Voice Mail systems

d. All Classified information shall be completely cleared from the server and portable computer before disposal or re-use.

e. Classified waste material (classified documents no longer required and the materials used in the production of such documents) shall be destroyed by shredding.

f. All classified data shall be erased before the media in which they reside such as disks and magnetic tapes are to be reused or disposed of.

g. Procedure needs to be developed to dispose the Information Assets/Data

h. Access control standards and data classification standards shall be periodically reviewed and maintained at all times.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

# 3.6 Encryption Policy

Electronic mail (e-mail) is an important communication tool used widely in the organization to correspond internally within and/or externally with customers, business partners, suppliers and others in a fast and efficient way.

## Objective

The objective of this policy is to ensure that Confidentiality and Integrity of sensitive/confidential data stored or transmitted is maintained.

### Data Encryption

The organization will provide maximum protection to classified, sensitive and confidential information by efficiently utilizing data encryption.

The organization will implement suitable encryption measures for any data being sent over third party networks and communication backbone. While implementing these encryption methods; the organization will adopt best standards for encryption and effective key management practices.

The concerned department head and the information security division will jointly approve the requirements for encryption of network traffic.

**Confidential data** transported on computer-readable storage media such as magnetic tape, floppy disk, or CD-ROM, etc., will be encrypted and appropriately safeguarded.

Proven, standard encryption algorithms with long keys will be used for data encryption.

Symmetric cryptosystem key length will be 128 bits long.
Asymmetric cryptosystem keys will be of a 1024 bit length.

The requirement for the key length will be reviewed on a regular basis by the information security team based on the nature and criticality of the business information.

### Responsibilities

The INFORMATION SECURITY OFFICER is responsible for:

- Regularly reviewing the use of cryptography and cryptographic keys in organization
- Acting upon any non-compliances with this policy

The System Security Administrator is responsible for:

- Creating keys and revocation keys for all users of the cryptographic solution in place and storing the revocation keys securely
- Revoking all cryptographic keys if an organization employee leaves the information after ensuring accessibility of all documents received from this employee

### Use of Encryption

Encryption technology will not be used for confidential/restricted information unless the organization’s management has first approved the technology.

The organization will consider use of cryptographic controls for protection of its information. At present, PKI is the most favored technology for secure Internet based services.

- All critical communication between the browser and the web server will be encrypted using standard and secure encryption algorithms. 128-bit SSL encryption will be used.

- Web e-mail will be accessed via SSL and if needed with an RSA token.
- PGP will be used for e-mail encryption to send confidential data.
- All users will be trained on how to use the encryption software by the information security team as follows:
- Encrypting sensitive/confidential files and folders on the Desktop/Laptop.
- Encrypting sensitive/confidential files and folders when sending it externally through an email.

## Statements

- Encryption shall be used in accordance with the Information handling and Classification Policy.
- Users shall use proven, standard algorithms installed by the information security team on desktop and/or laptop as the basis for encryption technologies.
- Users shall not use proprietary encryption, unless reviewed and approved by the information security team.
- Users shall encrypt all sensitive/confidential data residing on their desktop or Laptop.
- Users must use the PGP encryption software to send sensitive/confidential data through e-mail.
- Users must not share encryption keys among each other.
- No user shall attempt to generate own encryption keys, only the keys provided by the System Security Administrator shall be used.
- The PGP expiry date is one year.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

# 3.7 Desktop & Laptop Usage Policy

Whilst the desktop and physical laptop is a valuable asset which, if damaged, stolen or lost, will need to be replaced, the loss of Laptop could also mean that vital Information Assets which are stored on the Laptop could be accessed by unauthorized individuals and result in damage to the organization and its users.

## Objectives

### The objectives of this policy are:

- Ensure the acceptable use of organization information systems such as desktop and laptop.
- Ensure that if a laptop is lost or stolen, the only impact to the organization is the loss of the physical laptop asset value and not the valuable information residing on it.
- Ensure that employees follow an appropriate level of responsibility to safeguard the desktop and laptop that they have been allocated.

Desktops and Laptops will be issued to the user only after the approval/authorization by the Manager of the concerned department.

The Desktop and Laptop will be withdrawn when the employee leaves the organization and/or if a user's contract comes to an end or upon a request from the Manager of the concerned department.

### Statements

- Users must safeguard their Desktop against any damage.
- Users must safeguard their Laptop against loss, theft or damage.
- Users must not leave their Laptops unattended even for few minutes for example, in public area, airports, etc.
- Users must lock their account when leaving the Desktop and/or Laptop unattended.
- Users must ensure that the Corporate Anti Virus program is updated on their Desktop and/or Laptop.
- Users are prohibited to connect their personal Laptops to the organization's network.
- Users must have Corporate Anti Virus program running on their Laptop and updated by the information security team before connecting to the organization's IT Infrastructure after a business trip.
- Users must take care to safeguard Information Assets when accessing the IT Infrastructure from a public place.
- Users must adhere to the approved organization's encryption policy when storing sensitive and confidential information on their Laptop.
- Users must backup their business related files that they store on their Desktop and/or laptop on a regular basis on their network shared folders on the File Server.
- Users must not tamper with the Administrative functions of the Desktop and/or Laptop such as its Operating System or Administrator identification and password.
- Users must use the corporate request and approval procedures for requesting the

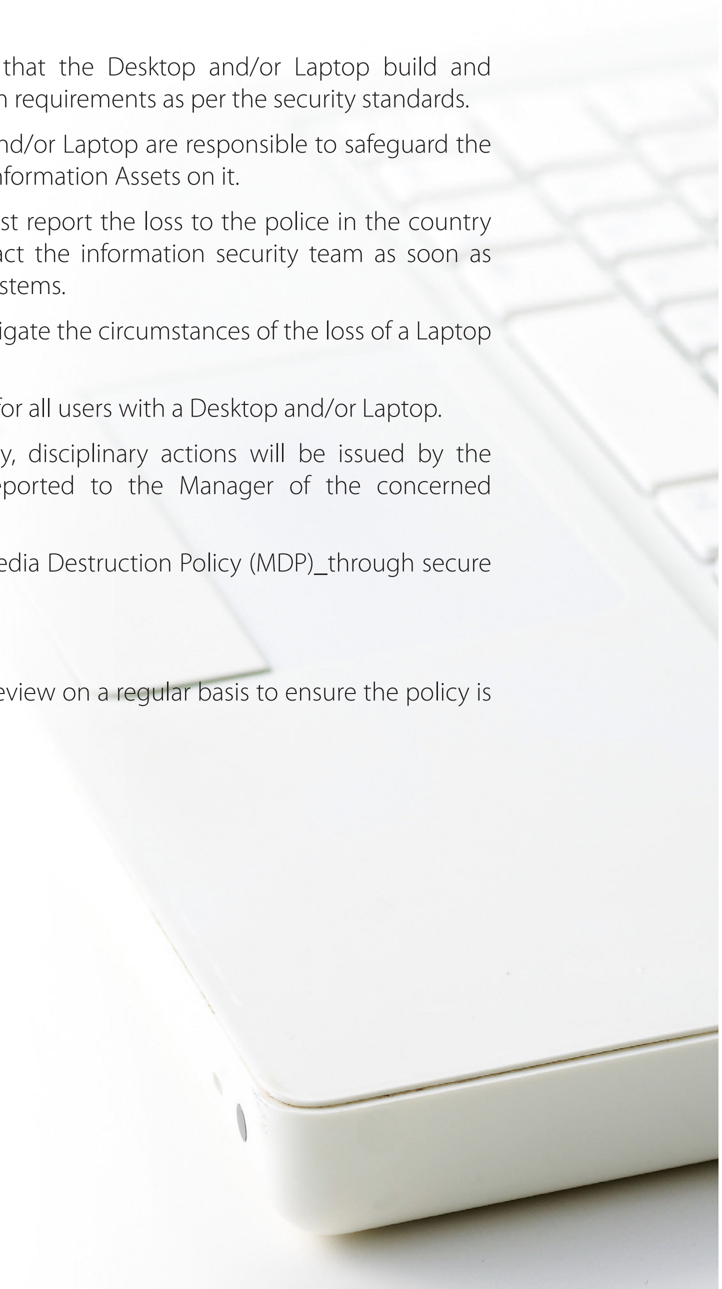
installation of external devices such as printers, storage devices, and third party software to their Desktop and/or Laptop.

## Terms and Compliance

- Information security team must ensure that the Desktop and/or Laptop build and implementation conforms to the minimum requirements as per the security standards.
- All users who are issued with a Desktop and/or Laptop are responsible to safeguard the physical Desktop/Laptop and any stored Information Assets on it.
- In the event of loss of a Laptop, users must report the loss to the police in the country where the loss occurred and must contact the information security team as soon as possible to limit the access to corporate systems.
- The information security team must investigate the circumstances of the loss of a Laptop before a replacement is issued to the user.
- Compliance with this policy is Mandatory for all users with a Desktop and/or Laptop.
- In case of non-compliance to this policy, disciplinary actions will be issued by the Information Technology division and reported to the Manager of the concerned department.
- Device replacement must comply with Media Destruction Policy (MDP)_through secure data eraser or breaking.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.



