IT POLICIES

AND

PROCEDURES

Document Number	ITNOCP01
Date	2/06/24
Revision No	2.1
Information Classification	Internal

`

Revision: 2.1

Issue Status: A

Prepared by	Designation
Ejilson.N	IT -Manager
Approved by	**Designation**
Walter Aceituno	Chief Information Security Officer

TABLE OF CONTENTS

1.0 IT ACCESS CONTROL POLICY

Purpose

Access to SYSTECH SOLUTIONS PVT LTD computing resources is granted in a manner that carefully balances restrictions designed to prevent unauthorized access against the need to provide unhindered access to informational assets.

Scope

All assets identified under the ownership of IT Department are included under IT Assets Control Policy.

Responsibility

IT Manager

Access Control

SYSTECH SOLUTIONS PVT LTD will provide all employees and other users with the information they need in order to carry out their responsibilities in an effective and efficient manner as possible. Access to Confidential Information would be limited to authorized persons determined by a approval process, as per the job responsibilities and subjected to applicable laws and regulations.

Procedure

1. **New Employees**: Access is requested by HR Manager for establishment of a unique account thro' email. The IT Manager shall create an account for the particular User and furnish the User ID and Password as per the privileges identified by the HR Manager or by the roles & responsibilities of the User.

2. **Existing Employees**: Access is requested by the Department Manager for establishment of a unique account in order to access information or information processing facilities at SYSTECH SOLUTIONS PVT LTD . The IT Manager shall create an account as per the privilege identified in the email. The

Department Manager shall ensure to provide the requirements and identify the purpose for which the User shall have access to the information or information processing facilities.

3. **Third Party or Vendors**: Access is requested by the Department Manager through filling the Extranet Request Form to the IT Manager and with a copy to LEADER/ISC and the representative of the Top Management. LEADER/ISC shall provide with the possible level of risk that needs control measures and approval is sent. Based on the comments of the LEADER/ISC, the top management representative shall approve the request form. The IT Manager shall proceed to establish the unique account which shall be regularly reviewed and audited by the IT Manager on the appropriate usage. The Department Manager shall take responsibility for ensuring that the Vendor/Third Party utilizes the account for the purpose assigned therein.

Exceptions

1. This policy excludes stand-alone personal computers, public access computers or related resources, and those areas where individual employee accounts are not required.
2. This policy for the IT Access Control is applicable to new Vendors or Third Party identified by the SYSTECH SOLUTIONS PVT LTD with effect from[Commencement DATE]. The access and privileges given to the existing third party or vendors shall be reviewed and audited at regular intervals, unless the Top Management decides to rule out the exemption.

Best Practices

- All Users authorized to access information or information processing facilities are expected to become familiar with and abide by SYSTECH SOLUTIONS PVT LTD policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. All users will have access to expectations, knowledge, and skills related to information security.
- Every User must maintain the confidentiality of information assets, even if technical security mechanisms fail or are absent. Users electing to place information on digital media or storage

devices or maintaining a separate database are responsible for ensuring that security, confidentiality, and integrity are maintained in accordance with this Policy.

- Users shall maintain reasonable steps to protect the confidentiality of the information.
- Users shall ensure not to divulge or provide access to any other third parties without the prior written permission of SYSTECH SOLUTIONS PVT LTD .
- Users are obligated to report instances of non-compliance.
- IT Manager shall regularly conduct review on the usage of the account by the respective User/s and report any instances of incident.

Definitions

- **Access** is defined as the ability and means necessary to store data in, to retrieve data from, to communicate with, or to make use of any resource of a system.
- **Confidential Information:** All information that is generally confidential in nature. For instance, the term includes Information in the nature of proprietary, intellectual property, client related and trade secrets, those are unknown to the general public.
- **Authorized Persons** are defined as people who have established a need and received the necessary authorization. Persons must be a member of the management or staff or other individuals sponsored by the SYSTECH SOLUTIONS PVT LTD.
- **Informational Processing Facilities** include computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services at SYSTECH SOLUTIONS PVT LTD .

2.0 CLEAN DESK AND CLEAR SCREEN POLICY

Purpose

The main reasons for a clean desk policy are:

- A clean desk can produce a positive image when our customers visit the SYSTECH SOLUTIONS PVT LTD.
- 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. SYSTECH SOLUTIONS PVT LTD provides locking desks and filing cabinets for this purpose.

Applicability

This Policy guideline applies to all SYSTECH SOLUTIONS PVT LTD employees, including directors, officers and agents, consultant or contractors, who collect, generate, use or otherwise handle Confidential or Internal Use information.

Guidelines

- Users must “log off” their computers when their workspace is unattended.
- Users must lock their computer (Ctrl + Alt + Delete), when they leave their workspace
- Users must “shut down” their computers at the end of the workday.
- All Confidential and Internal Use information must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.
- File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.

- Keys used to access locked drawers or rooms containing Confidential or Internal Use information must not be left at an unattended work area.
- Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday.
- Passwords must not be posted on or under a computer or in any other accessible location.
- Copies of documents containing Confidential or Internal Use information must be immediately removed from printers.
- Documents containing Confidential of Internal Use information must be immediately removed from facsimile machines.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Such breaches are considered incidents which shall be reported to any member of the Information Security Team or their hierarchical managers.

3.0 IT ASSET CONTROL POLICY

Summary

All employees and personnel having access to organizational computer systems must adhere to the IT asset control policy in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. This policy is defined to assist the IT department in tracking and protecting their assets include safe disposal.

Purpose

To protect organizational resources on the network

Scope

IT assets

Responsibility

IT Manager

Policy

A. Assets

This defines the assets that are covered under this policy and the extent to which they are tracked and protected.

1. Types

The IT assets categorized for implementing this policy are:

a. Desktop workstations;

b. Laptops;

c. Mobile PDA's or Phones;

d. Printer, Scanner and Fax Machine;

e. Servers;

f. Firewall;

g. Routers;

h. Switches;

i. Bridges;

j. Memory devices, including backup tapes;

k. Tape drives; and

l. Any other hardware or software or firmware devices used in the operation of day-to-day business of SYSTECH SOLUTIONS PVT LTD.

B. Assets Tracked

Regardless of costs, all IT assets of SYSTECH SOLUTIONS PVT LTD. shall be tracked, especially assets holding data. For this purpose, the assets could include:

a. Hard drives;

b. Temporary Storage drives;

c. Tapes with data stored on them including backup data;

d. Data stored on hard drives on the work stations.

Measures to be taken to effectively secure the data stored on any hard devices before disposed to third party vendor for secure storage or destruction or for maintenance. Any devices authorized and approved by the IT Manager shall be allowed and tracked and it is the User's responsibility to handle the SYSTECH SOLUTIONS PVT LTD's assets in a responsible manner.

1. Asset tracking requirement

a. All assets will have an Asset ID

b. To maintain an asset inventory list called "Asset Register."

c. The Asset Register shall also identify the asset owner who shall be individually responsible for handling of assets.

d. To identify other information such as manufacturer ID, its location.

e. When any new asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

f. Any request for transfer of asset ownership shall be mailed and suitable changes to be identified in the Asset Register.

C. Asset Transfer

1. Requirements

This procedure applies to all requests made under B (1) (f) of this Policy and shall be implemented accordingly:

a. Any asset type listed under this policy is transferred to a new location, then such request shall formally made thro' a checklist identified by the Requestor. The template used shall be "Asset Transfer Checklist."

b. Any request as per C (1) (a) shall be approved by the authorized representative of the organization.

For this purpose, the authorized representative shall be identified as:

1. Any request by User level, the authorized representative shall be the respective Process Owners;

2. Any request by Process Owners or departmental heads, the authorized representative approving the request shall be IT Manager

3. Any request by IT Manager or management groups shall be approved by the Chief Technology Officer or Head - IT

c. The request as per C (1) (a) shall contain the following requirements:

a. Asset Type;

b. ID Number;

c. Asset Name;

d. Date of Request;

e. Current Location;

f. Present User;

g. New Location;

h. New User;

i. Locations of Sensitive Data;

j. Remarks (if any)

k. Requester Signature;

   i. In the event of a hard copy, the Owner of the Asset shall maintain the signature appended copy for any reference;

   ii. When a request is made through email communication, the Owner of the Asset shall seek approval through email.

   iii. However, the Asset Transfer check list will be duly filled and reference to Email date of Request and Approval shall be filled in respectively in the document. The document shall be retained in a soft copy at a retrievable location by the Owner.

l. Authorized Representative Signature

d. The authorized representative as defined under C (1) (b) shall approve them by appending his signature or through email to the Asset Transfer Checklist.

e. Upon effective implementation, the email shall be copied to the IT Manager, who shall be responsible for entering the information's in the Asset Register within one week of implementation.

f. Regular reviews shall be conducted by the IT Manager to periodically check for assets that were recently moved or added to the Asset Register and maintain any incidents that are reported to the Information Incident Response Team.

2. Applicability

This policy applies to any assets transferred under C (1), including, but not limited to:

1. New assets purchased; or
2. Assets relocated either within or outside their present location; or
3. Changes of Owners or Users as per privileges; or
4. Changes of Owners or Users due to employment termination; or
5. Asset disposal.

D. Asset Disposal

1. Requirements

This procedure applies to all requests made under C (2) (5) of this policy and shall be implemented accordingly:

a. Removal of sensitive data prior to disposal;

b. Assessment shall be conducted by the authorized owner on the sensitivity level of the information in the asset.

c. Approval to be sought from the authorized representative who shall authorize such disposal.

Sensitivity of the data shall be determined on the basis of following categorization:

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.

2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Privileged) - The data must be erased using an approved technology to make sure it is not readable using special high technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:

    1. Memory stick;
    2. CD ROM disk;
    3. Storage tape;
    4. Hard drive;
    5. RAM memory; and/or
    6. ROM memory or ROM memory devices.

2. Disposal Procedure

The methods approved for use at SYSTECH SOLUTIONS PVT LTD. are two of those identified as “effective removal methods”: wiping and destruction.

- **Wiping:** is the process of writing data over the hard drive, such that any data stored on the drive are overwritten by the new data and may not be retrieved. Wiping may be carried out at SYSTECH SOLUTIONS PVT LTD. or at the premises of a third party service provider approved by the management.

- **Destruction:** is the physical demolition of the data storage media to render it unusable. “Destroy” is defined as “to disintegrate, incinerate, pulverize, shred, or melt the equipment.” The following specific techniques are required for specific media:

    - Hard disk drives, flash drives, memory cards – strike with a heavy object until the drive is verified inoperable. Scraping away recording media with a sharp object on hard disk platters is an acceptable alternative.
    - CDs, DVDs, floppy disks, data tapes – shred or break into multiple pieces.

3. Applicability

This procedure applies to all assets that are owned by SYSTECH SOLUTIONS PVT LTD.

E. Media Use

1. Requirement

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

1. Floppy disk
2. Memory stick
3. CD ROM disk
4. Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

1. Unclassified - Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
2. Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
3. Confidential - The data may only be removed from secure areas with permission of a Vice -president or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
4. Secret - - The data may only be removed from secure areas with the permission of the President or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
5. Top secret - The data may never be removed from secure areas.