PARTNERSHIP
NEWS
CONTACT US
SITEMAP
Announcements
19 - 21 March 2012
International Security and National Resilience 2012
read more
EN
5:55 PM
3/13/2012
CERT ae
Computer Emergency Response Team

Solution
Einfg
Pos 1
Ä

# 3.8 Software Compliance Policy

## Objectives

This policy defines standards for use of company and third party software. This policy addresses software licensing, copyright and usage security requirements for all the users.

### Software Licensing

Purchase and use of third party software must be in accordance with third party licensing agreements.

The following restrictions should be considered for such software:

- Specific user restrictions such as the number of copies allowed to be installed, the number of desktops, laptops and servers the software can be installed on, or the number of concurrent users of the software allowed at one time.
- The use or copying of purchased software so that it can be used on a computer other than the computer for which it is licensed is strictly prohibited.
- Users are not allowed to install any software prior the approval and authorization of the Manager of the concerned department and the approval of Information Technology division.
- The duplication of the media, documentation, etc. is prohibited.

Failure to follow this standard can place the user and/or the organization in legal risk.

The information security team will perform periodic reviews of software used on the organization desktops, laptops and servers to ensure that it is in compliance with licensing agreements.

All software found in violation will be removed immediately. Individuals responsible for downloading and/or using non-compliant software on the organization system will be subject to disciplinary actions by the management.

### Software Copyrights

All users of software on the organization systems must strictly abide by the "Copyright Laws" and restrictions detailed by the software manufacturer.

### Use of Shareware and Freeware

Many freeware and shareware programs are available on the Internet and other locations. Most of these programs are legitimate and perform their advertised functions properly. Some of these programs are ineffective, inefficient, not secure, and actually include malicious code to harm the systems or the network. Most users are not capable of evaluating the performance or security of the programs. Therefore, information security team reserves the rights to either approve or disapprove the software requested for the freeware and shareware for use on the organization's systems and network.

### Software Ownership

Computer software developed by or for the organization is the sole property of the organization. This policy must be conveyed to all third parties who develop software or applications for the organization's use. This prevents dispute about ownership of the software, including the source code, once the project is complete. Software developed by the organization's employees on company time becomes the property of the organization.

### Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

aeCERT
Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي
BACKUP AND RESTORATION

# 3.9 Backup and Restoration Policy

## Objectives

The objective of a Backup & Restoration policy is to recover the information and information systems from an unplanned business disruption that could cause damage to its integrity, confidentiality and/or availability.

### Backup Requirements

- Backup requirements for all information and information systems within the organization must be identified and documented.
- The information security team will record and maintain the backup requirements for all systems under the responsibility of IT At a minimum, this will include details of backup frequency, information to be backed up, storage media, retention and recycling.
- In the case of data stored locally on desktops/laptops, it will be the responsibility of the users to ensure that the data is backed up on a periodic basis. Users wishing to backup their data, may either transfer data onto their network drive folders or request the IT team to make a backup on suitable data storage media. Such requests will require specific authorization by the concerned Head of Department.
- The IT team will decide which information is to be backed up and the frequency of backups in consultation with the information owner on the system criticality and it's Recovery Time.
- Users are responsible for the backup. It can be done through file print server or removable device belongs to the organization.

### Backup Schedule

All systems software, application software, user data, database information and associated documentation, will be backed up on a regular basis to facilitate recovery in the event of an unplanned system disruption. The frequency of the backup will be at a minimum:

- System Software: Before and after any changes to systems such as an upgrade, changes in configuration, patch updates etc.
- Application Software: Before and after any changes to the application such as a new version release or modification to application source code
- User Data/Database Information: On a periodic basis (Daily / Weekly / end of Year), based on the backup frequency identified for the individual systems.
- Device Configurations: Before and after any changes to the configurations of critical devices such as Routers, Firewalls, IDS etc.
- Documentation: Latest copies of system documentation (e.g. Technical reference manuals, User manuals etc.) will be backed up and maintained.

### Performing backups

- The IT team will maintain a weekly backup checklist specifying the various backups that are required to be taken for that day.
- The weekly backup operations will be logged against the checklist reviewed and signed off by the assigned engineer at the end of the day. At a minimum, the backup log will

record details about the backup carried out, start & end time, identification of the media used and success / Failure status.

- Any Unscheduled/One-time backups will require specific authorization by the concerned Head of Department. This will also be recorded in the daily backup list with appropriate reasons for the same.
- The backup checklist will be independently reviewed by Head of IT division periodically.

## Backup storage

- Backup media will be stored in two different locations – one onsite within the organization's premises, and the other at a location set by the organization.
- Physical access to the backup media will be adequately secured by implementing appropriate controls/encryption.
- Physical access to the backup storage locations will be restricted only to authorized personnel. A list of personnel authorized to access the same will be maintained, which will be approved by Head of IT.
- A physical access log will be maintained for recording access to the backup storage locations. This will be reviewed on a periodic basis by Head of IT.
- Backup media will be stored in an environment that is adequately protected from fire, dust and humidity, magnetic interference etc.

## Tape Storage

1. All backup tapes are to be labeled using a bar-coding system and include the following information:

- Job Name
- Creation Date and Time
- Backup Type (Incremental, Differential or Full)

2. Daily backups will be performed on starting Sunday through Saturday. These tapes will be stored onsite in tape library during the following backup cycle. (Refer to Section Age of the Tape Backup Retention).
3. A weekly backup will be performed and the backup set will be stored onsite in the tape library during the following backup cycle. At the end of the latter cycle, the weekly tape will be removed to a predetermined onsite location for storage to a maximum of 11 weeks. When this 11 week period has elapsed, the tapes will be brought back on site for reuse.
4. Monthly backup will be performed at the last weekend of the month or the first week of the next month. The tape are removed from the library and handed over to Information Security Department.
5. Yearly backup will be performed at the first week of the New Year. The tapes are removed and handed over to Head of IT Security Department.

## Age of Tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than two years shall be discarded, destroyed and replaced with new tapes.

## Media and Restoration Management

The IT team will maintain an up to date inventory of all backup media within the organization. This will include details such as Media identification, Data contents, Physical location, Start date of usage, number of tape writes etc.

All backup media will be clearly labelled and classified to ensure that they are easily identifiable and maintain the organization's information classification policy.

The IT team will carry out a physical verification of the media inventory at least every six months. Media due for disposal will be identified in advance and a report will be generated for the same, which will be circulated to the respective system owners for approval.

All backup media will be disposed off in a secure manner at the end of their life. It will be ensured that:

- The media is properly degaussed;
- Labels/tags containing reference to the organization internal information are removed;
- Tapes and other non-reusable data storage media are physically destroyed.

The IT team will ensure that all backup media is checked for readability and data restorability. Data on backup media will be restored at least once in every 6 months to verify the recoverability of data.

## Testing and Restoring

The ultimate goal of any backup process is to ensure a restorable copy of data exists on the backup tapes or backup media. As a result, it's essential to regularly restore the data from backup tapes or backup media. Full restore will be performed according to the annual restore plan. IT Team plans which will be reviewed by Information Security Officer.

## Data will be restored if

- There is a compromise of the system / device
- Files have been corrupted, deleted, or incorrectly modified but try to recover.
- The Information to be accessed is located in an archive backup

## In the event a data restore is desired or required, the following policy will be adhered to:

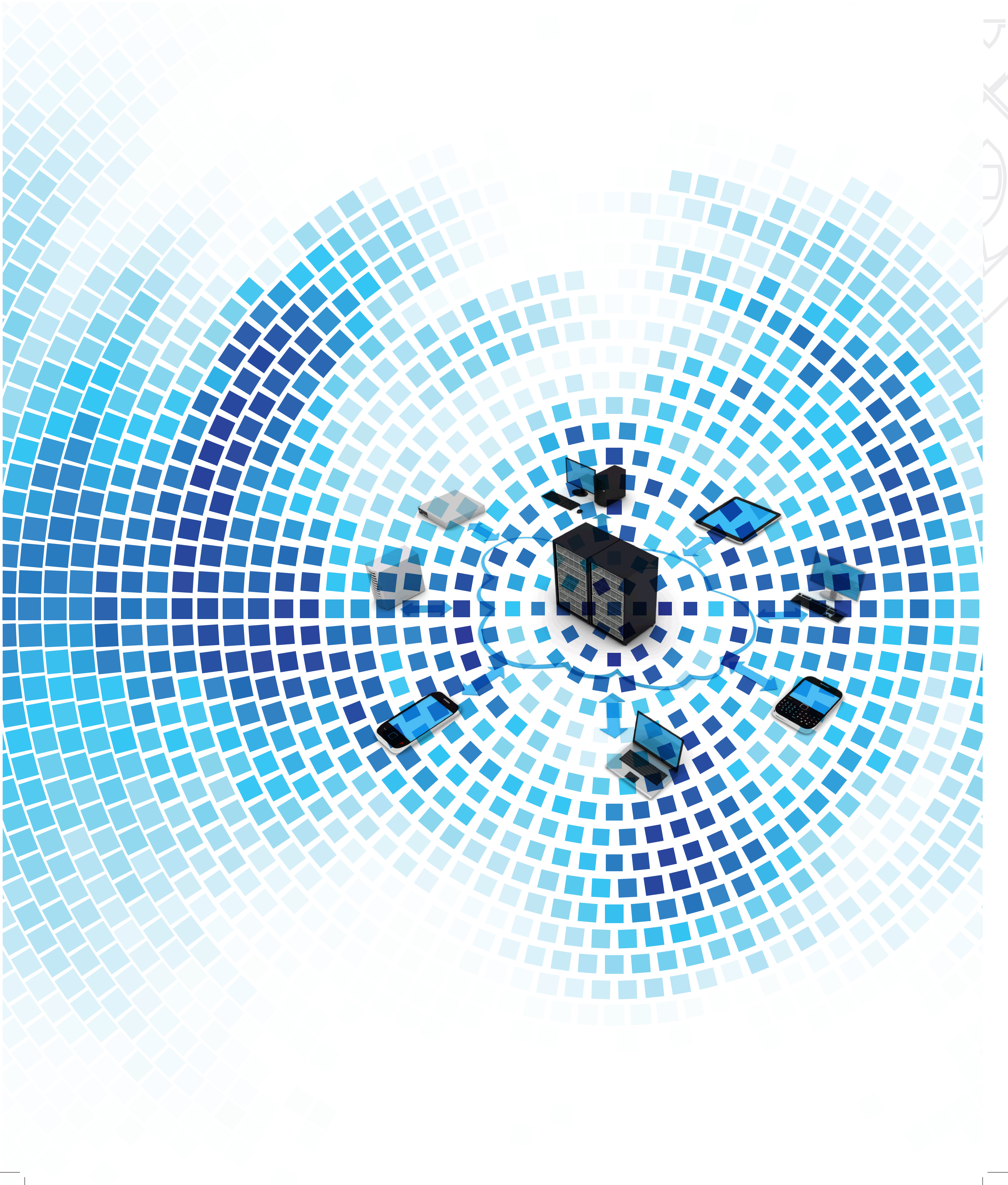
1. An approval is need for any restoring for each System/Device.
2. If a user has a restore request, he must contact Head of IT Security.
3. In the event of natural disaster, consult applications specific recovery documents for full restoration procedures.
4. In the event of a local data loss due to human error, the affected end user may contact the Technology and Innovation Department as defined above and request a data

## restore. The end user must provide the following information:

- Name of file(s) and/or folder(s) affected.
- Last known location of files(s) and/or folder(s) affected.
- Extent and nature of data loss.
- Events leading to data loss, including last modified date and time (if known).
- Depending on the extent of data loss, a daily tape, weekly tape, or combination of both will need to be used. The timing in the cycle will dictate whether or not these tapes are onsite or offsite.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.



# 3.10 Remote Access Policy

## Objective

### The objectives of this policy are to

- Define standards for connecting to the organization's network from any remote host.
- Minimize the potential exposure to the organization from damages which may result from unauthorized use of its resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, VPN, SSH, etc.

### User Responsibilities

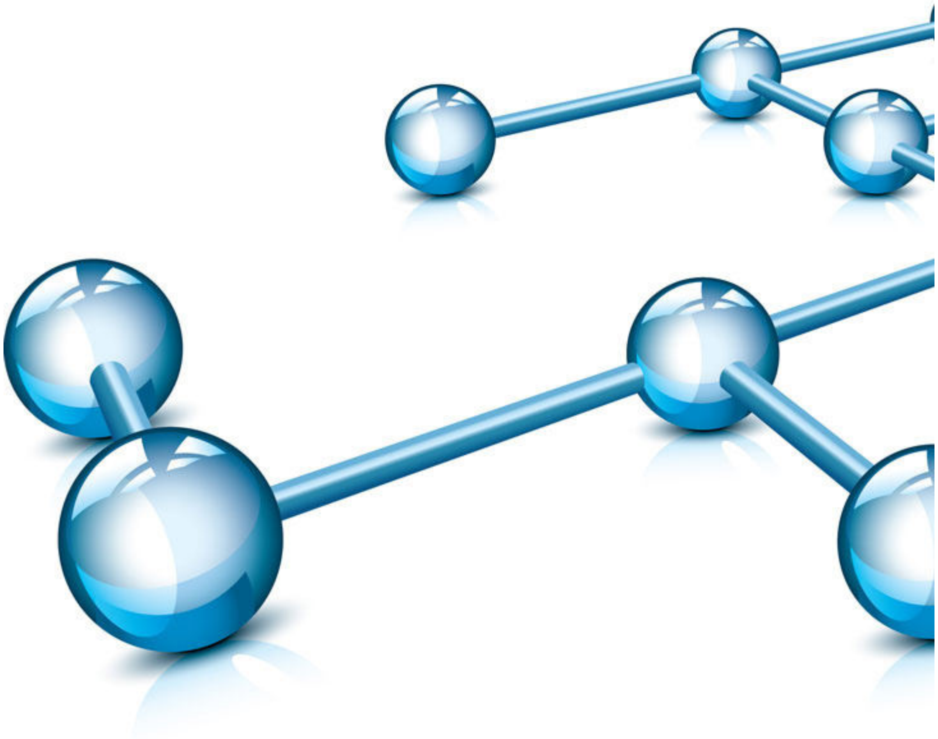
- It is the responsibility of the users with remote access privileges to the corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the organization.
- The user is responsible to ensure no one violates any of the organizations policies, does not perform illegal activities, and does not use the access for outside business interests when accessing the corporate network remotely. The user bears responsibility for the consequences should the access be misused.
- Users with remote access privileges must ensure that their organization-owned or personal computer or workstation, which is remotely connected to organization's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- At no time should any user provide their login or email password to anyone, not even family members.
- Users with remote access privileges to the organization's corporate network must not use non-corporate email accounts (i.e., Hotmail, Yahoo, AOL, etc), or other external resources to conduct the organization's business, thereby ensuring that official business is never confused with personal business.
- Personal equipment that is used to connect to the corporate networks must meet the requirements of the organization-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard remote access solutions to the organization's production network must obtain prior approval from the information security team.
- All hosts that are connected to the corporate network via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
- User must approach the organization and its information security team to approved non-standard hardware configurations for access to hardware.
- Routers for dedicated ISDN lines configured for access to the corporate network must meet minimum authentication requirements of CHAP.

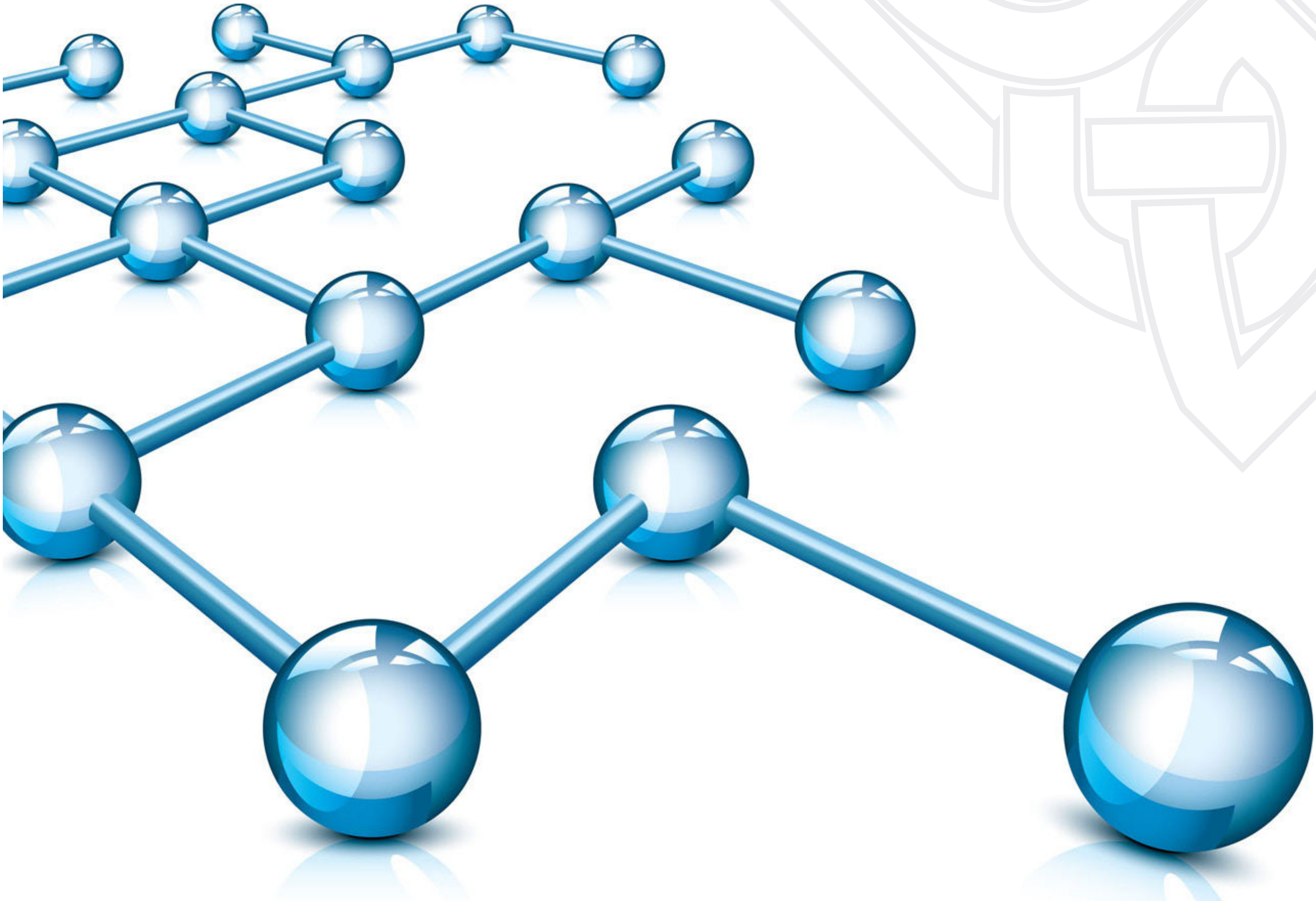
## Information Security Team Responsibilities

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.
- Pass-phrases must be changed periodically.
- The availability of accounting mechanism to ensure tracking the usage of the corporate network resources.
- Ensuring only authorized access is permitted.
- Remote access must only be permitted to users complying with Anti-Virus Policy.
- Remote Access must only be granted through the encryption mechanism approved by the information security team.
- Split-tunneling must not be permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.