Disposal of media shall be implemented according to D (2) of this Policy.

2. Applicability

This procedure applies to all assets that are owned by SYSTECH SOLUTIONS PVT LTD.

F. Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

4.0 EMAIL SECURITY/ACCEPTABLE USE POLICY

Overview

Email is perhaps the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via email. Email is not inherently secure, particularly outside our own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues.

Scope

This policy defines and distinguishes acceptable/appropriate use of email from unacceptable/inappropriate use of electronic email.

Applicability

This is a standard corporate policy that applies throughout the organization as part of the corporate governance framework. It applies to all users of the corporate email systems.

Policy Axioms (Guiding Principles)

A. Email users are responsible for avoiding practices that could compromise information security.

B. Corporate email services are provided to serve operational and administrative purposes in connection with the business only. All emails including group email ID and distribution lists processed by the corporate IT systems and networks are considered to be the organization's property.

Detailed Policy Requirements

1. Do not use email:

- To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;
- To create, send, forward or store emails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public *i.e.* sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
- To commit the organization to a third party for example through purchase or sales contracts, job offers or price quotations, unless you are explicitly authorized by management to do so (principally staff within Administration and HR). Do not interfere with or remove the standard corporate email disclaimer automatically appended to outbound emails;
- For private or charity work unconnected with the organization's legitimate business;
- In ways that could be interpreted as representing or being official public statements on behalf of the organization, *unless* you are a spokesperson explicitly authorized by management to make such statements;
- To send a message from anyone else's account or in their name (including the use of false 'from:' addresses). If authorized by the manager, a secretary may send email on the manager's behalf but should sign the email in their own name *per pro* ('for and on behalf of') the manager;
- To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, color, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;
- For any other illegal, unethical or unauthorized purpose.

2. Apply your professional discretion when using email, for example abiding by the generally accepted rules of email etiquette. Review emails carefully before sending, especially formal communications with external parties.
3. Do not unnecessarily disclose potentially sensitive information in "out of office" messages.
4. Emails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Technically, the scanning process is not 100%

effective to scan compressed and encrypted attachments. Deleting such mails from the Inbox and reporting them as security incidents to the IT Helpdesk or the Departmental Manager.

5. Attachments to the email (unless permitted and authorized by management) shall not exceed above 4 MB in size.
6. Except when specifically authorized by management or where necessary for IT system administration purposes, employees must not intercept, divert, modify, delete, save or disclose emails.
7. Limited personal use of the corporate email systems is permitted at the discretion of local management *provided* always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees. SYSTECH SOLUTIONS PVT LTD. reserves the right to monitor message without prior notice.
8. Do not use Gmail, Hotmail, Yahoo or similar external/third-party email services (commonly known as "web-mail") for business purposes. Do not forward or auto-forward corporate email to external/third party email systems. [You may access your own web-mail via corporate IT facilities at local management discretion provided that such personal use is strictly limited and is not considered private (see previous statement)].
9. Any mails related to virus/malware warnings, or mass mailings on security front shall be controlled and sent only after prior approval of the IT Manager. These restrictions also apply to the forwarding of mail received either from internal source/external source by SYSTECH SOLUTIONS PVT LTD. employees.

Responsibilities

All employees of SYSTECH SOLUTIONS PVT LTD. shall have no expectation of privacy in anything they store, send or receive on the SYSTECH SOLUTIONS PVT LTD's email system.

I. **Information Security Team members are** responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

II. **IT Department** is responsible for building, configuring, operating and maintaining the corporate email facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy.

III. **IT Help Desk** is responsible for assisting users with secure use of email facilities, and acts as a focal point for reporting email security incidents.

IV. **All relevant employees** are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (*e.g.* by contractual terms and conditions) or implicitly bound (*e.g.* by generally held standards of acceptable behavior) to comply with our information security policies.

V. **Internal Audit** is authorized to assess compliance with this and other corporate policies at any time.

Enforcement

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

5.0 INFORMATION CLASSIFICATION POLICY

Purpose

SYSTECH SOLUTIONS PVT LTD. provides fast, efficient, and cost-effective electronic services for a variety of clients worldwide. As an industry leader, it is critical for SYSTECH SOLUTIONS PVT LTD. to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, SYSTECH SOLUTIONS PVT LTD. has adopted this information classification policy to help manage and protect its information assets.

Scope

SYSTECH SOLUTIONS PVT LTD. and its associates (i.e. includes affiliates, third party, vendors, and outsourcing partners) share in the responsibility for ensuring that organization's information assets receive an appropriate level of protection by observing this policy.

Responsibility

- Department Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. ('Owners" have approved management responsibility. 'Owners' do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All SYSTECH SOLUTIONS PVT LTD associates shall be guided by the information category in their security-related handling of SYSTECH SOLUTIONS PVT LTD information.

Policy

All SYSTECH SOLUTIONS PVT LTD information and all information entrusted to SYSTECH SOLUTIONS PVT LTD from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity.

Information Category	Description

Public	Information is not confidential and can be made public without any implications for SYSTECH SOLUTIONS PVT LTD. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.
Internal	Information is restricted to internal access within management approved departments and protected from external access. Unauthorized access could influence SYSTECH SOLUTIONS PVT LTD's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.
Confidential	Information received from clients or produced within the SYSTECH SOLUTIONS PVT LTD accessible to a restricted department or members in any form for processing in production by SYSTECH SOLUTIONS PVT LTD. The original copy of such information must not be changed in any way without written permission from the owner (either Client or the SYSTECH SOLUTIONS PVT LTD). The highest possible levels of integrity, confidentiality, and restricted availability are vital.
Classified	Information with a "Top Management Only" visibility. Example: Business Plan

6.0 INFORMATION SECURITY RISK ASSESSMENT POLICY

Purpose

To allow IT Manager or Departmental Manager or any designated security officer to perform periodic information security risk assessments (RA) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope

Risk assessments can be conducted on any entity within SYSTECH SOLUTIONS PVT LTD. or any outside entity that has signed a Third Party Agreement with SYSTECH SOLUTIONS PVT LTD. Risk Assessment can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy

The execution, development and implementation of remediation programs are the joint responsibility of the IT Department and respective process or domains for which the systems are being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with other departments including the Information Security Team in the development of a remediation plan.

Risk Assessment Process

Enforcement

Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

Definitions

Term	Explanation
Entity	Any business unit, department, group, or third party, internal or external to SYSTECH SOLUTIONS PVT LTD., responsible for maintaining SYSTECH SOLUTIONS PVT LTD. assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of SYSTECH SOLUTIONS PVT LTD.'s key information assets and systems. The Risk Assessment Team is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets on SYSTECH SOLUTIONS PVT LTD. networks, while minimizing the impact of security procedures and policies upon business missions.

7.0 LAPTOP SECURITY POLICY

Purpose

This policy describes the controls necessary to minimize information security risks affecting SYSTECH SOLUTIONS PVT LTD. laptops.

Scope

This policy refers to certain other/general information security policies, but the specific information given here is directly relevant to laptops and, in case of conflict, takes precedence over other policies.

Applicability

- All SYSTECH SOLUTIONS PVT LTD. computer systems face information security risks. Laptops and desktops are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside SYSTECH SOLUTIONS PVT LTD.'s premises increases the threats from people who do not work for the SYSTECH SOLUTIONS PVT LTD. and may not have its interests at heart.

- Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

- Do not forget that the impacts of such breaches include not just the replacement value of the hardware, but also the value of any SYSTECH SOLUTIONS PVT LTD. data on them, or accessible through them. Information is a vital SYSTECH SOLUTIONS PVT LTD. asset. We depend very heavily on our computer systems to provide complete and accurate business information when and where we need it. The impacts of unauthorized access to or modification of, important and/or sensitive SYSTECH SOLUTIONS PVT LTD. data can far outweigh the cost of the equipment itself.

Guidelines on Physical Security

- The physical security of 'your' laptop is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.
- Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
- If you have to leave the laptop temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.
- Lock the laptop preferably in a strong filing cabinet or safe, when you are not using it. This applies irrespective of whether they are used at home or office or in a hotel. **Never** leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box, but it is generally much safer to take it with you.
- Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about! Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.
- Keep a note of the make, model, serial number and the SYSTECH SOLUTIONS PVT LTD. asset label of your laptop, but do not keep this information with the laptop. If it is lost or stolen, notify the Police or concerned authority immediately and inform the IT Help Desk as soon as practicable (within hours not days, Please).

Virus protection for laptops

- Viruses are a major threat to SYSTECH SOLUTIONS PVT LTD. and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software MUST be updated at least monthly or on a regularly basis by the IT Department. The easiest way of doing this is simply to log on to the SYSTECH SOLUTIONS PVT LTD. network for the automatic update process to run. If you cannot

log on for some reason, contact the IT Help Desk for advice on obtaining and installing anti-virus updates.

- Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.
- Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically but the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.
- Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimise the damage
- Respond immediately to any virus warning message on your computer, or if you suspect a virus (*e.g*. by unusual file activity) by contacting the IT Help/Service Desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.
- Be especially careful to virus-scan your system before you send or receive any files outside the SYSTECH SOLUTIONS PVT LTD. This includes EMAIL attachments and CD-ROMs that you create.

Controls against unauthorized access to laptop data

- You must use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure. Contact the IT Help Desk for further information on laptop encryption. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.
- You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.
- Corporate laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.
- Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

Other controls for laptops

- **Unauthorized software**

Do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the SYSTECH SOLUTIONS PVT LTD. networks as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (*e.g*. PC anywhere) and 'hacking tools' (*e.g*. network sniffers and password crackers) are explicitly forbidden on SYSTECH SOLUTIONS PVT LTD. equipment unless they have been explicitly pre-authorized by management for legitimate business purposes.

- **Unlicensed software**

Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a licensed payment. Individuals and companies are being prosecuted for infringing software copyright: DO NOT RISK by bringing yourself and SYSTECH SOLUTIONS PVT LTD. into disrepute by breaking the law.

- **Backups**

Unlike desktop PCs which are backed up automatically by IT, you must take your own backups of data on your laptop. The simplest way to do this is to logon and upload a data from the laptop to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks *etc*. **Make sure that off-line backups are encrypted and physically secured.** Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of heartache and extra work.

- **Laws, regulations and policies**

  You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet).

- **Inappropriate materials**

  Be sensible! SYSTECH SOLUTIONS PVT LTD. will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call IT Help Desk to check your spam settings.

- **Health and safety aspects of using laptops**

  Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Balancing the laptop on your knees hardly helps the situation! Limit the amount of time you spend using your laptop. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you tend to use the laptop in an office most of the time, you are advised to use a 'docking station' with a full-sized keyboard, a normal mouse and a display permanently mounted at the correct height. Stop using the portable and consult Health and Safety for assistance if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the portable.

8.0 INFORMATION SECURITY POLICY ON OUTSOURCING

Objective

This policy specifies controls to reduce the information security risks associated with outsourcing.