# 3.11 Wireless Communication Policy

## Objective

The purpose of this policy is to secure and protect the information assets owned by the organization. The organization provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. It grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the corporate network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the information security team are approved for connectivity to the corporate network.

### Statements

All wireless infrastructure devices that reside at the organization site and connect to its network, or provide access to information classified as Internal Use Only, Company Confidential or Strictly Confidential must:

- Abide by the standards must comply with Wireless Device Requirements section below.
- Be installed, supported, and maintained by an approved support team.
- Use organization's approved authentication protocols and infrastructure.
- Use organization's approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.
- VPN tunnel must be enabled.

All lab wireless infrastructure devices that provide access to organization's Internal Use Only, Company Confidential or Strictly Confidential information must abide by the Wireless Devices Requirements section below. Lab and isolated wireless devices that do not provide general network connectivity to the organization's network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity).
- Have a different service set identifier name than the user's service set identifier name.

- Not interfere with wireless access deployments maintained by other support organizations.

## Wireless Device Requirements

Wireless infrastructure devices that provide direct access to corporate network must:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK or WPA2-PSK). It also must use Advanced Encryption System (AES) with minimum of 128-bit key length.
- Be long (at least 20 characters) with complex character combinations.
- Be configured to disable the broadcast of the Service Set Identifier (SSID).
- Be configured to change the default SSID name.
- Be configured to change the default login username and password.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the corporate network. Access to the corporate network through this device must use standard remote access authentication.
Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

WiFi
zone

# 3.12 Mobile Phone Policy

## Objective

This is a policy that applies to employees, temps, freelancers and contractors working for the organization and any subsidiaries or service providers under contract and is issued under the authority of the Head of IT Security. It describes the rules covering use of mobile computing devices that can be attached to organization Networks, or containing organization Information. This includes, but is not restricted to, Personal Digital Assistants (PDA's), tablets, and Smartphones.

## Scope

As technology and business demand moves forward, there has been an introduction of many devices that can be classed as Portable Media. The organization allows usage of these devices as part of normal business processes. However, care needs to be taken over their use, and of the data that they hold. Information Processing Equipment, Internet, Intranet and e-mail access provided by the organization is intended primarily for organization business use, but limited access for Personal Use is allowed.

## Statement

All organization supplied mobile devices and their contents remain the property of the corporation and are subject to regular audit and monitoring. These devices should only be connected to a laptop or desktop that has been approved for use at the organization.

Users must be aware that the device contains organization data, and take appropriate action to protect the device from being lost or stolen. Only devices which have been built to organization published standards and/or from approved suppliers, should be attached to the organization data network either directly or through an organization (owned or leased) PC or laptop.

This should ensure that appropriate security controls have been built into the implementation. Once received, the user is not authorized to change any security device settings without reference to the service desk, as they may affect the security of the device, or stop it functioning with the supplied service. (This does not apply to resetting the PIN) In certain business situations there is a need to attach non-organization owned devices. Only devices that do not directly attach to the organization data network can be authorized (i.e. only devices that connect to a organization desktop or laptop PC, via infrared, Bluetooth or USB – this is restricted to a few PDA's and smart phones). Devices eligible for this dispensation are limited to smart phones, blackberry or PDA's that are currently on the organization authorized hardware list. These devices must have their security settings (such as passwords) configured as per the requirements detailed in this document.

Only applications provided with the device, or provided/approved by the organization can be run. If the information you carry has been classified as organization Confidential, then this information should not be carried on mobile devices unless it is encrypted (where this facility is available on the device, where it is not, the user must consider carefully before allowing it to be stored on the device). Blackberries will potentially receive confidential information via e-mail, this is recognized and dispensator until an encrypted solution is available.

## Guidelines:

- No changes to the security settings or configuration of any approved device can be made without prior authorization from Head of IT Security.
- Never attempt to use an unapproved device, via any method of communication, with any IT equipment that belongs to the organization.
- Personal mobile phones with cameras and personal digital cameras are permitted in the office but must not be used to collect and store data that belongs to the organization.
- Specific points on the use of Blackberry devices
- The pin-2-pin option is not permitted from or to organization owned or operated devices.
- The Blackberry web client is configured to use the organization internet provision, so is permitted.
- The Blackberry Desktop re-director software is not permitted, the only route for mail to reach the Blackberry is to use the organization provided BES service (this ensures appropriate security settings are correctly applied).
- organization Blackberry devices should not be attached to non-organization owned laptops or desktop PC's

## Specific points on the use of Camera Phones

- Phones enabled with cameras should primarily be used for taking business related pictures. However, some limited personal use is allowed, but storage must not interfere with organization Business use.
- Inappropriate content prohibition applies to mobile phones as it does other forms of communication.
- Information should be downloaded to a secure device (organization Laptop for example) and removed from the phone at the users' earliest opportunity.
- Privacy, only take pictures of individuals with their permission to do so, or follow current policy where this is impractical.

## Specific points on the use of non-organization owned devices

- Only devices currently supported as purchased organization devices are supported. If the device requires special software to be incorporated onto the desktop, this is not allowed.
- The permission to attach non organization devices is prior arranged by job function and division through the Infrastructure Team

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

SECURITY

# 13 Disposable of Media Policy

The data stored on hard and floppy disks, and other storage media such as tape must be protected when these media, or equipment containing them, are no longer required or do not function.

## Objective

All such storage media will be physically or magnetically destroyed permanently before disposal. This will be performed by Information Security Officer, or by official agents on their behalf. In the case of an external company being used to destroy media on a large scale, then "certificates of secure destruction", must be obtained. In the event of magnetic media being taken off-site by third contractors, these contractors must be bound by a confidentiality agreement.

Where the equipment or media are to be used again by other staff or outside the organization a secure overwriting of previous data must be performed.  All items disposed of (whether sold/removed/destroyed) must be documented accordingly by recording the asset numbers in the IT hardware asset inventory.