Scope

The policy applies throughout SYSTECH SOLUTIONS PVT LTD. for any service that is expected from outsourcing providers (also known as “outsourcers”) include:

- hardware and software support and maintenance staff;
- external consultants and contractors;
- IT or business process outsourcing firms;
- Temporary staff.

The policy addresses the following controls found in the ISO/IEC 27002:2005 and ISO/IEC 27001 standards:

- A. 6.2.1 Identification of risks related to external parties
- A. 6.2.2 Addressing security when dealing with customers
- A. 6.2.3 Addressing security in third party agreements

Exception

The list of approved vendors prior to the implementation of this Policy shall not be subjected to procedural formalities, except having a Confidentiality Agreement executed.

Policy Axioms

- The commercial benefits of outsourcing non-core business functions must be balanced against the commercial and information security risks.

- The risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural and managerial controls.

Procedure

- **Selection of an Outsourcer**

Criteria for selecting an outsourcer shall be defined and documented, taking into account the:

- SYSTECH SOLUTIONS PVT LTD's reputation and history;
- quality of services provided to other customers;
- number and competence of staff and managers;
- financial stability of the SYSTECH SOLUTIONS PVT LTD and commercial record;
- retention rates of the SYSTECH SOLUTIONS PVT LTD's employees;
- Quality assurance and security management standards currently followed by the SYSTECH SOLUTIONS PVT LTD (*e.g*. certified compliance with ISO 9000 and ISO/IEC 27001).

Further, information security criteria may be defined as the result of the risk assessment.

- **Assessing outsourcing risks**

Management shall nominate a suitable SYSTECH SOLUTIONS PVT LTD. owner for each business function/process outsourced. The owner, with help from the local Information Risk Management Team, shall assess the risks before the function/process is outsourced, using SYSTECH SOLUTIONS PVT LTD.'s standard risk assessment processes.

In relation to outsourcing, specifically, the risk assessment shall take due account of the:

- ✓ nature of logical and physical access to SYSTECH SOLUTIONS PVT LTD. information assets and facilities required by the outsourcer to fulfill the contract;
- ✓ sensitivity, volume and value of any information assets involved;

- ✓ commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to SYSTECH SOLUTIONS PVT LTD.'s competitors where this might create conflicts of interest; *and*
- ✓ Security and commercial controls known to be currently employed by SYSTECH SOLUTIONS PVT LTD. and/or by the outsourcer.

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. LEADER shall present the results of the risk assessment to the Management for strategy decisions without violating the business policy and legal requirements. Management shall decide if SYSTECH SOLUTIONS PVT LTD. will benefit overall by outsourcing the function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (*e.g*. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

- ➢ **Contracts and confidentiality agreements**

A formal contract between SYSTECH SOLUTIONS PVT LTD. and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing. If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between SYSTECH SOLUTIONS PVT LTD. and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).

a. Information shall be classified and controlled in according with SYSTECH SOLUTIONS PVT LTD. policy.

b. Any information received by SYSTECH SOLUTIONS PVT LTD. from the outsourcer who is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.
c. Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.
d. All contracts shall be submitted to the Legal for accurate content, language and presentation.
e. The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided (e.g. defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract, such as:

- Legal, regulatory and other third party obligations such as data protection/privacy laws, money laundering *etc.*[*];
- Information security obligations and controls *such as:*
  - Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001;
  - Background checks on employees or third parties working on the contract;
  - Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities *etc.*;
  - Information security incident management procedures including mandatory incident reporting;
  - Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
  - Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed in the course of the contract;
  - Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
  - Anti-malware, anti-spam and similar controls;
  - IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks;
- The right of SYSTECH SOLUTIONS PVT LTD. to monitor all access to and use of SYSTECH SOLUTIONS PVT LTD. facilities, networks, systems *etc.*, and to audit the outsourcer's compliance with the contract, or to employ a mutually agreed independent third party auditor for this purpose;

* In the case of "offshore" outsourcing, special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy and similar laws may conflict. Take qualified legal advice as a matter of course.

- Business continuity arrangements including crisis and incident management, resilience, backups and IT Disaster Recovery.

Although outsourcers that are certified compliant with ISO/IEC 27001 can be presumed to have an effective Information Security Management System in place, it may still be necessary for SYSTECH SOLUTIONS PVT LTD. to verify security controls that are essential to address SYSTECH SOLUTIONS PVT LTD.'s specific security requirements, typically by auditing them.

- **Hiring and training of employees**

Outsource employees, contractors and consultants working on behalf of SYSTECH SOLUTIONS PVT LTD. shall be subjected to background checks equivalent to those performed on SYSTECH SOLUTIONS PVT LTD. employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):

- Proof of the person's identity (*e.g*. passport);
- Proof of their academic qualifications (*e.g*. certificates);
- Proof of their work experience (*e.g*. résumé/CV and references);
- Criminal record check;
- Credit check.

Companies providing contractors/consultants directly to SYSTECH SOLUTIONS PVT LTD. or to outsourcers used by SYSTECH SOLUTIONS PVT LTD. shall perform at least the same standard of background checks as those indicated above.

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

- **Access controls**

In order to prevent unauthorized access to SYSTECH SOLUTIONS PVT LTD.'s information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design suitable controls architecture.

✓ **Technical access controls shall include:**

- User identification and authentication;
- Authorization of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls;
- Data encryption in accordance with SYSTECH SOLUTIONS PVT LTD.'s encryption policies and standards defining algorithms, key lengths, key management and escrow *etc*.
- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

Procedural components of access controls shall be documented within procedures, guidelines and related documents and incorporated into awareness, training and educational activities. This includes:

- Choice of strong passwords;
- Determining and configuring appropriate logical access rights;
- Reviewing and if necessary revising access controls to maintain compliance with requirements

✓ **Physical access controls shall include:**

- Layered controls covering perimeter and internal barriers;
- Strongly-constructed facilities;
- Suitable locks with key management procedures;
- Access logging though the use of automated key cards, visitor registers *etc.*;
- Intruder alarms/alerts and response procedures;

If parts of SYSTECH SOLUTIONS PVT LTD.'s IT infrastructure are to be hosted at a third party data centre, the data centre operator shall ensure that SYSTECH SOLUTIONS PVT LTD.'s assets are both physically and logically isolated from other systems.

SYSTECH SOLUTIONS PVT LTD. shall ensure that all information assets handed over to the outsourcer during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

- **Security audits**

- If SYSTECH SOLUTIONS PVT LTD. has outsourced a business function to an outsourcer based at a different location, it shall audit the outsourcer's physical premises periodically for compliance to SYSTECH SOLUTIONS PVT LTD.'s security policies, ensuring that it meets the requirements defined in the contract.
- The audit shall also take into consideration the service levels (if any) agreed in the contract, determining whether they have been met consistently and reviewing the controls necessary to correct any discrepancies.
- The frequency of audit shall be determined by management on advice from functions such as Internal Audit, Information Security Management and Legal.

Responsibilities

- **Management**

  - Management is responsible for designating suitable owners of business processes that are outsourced, overseeing the outsourcing activities and ensuring that this policy is followed.
  - Management is responsible for mandating commercial or security controls to manage the risks arising from outsourcing.

- **Outsourced Business Process Owners**

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

- **Information Security Team**

  - Members of Information Security Management System at SYSTECH SOLUTIONS PVT LTD., in conjunction with functions such as Legal, Compliance and Risk Management, is responsible for assisting outsourced business process owners to analyze the associated risks and develop appropriate process, technical, physical and legal controls.
  - Members of the Information Security Team shall be also responsible for maintaining this policy.

- **Internal Audit**

  - Internal Audit is authorized by management to assess compliance with all corporate policies at any time.
  - Internal Audit may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

9.0 MOBILE COMPUTING AND TELE-WORKING POLICY

Purpose

The purpose of this Policy is to provide guidance for those staff/employees/agents of SYSTECH SOLUTIONS PVT LTD. who use any of the equipment identified below.

- Laptop computer
- Handheld computer
- Notebook computer
- Palmtop computer
- Personal Digital Assistant (PDA)
- Mobile phone
- Digital camera
- Portable printer
- Portable scanner
- Media – including discs, memory sticks

A breach of security and/or confidentiality can occur very easily with the loss or misuse of portable equipment.

Scope

All information recorded and/or stored onto portable equipment must comply with the SYSTECH SOLUTIONS PVT LTD. Information Security Policy. This should also be referred to when reading and referring to this Policy.

Management responsibilities

1. Risk Assessment to be done to identify potential risks to the data/information, programs and the equipment/media. The Risk Assessment conducted shall identify vulnerabilities and establish sufficient counter-measures as per the Risk Assessment Procedure outlined.

2. The User/personnel assigned with the equipment shall be made aware of the responsibility to hold/store information for work/business purposes only. The IT Manager shall liaise to provide advice on legal compliances with relevant data protection principles.
3. The Asset Register shall include the employee/third party details logged and to be aware of the responsibility for the portable equipment.
4. All equipment will be security marked with the Asset ID.
5. The Management shall authorize any personnel who are exempted from logging into Laptop Register. The document authorizing such exemption shall be retained with the HR and a copy to be made available with the security at the entry/exit.

User responsibilities

The User authorized to carry the equipment shall follow:

- To follow and adhere to the guidelines identified under the Laptop Security Policy;
- Users must be aware they have personal responsibility for the equipment and maintain confidentiality, integrity for all data/information held/stored on the equipment and acSYSTECH SOLUTIONS PVT LTDing media.
- All users of portable equipment must ensure they have read and understood this Policy.
- Users must also be made aware of the requirements detailed in the Information Security Policy.
- All equipment will be signed at the entry/exit point, unless exempted by the Top Management due to their roles and responsibilities.
- Unless exempted by the Top Management, Users who handle laptop outside the office location shall need to register the details in the Laptop Register, available with the security at entry/exit points. Such Users shall produce the authorization mail or letter approved by their respective Departmental Manager.
- Users to comply as per the relevant laws and regulations and adhere to the organizational security policies and procedures.
- User shall return the equipment on the occurrence of any event, where in the User leaves employment, changes job and no longer needs the equipment or is off on long term sickness or extended annual leave.
- Users must be made aware of action to be taken in the event of the equipment being lost or stolen. Action required is detailed as per the Incident Reporting Policy which staff should also be made aware of.

Physical Protection

- Portable computers/equipment is prone to rougher treatment than a desktop computer unit and is therefore more likely to breakdown or become damaged. All employees/users should ensure they take care of the equipment available in their custody.
- Portable equipment must not be left unattended in any public places or open offices.
- If the portable equipment is to be used in an office, then they shall be locked in a cabinet or a safe when unattended.
- It is normal for portable computer equipment to come with a purpose made carry case. These cases should always be used when transporting the equipment inside or outside of SYSTECH SOLUTIONS PVT LTD. premises.
- Portable equipment must be kept in the possession of the employee at all times. Example: The equipment must be removed from the car/two-wheeler when the employee leaves them unattended.
- Portable computers should be carried as hand luggage and disguised whenever possible during travel.
- If the portable equipment has a removable disc which can hold data/information it is sometimes better to detach the two and transport separately e.g. equipment in carry case and disc in inside pocket of coat.
- Carry cases and straps should be checked regularly to ensure that breakage will not occur as equipment damaged through being dropped is not normally covered by any maintenance or warranty agreements.
- Adequate insurance cover should be in place to protect the equipment off-site.