**The disposal of IT equipment should be authorized by the Head of IT Security.**

### Secure Disposal of Confidential Paper Products

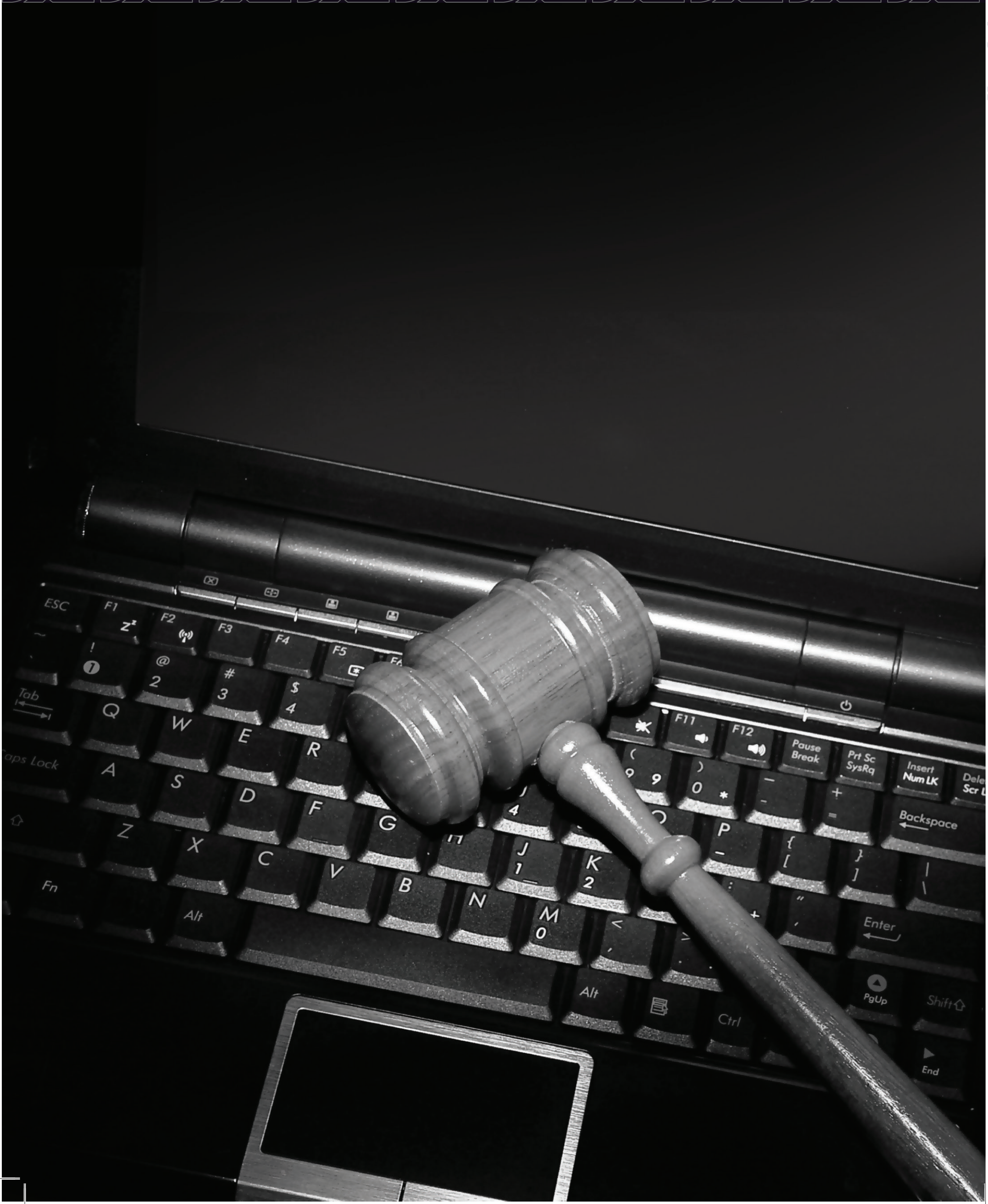
Confidential waste paper products shall be stored separately from ordinary paper waste for recycling and kept for the minimum period necessary.  All such waste must be cross-shredded before removal from Organization premises. The confidential waste shall only be removed by authorized persons. Confidential waste should be securely stored and not left in corridors or outside awaiting removal. Confidential waste shall not be used for any other purpose either before or after it has been shredded, for example, as scrap paper or packing material.

### Secure Disposal of Digital Storage Media

Any digital storage media to be disposed of must be securely wiped. In addition, they need to be physically damaged beyond repair.

### Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.



# 3.14 Visitor Premises Policy

## Objective

This policy is intended to be applied on visitors who physically access the organization's premises and sponsoring employees. All visitors must be accompanied by an employee at all times. Related documents will need to be applied accordingly.

### Disclosure of Information

- Visitors must not request for information out of the scope of their visit.
- Visitors must sign the approved Non-Disclosure Undertaking (NDU). This document gives the organization the right to investigate the carried bags or electronic devices.

### Parking

- Visitors, using their own vehicles, must park the vehicle on specific visitor/guest parking area.

### Checking In

- Visitors must enter the premises from the main entrance.
- A government-issued photo identification document must be presented upon checking in.
- The sponsoring employee must be present during the check-in process.
- Only authorized employees of this organization can sponsor visitors.
- Visitors are not allowed to carry any equipment without an authorization.

### Visitor Badges

- Visitors badges must be visibly worn at all time during the visit.
- Employees must report any person within the premises not wearing a badge.

### Privileged Access

- For visits that require accessing privileged areas, such as network or telephone room, the access must be authorized beforehand.
- Visitor needs to be accompanied by authorized employee.
- Access details must be documented (visitor's name, designation, company, entrance time, exist time and purpose).

### Photography and Videography

- Visitors are prohibited to take photographs or record videos.

### Checking Out

- Visitors must return to the access point they entered from.

### Exit Inspection

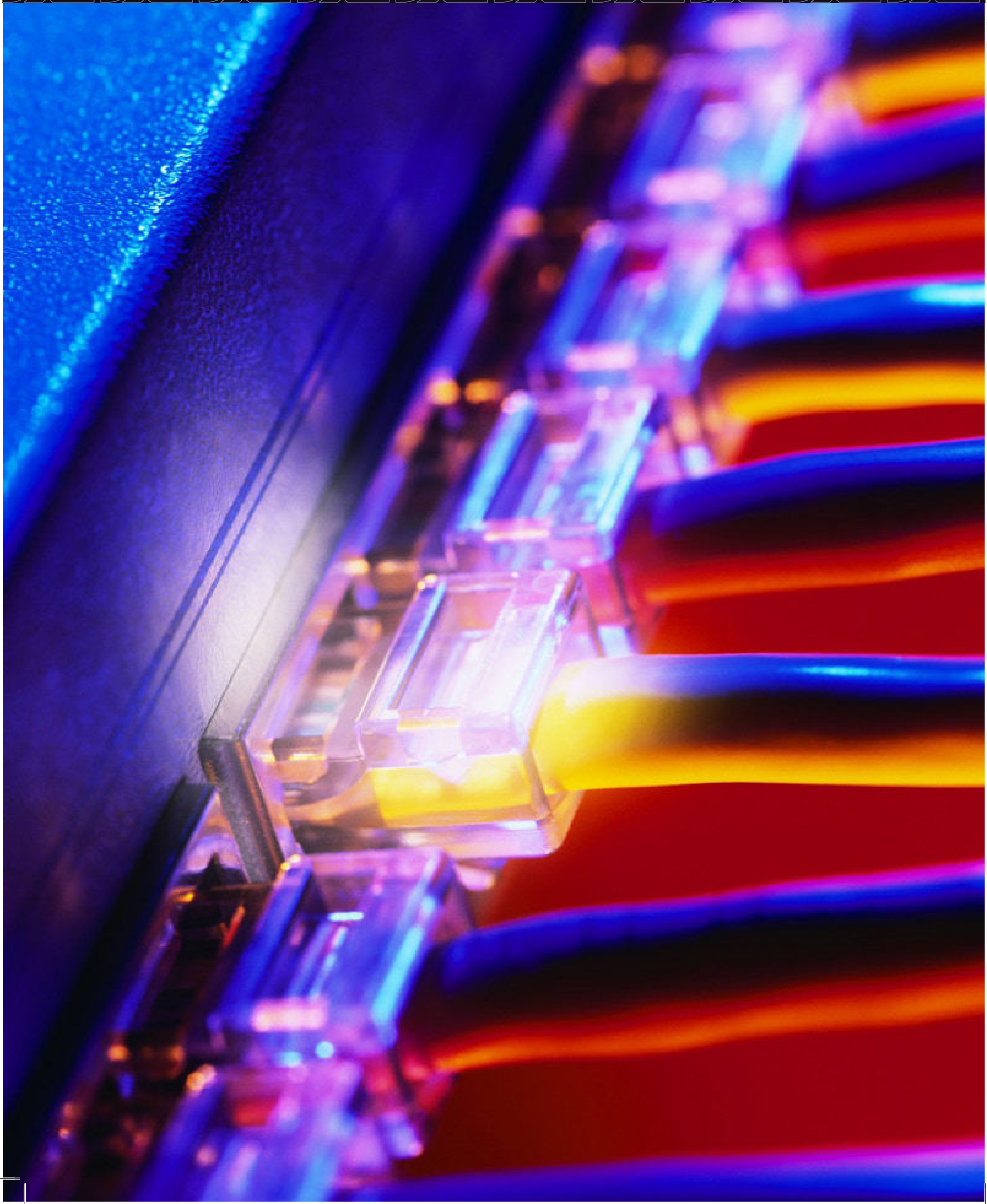
- Bags and electronic devices of visitors may be subject to investigation.

### Emergency Evacuation

- In case of emergency evacuation, the sponsoring employee is responsible for making sure that the visitor reaches and remains in the evacuation assembly area.

### Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.



# 3.15 Physical Access for Data Center Policy

## Objective

The objective of this policy is to establish rules for accessing the datacenter and the disaster recovery site.

### Controlling the Access

- All doors of the data centre shall be closed at all times. Access mechanism shall be in place.
- Any access to the data centre shall be logged (in and out, accessing ID, reasons, authorized by whom). In addition, all accompanying persons shall be listed.
- Authorization and approval to access the datacenter shall be provided by the operations staff in either email or paper.
- Any non organization staff accessing the datacenter shall be accompanied by authorized employees from organization at all time.
- Visitors are not allowed to bring in any bags, phones or computer, except they have a written permission. The written permission shall contain whom they intend to visit and the reason for that visit. That is as well valid for any maintenance person. Permissions shall be approved from operations staff in either email or paper.
- Special provisions shall be made to guarantee access to the datacenter in case of emergencies.

### Monitoring the Access (will be implemented in the new premises)

- Any access and activity inside the datacenter shall be recorded.
- CCTV shall be working and recording all motions in the datacenter.
- Windows to the datacenter have to be clear all the time, to be able to watch the people inside the datacenter.

### Logging the Access

- Every instance of access from anybody shall be logged. In addition, all accompanying persons shall be listed.

### Audit and Review

- Access rights to the data centre shall be reviewed twice a year by the Information Security Officer of organization.

The access to the disaster recovery site shall be controlled in exactly the same as the access to the data centre.