Software/Data protection

- Before personal information is to be stored on the portable equipment to be transported a risk assessment should be completed to identify risks, vulnerabilities and countermeasures to reduce the risks
- All portable equipment should have a machine/boot up password or user id that should be required (in the set up) when powered up. This is to stop unauthorized access to the information/data stored on the equipment and also to stop unauthorized persons being able to

access the operating system and programs. It is also desirable to have the floppy/CD drive disabled during start up.

- Approved users of laptops will be allowed access (as per need) to SYSTECH SOLUTIONS PVT LTD. network/database, from the portable equipment, by the use of a VPN (Virtual Private Network) connection/token on their laptop
- If information is to be uploaded there should be sufficient security and authorization checks in place to ensure no disruption to services or corruption to data can occur. This may be relevant for some employees of the organization.
- The data/information should where possible be encrypted or at the very least the files should be password protected. Guidance on this should be available from the IT experts within SYSTECH SOLUTIONS PVT LTD..
- The software on the portable equipment must comply with the organizational standards to ensure it is supportable.
- Where the equipment can receive and send data files/e-mails and attachments there will be a need to have up to date virus detection software installed. The organization must take into account that there will be a requirement to keep the virus detection software up to date with the current version available.
- There must be no loading of unauthorized software. Any software on the equipment must be that which is authorized and licensed. This is usually loaded by the IT department and should not be tampered with by any employee or other person using the equipment. Any tampering of the software may be considered a disciplinary offence.
- If the equipment is likely to be used to access the Internet, the users must ensure that the Internet and E-Mail security policies are not compromised.
- Users must be aware that they have a responsibility to ensure the information is available where and when it is needed. If information is to be stored on the hard disc, a second copy should also be made on to a portable media e.g. memory sticks or e-mailed to the user's official e-mail account. It is important that back-ups are performed on a regular basis and they not stored with the equipment e.g. not in the equipment carry case but, for example, in the office. If there are no back-ups and the equipment was to be stolen the information would also be lost which could cause problems with breaches of confidentiality, security and availability of the information.
- Care should be taken if mobile computing facilities have to be used in public places/areas, meeting rooms, on the train and other unprotected areas outside of the organization's premises, including cafe's and mall having Wi-Fi access. Protection should be in place to avoid the

unauthorized access or disclosure of the information stored and processed by the equipment e.g. no other person should be able to access the equipment or view information on the screen.

Retention of information

- It is important that when an employee who has a piece of portable equipment leaves the employment of SYSTECH SOLUTIONS PVT LTD., then the equipment is returned to their Process Head or Departmental Manager. Unless returned, the employee shall not be relieved from his duty.
- If the equipment is to be re-assigned to another part of the organization it will normally be necessary to up load and/or delete the information that is held/stored on the equipment before it is re-assigned as per the Asset Transfer or Asset Disposal requirement under IT Asset Control Policy.
- The retention of the information shall be as per the Data Backup and Storage Policy.

10.0 PERSONNEL SECURITY POLICY

Purpose

Intentional and unintentional misuse and abuse of SYSTECH SOLUTIONS PVT LTD. systems pose the greatest threats to information confidentiality, integrity, and availability. Therefore, SYSTECH SOLUTIONS PVT LTD. requires that all users of organizational information systems meet minimum personnel requirements related to the sensitivity of their roles, suitability for employment, personnel investigations, and other personnel security considerations.

Scope

All personnel who use, manage, design, or implement SYSTECH SOLUTIONS PVT LTD. Information Resources.

Roles and Responsibilities

LEADER

- Publishes and maintains policy guidelines for personnel security
- Determines the security access requirements for all positions
- Ensures that all personnel have undergone the appropriate background checks and security training

Information Security Coordinator (ISC)

- Prepares and responsible for implementation of personnel security policy
- Monitors the effectiveness of the personnel security policy
- Ensures all personnel are trained in the computer security responsibilities and duties associated with their jobs

IT Manager

- Communicates to the users the personnel security requirements outlined in this policy
- Monitors the adherence to the personnel security policy
- Ensures all personnel are trained in the computer security responsibilities and duties associated with their jobs
- Informs Security Officer when access is to be removed
- Responsible for tracking new personnel account requests, creation, issues, and deletions.
- Monitors compliance with personnel security policy.
- Promptly deletes passwords for systems and applications under their control when users terminate employment, suspect passwords are compromised, or no longer need access.
- Responsible for tracking users and their access authorizations.

Users

- Understand their personnel security responsibilities and duties
- Use SYSTECH SOLUTIONS PVT LTD. information in accordance with job functions, internal policy, and external regulations and laws
- Immediately notify supervisor of suspected misuse of data, security breaches, violations of policies and procedures, or compromise of password security

Policy

- All organizational positions (users, application managers, system management personnel, and security personnel) must be defined. Security issues related to the functions and responsibilities of these positions must be identified and addressed.
- Access privileges for any given position must be based on principles of
    a. Separation of Duties
    b. Least Privilege.
- All employees are subject to a limited background check, depending on role and system access needs.
- Employees shall be trained in computer security responsibilities and duties associated with their jobs.
- User account management on a system will be reviewed not less than once per 3 months and/or under the following security incidents.