# 3.16 Patch Management Policy

## Objective

All operating systems and applications need regular patching to ensure their continued security and reliability. If patches are not applied in time, this might permit hackers to compromise a computer, which, in turn, threatens all computers and networks connected to it.. Therefore, any computer equipment that runs an operating system or application and is connected to the organization network shall have up-to-date security patches applied.

### Statements

The following requirements apply to all server, desktop, handheld, and laptop computers inside the organization network:

- Scheduled vulnerability assessments shall be performed by organization security quality service team and according to the results system patching shall be performed by organization IT infrastructure team.
- All servers, desktop, and laptop systems, including all hardware and software components, shall be accurately listed in the organization asset inventory to aid in patching efforts.

In addition to the scanning, the IS Officer shall regularly check the Web for newly released information about vulnerabilities. This shall include using the information sent by organization alerting solution.

- The system security engineer shall assess each vulnerability alert prior to taking any action in order to avoid unnecessary patching.
- The decision to apply a patch, and within what timeframe, shall be done as presented in the patch priority matrix below.
- All patches shall be downloaded from the relevant vendors or other trusted sources. Each patch's source shall be authenticated and the integrity of the patch verified. All patches are submitted to an anti-virus scan upon download.
- New servers and desktops shall be fully patched upon coming online by the IT infrastructure team and deployed in order to limit the introduction of risk.
- The IT team shall develop a list of vendors whose patches are trusted and are applied without test. All other patches shall be tested prior to implementation. A server should be designated to serve as a test bed for newly released patches with a test period of below matrix before issuing live patches to the production network.
- A rollback plan that allows safe restoration of systems to their pre-patch state is devised prior to any patch rollout in the event that the patch has unforeseen effects.

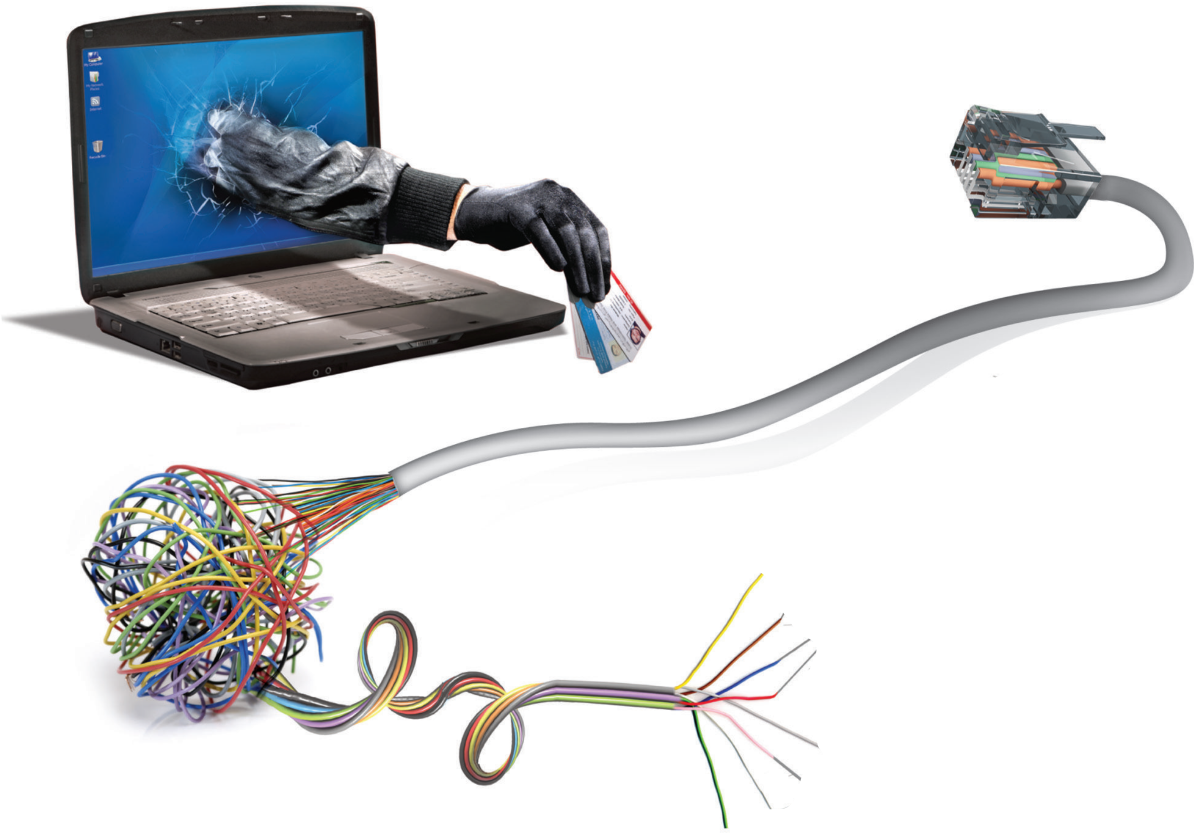
## Patching Priorities

The following patch priority matrix represents all systems at organization, their relative priority for vulnerability patching, and timeframes within which patches must be applied (i.e., twenty-four (24) hours, forty-eight (48) hours, seven (7) days, or thirty (30) days).

| System | Criticality | High Priority Patch | Moderate Priority Patch | Low Priority Patch |
|---|---|---|---|---|
| Workstations/Laptops | Medium | 48 Hours | 7 Days | 30 Days |
| DNS/ Domain Controller | High | 24 Hours | 72 Hours | 7 Days |
| Servers providing web services | High | 24 Hours | 72 Hours | 7 Days |
| Mail Servers | High | 24 Hours | 72 Hours | 7 Days |
| Antivirus server | High | 24 Hours | 72 Hours | 7 Days |
| Network appliances | High | 24 Hours | 72 Hours | 7 Days |
| Servers for service desk and shared folder | High | 24 Hours | 72 Hours | 7 Days |
| Other servers & appliances | Medium | 48 Hours | 7 Hours | 30 Days |

## Audit and Review

The information security team may conduct review on a regular basis to ensure that all patches are carried correctly.



# 3.17 Physical Access for Operation Center Policy

## Objective

The purpose of this policy is to establish rules for accessing the Operation Center.

### Controlling the Access

- Operation Center, all doors, must be closed at all times. Access mechanism should be in place.
- Every access from everyone should be logged (In and Out, ID, Reasons, authorized by whom). In addition to the log of the access control mechanism all persons must be listed who accompanied the authorized person.
- Authorization and approval to access the Operation Center should be provided by the Head of IT Security in either email or paper.
- Everyone accessing the Operation Center must be accompanied by authorized persons from organization at all time.
- Visitors are not allowed to bring in bags or computer, except they have a written permission. The written permission must contain as well, who to visit and for what reason, that is as well valid for any maintenance person. Permission must be approved from operations staff in either email or paper.

### Monitoring the Access

- Every access and activity inside the Operation Center should be recorded at the main door
- CCTV must be working and recording all motions in datacenter.

### Logging the Access

- Every instance of access from everyone should be logged. In addition to the log of the access control mechanism all persons must be listed who accompanied the authorized person.

### Audit and Review

Access rights to the Operation Center will be reviewed twice a year by the Information Security Officer of organization.

# 3.18 Change Management Policy

## Objective

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly and to avoid disruption to service provision and business continuity  Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

### Statements

- Every change to an organization Information Resources resource such as: operating systems, computing hardware, networks, and applications are subject to the Change Management Policy and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the Head of IT Security.
- The IS organization Board will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- A formal written change request must be submitted to the Head of IT Security for all changes, both scheduled and unscheduled.
- All scheduled change requests must be submitted in accordance with change management procedures so that the Head of IT Security has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- Each scheduled change request must receive formal Head of IT Security approval before proceeding with the change.
- The IS-Board of the Change Management may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate blackout plans, the timing of the change will negatively impact a key business process, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- User's notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
- Date of submission and date of change
- Owner and custodian contact information
- Nature of the change
- Indication of success or failure

All organization information systems must comply with an Information Resources change management process that meets the standards outlined above.

## Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of organization Information Resources access privileges, civil, and criminal prosecution. Military are subjected to martial law.

## Terms and Complaisance

- The organization network is owned and controlled by organization-IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.

- The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

# 3.19 User Access Management Policy

## Objective

The purpose of this policy is to prevent unauthorized access to the information systems and to ensure the availability of information for authorized users. The policy describes the registration and de-registration process for all information systems and services.

### New Users

Access to applications, databases, network, email and servers are controlled through a formal user registration process beginning with a formal notification from HR (for employees) and department heads (for temporary engagements) Each user is assigned a unique user ID in order for users to be identified and held accountable for their activities. The use of shared IDs is only permitted where they are suitable for the work carried out (i.e. Training). Based on the user's department management request, users will be provided with standard IT services (e.g. access to email, internet, shared folders, applications, remote access & network services).

A request for service must be submitted by (email or hard copy) by the newcomer's line manager or by HR. Login credentials will be only handed to the users, on the first day of their joining. IT will maintain a record of all New Users requests on the service desk. Users will be granted privileges on the basis of their job responsibilities and roles.

### Change of User Requirements

Changes in user access may be triggered by their respective line management and shall be implemented by the IT infrastructure team. . Requests must be submitted by (electronically) and must be directed to the infrastructure team in advance to avoid any disruption to service provision due to unavailability of data to an authorized employee Changes will be made on receipt of a properly completed request, the same details as shown above are required and requests will be filed on the service desk.

The Information Security Officer will not normally be copied in on requests but must be consulted if the request is not for a standard network service.

### Change of Password

Where a user has forgotten his/her password, the infrastructure team is authorized to reset the password after having the confirmation of the user's authenticity. Users which fail to authenticate themselves will have to consult the Infrastructure Team.

### Password Reset procedure

**Upon receipt of such a request the Infrastructure Team will**

1. Ensure the request is logged.
2. Issue a temporary, single use, password where the user will be require entering a new password upon his next login
3. Infrastructure Team will close the ticket and notifying the user of the same

### Removal of Users

Infrastructure Team will disable user's access to all services as soon as Infrastructure Team is notified either by Standard exit process (Final Clearance Form) or through HR. Infrastructure Team will file this in the Service Desk. Infrastructure Team is also responsible for reviewing all user access rights every month in organization domain controller. Infrastructure Team will coordinate with respective owner at the applications in order to disable user's access on applications. Infrastructure Team will move leaver's Flat files and mail boxes to pre-determined storage for the period of two month after which the data will be archived off from the system (but can be recovered if required).

## User Password Management

Passwords shall comply with the organization Password Policy. Temporary access may be granted on a need to use basis. Such logons may be granted by the Information Security Officer but must be recorded and reported on the normal form. Temporary logons must be identified by a specific login (starting T-****) and must have an expiry date.

## Audit and Review

The Information Security Officer will institute a review of all network access rights at least twice a year, which is designed to positively confirm all users.

Any lapsed or unwanted logons, which are identified, shall be disabled.

Twice a year, the Information Security Officer will institute a review of 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 disabled.

The review will be conducted as follows.

- The Information Security Officer 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 authorized to use the system.

- The Information Security Officer will ensure a response.

- Any user unconfirmed access shall be disabled.

- The Head of IT Security will maintain a file of:

    - Application owner signed responses for all the requirements
    - A record of action taken by providing access to the applications and  systems

# 3.20 Information Security and Business Continuity Incident Management Policy

## Objective

Information security and business continuity incident handling represents a key step in the ISMS (Information Security Management System) and BCMS (Business Continuity Management System) process. The purpose of this Policy is to assist in the prevention of security incidents, limit the damage if an incident occurs, awareness of information security related issues and to improve the organization IT process to serve the business effectively at organization. This policy also addresses the handling of incidents that might cause a business continuity situation. The Incident Management Policy applies to all the users of organization.

### Information Security Incident Practices

a. It is the responsibility of all staff of organization to promptly report information security incidents as defined in this policy.

b. The Incident Handling Team within organization shall be responsible for overseeing the incident handling processes at organization.

### Business Continuity Incident Practices

a. It is the responsibility of all staff of organization to promptly report business continuity incidents to the Business Continuity Manager by phone or email.

b. If the Business Continuity Manager is unavailable, all business continuity incidents shall be reported to the Deputy Business Continuity Manager by phone or email

c. This role includes:

- Focal point for incident reporting
- Managing the incident and activating business continuity plans, as required
- Taking control of the situation
- Containing the incident
- Communication with stakeholders

### Information Security Incident Handling

a. The incident handling team shall serve as a focal point in organization for computer security incident reporting and response and shall promote international standards and practices.

b. The incident handling team shall Handle computer security incident reports and provide assistance in recovery actions.

c. All Security Incidents shall be prioritized based on the Criticality of the affected assets, Current and potential technical effect of the incident.

d. A Security Incident Response Procedure shall be defined within organization with the steps to be followed in case an incident occurs.

e. Escalation Procedure shall be defined to escalate the incident to management and relevant parties to ensure that important decisions are promptly taken.

f. Procedures shall be developed, documented and updated to record any security breach, whether accidental or deliberate.

g. Whenever a Security breach occurs each incident shall be:

   I. Logged;

   II. Assigned for follow-up;

   III. Analyzed;

   IV. Recommendation made in respect of prevention;

   V. Closed out

h. Incident Handling Team shall be responsible for auditing the incidents on periodic basis and ensure that preventative action/process is in place to address such further incidents.

i. Incident Handling Team shall ensure that adequate details relating to software malfunctions (Security related malfunctions) are recorded and the actions to be followed are implemented.

j. Security review and audit of all IT systems shall be conducted on a regular basis to promptly identify any possible security loopholes and/or areas of improvement to the system.

k. Appropriate disciplinary action against individuals who caused the incident shall be conducted.

### Business Continuity Incident Handling

a. The Business Continuity Manager is responsible for handling all business continuity incidents.

b. The Business Continuity Manager is responsible for ensuring that personal safety takes priority.

c. Upon receiving notification of or observing an incident, the Business Continuity Manager shall:

- Take action to verify all details that have been reported;
- Evaluate this information against the criteria for activation of the business continuity plan;
- Notify emergency contacts and apply appropriate information dissemination;
- Ensure safe site evacuation, if required;
- Mobilize safety, first aid or evacuation-assistance teams;
- Identify root causes of the event;
- Limit the damage of the business continuity event;
- Management of media contact;
- Collect information, logs, reports etc. about the incident, as much as possible;
- Close the incident;
- Review incident logs at least once per month to identify trends and avoid re-occurrence.

d. The Business Continuity Manager shall ensure awareness of employees and compliance with the Business Continuity Strategy and the Business Continuity Plan.

## Audit and Review

a) The Incident Manager owns this plan and is responsible for its update.

b) Incident Handling Team is responsible for

i. Maintaining this policy and advising on information security controls.

ii. Closing the all security incidents.

iii. Implement the identified improvement areas from the Incident analysis.

iv. Informing the business continuity manager about any incidents that have the potential of causing business disruption.

v. Acting as a focal point for reporting information security related incidents.

c) **Infrastructure Team** is responsible for building, configuring, operating and maintaining magic desk to report incidents.

d) **Business Continuity Manager** acts as a focal point for reporting business continuity related incidents.

e) **All relevant employees** are responsible for complying with this policy. This policy also applies to third party employees, vendors and contractor/agents.

f) **Internal Audit** is authorized to assess compliance with this policy.

# 3.21 Acceptable Use of IT Equipment Policy

## Objective

The purpose of this policy is to outline the acceptable use of organization computing equipment / IT Business service and IT infrastructure services at organization. These rules are in place to protect the employee and organization Business services. Inappropriate use exposes organization to risks including virus attacks, compromise of network systems and services, and legal issues.

The intentions for publishing the IT Acceptable Use Policy are not to impose restrictions that are contrary to organization but to establish a culture of openness, trust and integrity. Organization is committed to protecting organization's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

## Scope

This policy applies to employees, vendors, consultants, internees, and other workers at organization, including all personnel affiliated with third parties. This policy applies to all equipment / IT Services that is owned or leased by organization in accordance with Desktop and Laptop Usage Policy .

## Acceptable Use and Ownership

1. Users shall report any suspicious activity observed on organization's Information systems to the Incident Handling Team immediately.
2. Organization Information Security Officer reserves the right to check networks and systems on a periodic basis to ensure compliance with IT Support Policy as well as this policy.
3. Desktop/server computing resources shall not be used to compromise, harm, destroy, or modify any other services or resources either internally or external services.
4. Software installations on the desktop/laptop computers shall be in compliance with the enlisting approved and supported software and services.
5. Operating System and Applications must be continuously updated with latest patches / service packs. Computers should not be shut down after working hours to allow IT to update overnight, the users' computers with necessary security patches, service packs and antivirus definitions.
6. Only authorized personnel shall have access to information stored on Intranet servers and shared folders.
7. Classified data and files shall be maintained in accordance with Information Classification and Control Policy.
8. The removal of property including data, hardware or software shall with the relevant custodian authorization and as per Secure Asset – Media Disposal Policy.
9. Email received from unknown senders, with or without attachment shall not be opened and employees shall take assistance from Incident Handling Team.

## Handling Proprietary, Confidential and Private Information

Organization has classified its information as defined in the Information Classification and Control Policy, that includes but is not limited to company private, competitor sensitive or research data, corporate strategies, trade secrets, specifications and customer lists. Organization would like to ensure the safeguard of its information assets at all times and that employees will take all necessary steps to prevent unauthorized access to this information

1. Authorized users are responsible for the security of their passwords and accounts.
2. All PCs, laptops and servers should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes.
3. Because information contained on portable computers is vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
4. Users should observe the organization Email Acceptable Use Policy when using corporate email postings unless posting is in the course of business duties.
5. All computers used by the employee that are connected to the organization Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database as per Malicious Code and Antivirus Policy.
6. Personal laptops or computing devices will not be connected to organization local wired or wireless network. These instead can be plugged to Guest wireless network only.

## Data Storage Policy

Data Storage Policy has been established in order to preserve the finite amount of storage space available on network servers. This policy is designed to curtail the increasing use of company server space for unauthorized, non-business-related files.

## Appropriate File for Storage

1. Files that directly pertain to the business of organization may be saved on a server. These include most business files created through the use of organization approved and installed software.
2. Inappropriate files include non-business-related MP3s, GIF files, games, executables, vbs files, and any other employee-installed software not approved by the organization. Not only do such files consume valuable server space, but they can also introduce damaging viruses into the network.
3. Attempts will be made to block the storage of all non-business-related files. If such files are detected on the server, users will be asked to remove them immediately.

## Storage Space Allocation

1. Each employee of organization will be allotted a minimum of 1 Gigabytes for their home directory. Some employees will be granted more space if demanded by their job function. Requests for more server storage space must be made to the organization employees.
2. Alerts will be sent to all employees who are close to exceeding their server space quota. If an employee exceeds their server space quota, they will be unable to save files until sufficient allocated space is freed in order to accommodate them. If an employee needs support in freeing storage space, he or she may contact the Infrastructure Team.

## Tips for Conserving Storage Space

It is the responsibility of every employee to ensure that they use their server storage space allocation wisely. Each employee should set aside time on a monthly basis to ensure that they remain within their space quota. Identify, remove and/or archive items that are:

- Outdated, such as preliminary draft versions of current documents;
- Out-of-use or orphaned files;
- Duplicated files; and
- Non-business related or non-critical files.

## Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

# 3.22 Clear Desk and Clear Screen Policy

## Objective

The purpose for this policy is to establish a culture of security and trust for all employees at organization. An effective clean desk effort involving the participation and support of all organization employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.

### The main reasons for a clean desk policy are:

- A clean desk can produce a positive image when our customers visit the company.
- It reduces the threat of a security incident as confidential information will be locked away when unattended.
- Sensitive documents left in the open can be stolen by a malicious entity.

### Scope

At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.

At the end of the working day the employee is expected to tidy their desk and to put away all office papers. Organization provides locking desks and filing cabinets for this purpose.

### Statements

a. Always clear your workspace before leaving for longer periods of time.

b. If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shred bin.

c. Consider scanning paper items and filing them electronically in your workstation.

d. Use the recycling bins for sensitive documents when they are no longer needed.

e. Lock your desk and filing cabinets at the end of the day

f. Lock away portable computing devices such as laptops or Mobile phones

g. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

# 3.23 Data Centre Document Management Policy

## Objective

This Data Centre Document Management Policy is an internal Infrastructure Team Policy and defines the requirements for documentation and document management. This Policy defines the storage location of all the documents related to Data Centre. To ensure that documents are placed in the right location. This Policy should complement disaster management, change management and recovery by ensuring that documentation is available in any incident or task.

### Statements

All the documents related to Data Centre should be stored outside the Data Centre, so in case of any disaster inside Data Centre documents can be recovered. The documents which should be stored are:

### The network structure diagram including:

1. IP addresses of all devices on the network with static IP addresses.
2. The locations and IP addresses of all hubs, switches, routers, and firewalls on the network
3. All subnets on the network and their relationships including the range of IP addresses on all subnets and net mask information
4. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices

### Configuration information on all network devices including:

1. Switches
2. Routers
3. Firewalls

### Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.

LOGIN

# 3.24 Log Management Policy

## Objective

Logs are records of events that occur within the information systems of an organization. Virtually every system, service, application and device in the Enterprise has built in logging capabilities. Originally log data was used to troubleshoot systems; but as systems and business requirements evolved, so did logging capabilities and log analysis. In today's Enterprise, logs are an invaluable resource used to optimize systems and networks, establish baselines, perform audits and assist with regulatory compliance.

System logs for operating systems and services, such as authentication, file and print, Citrix, DNS, email, and so forth, generate detailed information about their activity. Application logs have the ability to generate an audit trail of past transactions with time stamps, user names and object access details. Most network gear, such as firewalls, routers, switches, and so forth, have the ability to generate log data about their activity. Change management logs document all changes made to technologies within the Enterprise. Other types of logs, such as surveillance or physical access logs provide detailed physical access audit trails. Each of these logs sources are an integral part of their respective administrators' jobs because the collection and analysis of the log data is one of their responsibilities.

In conjunction with the appropriate tools and procedures, audit trails can validate individual accountability, a way to reconstruct events, detect intrusions, identify problems and demonstrate regulatory compliance. The need to audit individual accountability, reconstruct events, detect intrusions, identify problems and demonstrate regulatory compliance emphasizes the need for organizations to develop an effective log management strategy to generate, analyze, store and dispose of log data.

## Scope

This policy applies to all organization systems, network, databases and applications used to establish and support a production environment.

This policy as well provides a corporate policy framework to govern management decisions on whether a particular log should either be:

1. Retained – and if so in what format, and for how long; or
2. Disposed of - and if so when and by which method.

## Statements

The Head of IT Security shall implement and maintain a central log management system (LMS) that includes receiving, storing, analyzing, and disposing of computer log data. This LMS will:

1. Create and maintain a secure log management infrastructure by balancing system performance, storage resources, and legal requirements;
2. Commit resources to perform timely log review to identify and analysis access, change monitoring, malfunction, resource utilization, security events and user activity;
3. Identify roles and responsibilities of staff associated with this process;
4. Develop standards, procedures, and guidelines as needed to support this program;
5. Make the system available for applications that need log management and analysis

capabilities.

6. The system should log: User ID, Dates and times of logon and logoff, terminal identity (if possible) and Network address (if possible), unsuccessful system or data access attempts (if possible), System alerts or failures or other significant events as appropriate.
7. Special treatment should be performed for administrator, developer, super-user or other privileged access.

## Log Retention

Log retention has to be done according to legal requirements and targets, guidelines and security policies from organization.

In the course of running different services on the server's lot of logs are collected, like Web Logs, Email Logs, System Services Logs, Applications Logs and Security Logs. These logs can take many different formats e.g. Text, Word, Excel and Notepad Files, Email Format.

Many of the above documents can be retained as 'hard' paper records or in electronic form. Retention of specific documents may be necessary to:

1. Fulfill statutory or other regulatory requirements.
2. Evidence events/agreements in the case of disputes.
3. Meet operational needs.
4. Ensure the preservation of logs of historic or other value.
5. The premature destruction of documents could cause organization.
6. Operational problems.
7. Embarrassment.
8. Failure to comply with the Data Protection Acts (once officially published).

Conversely, the permanent retention of all logs is undesirable, and appropriate disposal is to be encouraged for the following reasons:

1. There is a shortage of storage space.
2. Disposal of existing logs can free up space for more productive activities.
3. Indefinite retention of personal data may be unlawful.
4. Reduction of fire risk (in the case of paper records).

## Retention and Protocol

1. Logs should be enabled for Operating Systems, Applications, Firewall, Switches and other devices in the data centre as defined in the log management policy.
2. Logs should be saved locally on the devices, logs are collected for the period of one week, after which logs will be transferred to centralized network storage.
3. The entire log should be reviewed by log mining tools for any malicious activity or at least manually once a year
4. The retention period for the logs should be 1 years
5. After the completion of retention period logs should be disposed securely
6. Head of IT Security is responsible to handle all the issues related to logs
7. Log can be used for the performance issues for the servers, applications, firewall, router or other devices.

8. Deletion should be done with the approval of Head of IT Security Department, where computer files are concerned
9. Physical destruction on site (paper records - shredding)
10. Migration of document to external body should be done in case of log retention for log period

## Audit and Review

The Head of IT Security shall have the responsibility and authority to cause this policy to be implemented and maintained.

## Head of IT Security

- Ensure that all aspects of this policy are implemented and operational in all relevant system components
- Periodically reviews all relevant activities as mentioned in the policy
- Assists the Head of IT Security in reconciling audit trail anomalies, the logs should be reviewed by Head of IT Security every Quarter

## Incident Handling Team

- Periodically monitors and reports all issues to Head of IT Security and Infrastructure Team all relevant activities
- Assists the Head of IT Security in reconciling audit trail anomalies, the logs should be reviewed by Head of IT Security every Quarter
- Reports security breaches or anomalies to the Head of IT Security and Infrastructure Team on monthly basis
- Will coordinate with Information Security Officer for incident reports or update.

## Information Security Officer

- Prepare and maintain policy guidelines on monitoring and audit trail recording, protecting, reviewing and reporting

# 3.25 Physical Access for organization office Policy

## Objective

The objective of this policy is to establish rules for accessing the organization offices. This policy applies for the organization offices.

## Statements

### Controlling the Access

- Offices main door must be closed at all times. Access mechanism must be activated.
- Individual Offices must be locked after leaving for breaks or vacations or after working hours.

### Monitoring/logging the Access

- Every access to the offices from outsiders, e.g. visitors, or other departments must be recorded at the main door.
- Every access from everyone should be logged. In addition to the log of the access control mechanism all persons must be listed who accompanied the authorized person.
- Visitors with cameras or combined devices are not allowed to access.
- Visitors are not allowed to bring in bags or computer, except they have a written permission. The written permission must contain as well, who to visit and for what reason.
- CCTV must be working and recording all motions in organization offices.
- Approvals and permissions are given by Head of Operations.

### Access to Operation Center

- Main door must be closed all times
- Visitors with cameras or combined devices are not allowed to access.
- Logging
- Windows should be secured and back rooms closed
- Access rights to Operation Center will be reviewed twice a year by security officer

### Audit and Review

The information security team may conduct review on a regular basis to ensure the policy is enforced.