- Periodic reinvestigation of personnel background and qualifications may be required.
- Managers will follow established procedures for:
    a. Personnel transfers or discontinuation the associated changes to or removal of access privileges, system accounts, and authentication tokens.
    b. Control of SYSTECH SOLUTIONS PVT LTD. physical keys.
    c. Training employees on their responsibilities for confidentiality and privacy.
    d. Return of SYSTECH SOLUTIONS PVT LTD. property and ongoing availability of data generated by individual employees.
    e. Involuntary termination and consequences, such as suspension of user accounts and, in some cases, the physical removal of personnel from the SYSTECH SOLUTIONS PVT LTD. offices.

Enforcement

Gross negligence or willful disclosure leading to illicit exposure of SYSTECH SOLUTIONS PVT LTD. information may result in prosecution for misdemeanor or felony resulting in fines, imprisonment, civil liability, and/or dismissal.

11.0 VIRUS/MALWARE PREVENTION POLICY

Overview

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Thus, organization implement solid security policies by blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention or any other malware and their detection and cleanup.

Scope

The Virus/malware Prevention Policy applies equally to all individuals that use any SYSTECH SOLUTIONS PVT LTD. Information Resources.

Policy Guideline

- All workstations whether connected to the SYSTECH SOLUTIONS PVT LTD. network, or standalone, must use the SYSTECH SOLUTIONS PVT LTD.'s approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each file server attached to the SYSTECH SOLUTIONS PVT LTD. network must utilize SYSTECH SOLUTIONS PVT LTD.'S approved virus protection software and setup to detect and clean viruses that may infect file shares.
- Each Email gateway must utilize SYSTECH SOLUTIONS PVT LTD.'S approved email virus protection software and must adhere to the Information Security rules for the setup and use of this software.

- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.

Enforcement

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; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of SYSTECH SOLUTIONS PVT LTD. Information Resources access privileges, civil, and criminal prosecution.

12.0 ANTI-SPAM & UNSOLICITED COMMERCIAL EMAIL POLICY

Overview

The practice of sending unsolicited, commercial mass e-mails represents a potential threat to organizational reputation and may be violation, which defines the quantity and characteristics of bulk commercial e-mails that may legally be sent.

All communications with customers, prospects and other professionals reflect SYSTECH SOLUTIONS PVT LTD.. In light of increasing antipathy to unsolicited email promotions of any kind, it is generally in the best interest of SYSTECH SOLUTIONS PVT LTD. to limit electronic mailings to legitimate communications with individuals have indicated a willingness to receive them.

Purpose

This policy describes the permitted and prohibited uses of corporate email systems for bulk emailing. Its purpose is to:

1. protect organizational reputation,
2. preserve the effectiveness of email as a business communication medium,
3. prevent potential breach of the US CAN-SPAM Act by SYSTECH SOLUTIONS PVT LTD. employees, and to generally encourage adherence to e-mailing best practices.

Scope

All individuals who use the SYSTECH SOLUTIONS PVT LTD. e-mail systems and addresses to send bulk e-mails to customers, prospects, or other types of recipients.

Guideline

- All mass emails or bulk emails must be approved by IT Manager.
- Individuals may send mass emails for the purpose of marketing or sales of SYSTECH SOLUTIONS PVT LTD. products, services, or programs ONLY to:
    - Recipients who specifically consented to receive SYSTECH SOLUTIONS PVT LTD. marketing or sales emails

  - Recipients who have not explicitly opted out of receiving marketing or sales SYSTECH SOLUTIONS PVT LTD. emails
- Mass emails sent from SYSTECH SOLUTIONS PVT LTD. computers or email addresses may not:
  - Contain false or misleading information in the subject line, headers, or email body
  - In any way misrepresent or disguise the sender, point of origin, or transmission path
- Individuals may not send any emails to addresses that have been illicitly harvested, mined, or skimmed from one or more third-party Web sites. Employees may not build e-mail addresses or lists by guessing or using software to generate character strings that are likely to be associated with live email accounts.

Anti-spam restrictions also apply to other forms of electronic messaging:

- Individuals may not post promotions or advertisements for SYSTECH SOLUTIONS PVT LTD. products, services, or programs in newsgroups, message boards, chat rooms, or other online services in violation of the terms of participation of those online services.
- Individuals may not post promotions or advertisements for SYSTECH SOLUTIONS PVT LTD. products, services, or programs in newsgroups, message boards, chat rooms, or other online services that do not explicitly permit advertisements.
- Individuals may not use vendors, software, or service providers or to circumvent the intent of this policy.

Enforcement

Violation of this policy may result in disciplinary action which may include performance sanctions; termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to restriction or suspension of SYSTECH SOLUTIONS PVT LTD. email privileges, as well as civil and criminal prosecution.

13.0 DATA BACKUP AND STORAGE POLICY

Overview

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

Purpose

The purpose of the SYSTECH SOLUTIONS PVT LTD. Data Backup and Storage Policy is to establish the rules for the backup and storage of SYSTECH SOLUTIONS PVT LTD. electronic information.

Scope

The SYSTECH SOLUTIONS PVT LTD. Data Backup and Storage Policy apply to all individuals within the SYSTECH SOLUTIONS PVT LTD. enterprise who are responsible for the installation and support of information resources, individuals charged with Information Security; and data owners. Information Services may have existing contracts for offsite backup data storage. These services can be extended to all SYSTECH SOLUTIONS PVT LTD. entities upon request.

Policy

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- SYSTECH SOLUTIONS PVT LTD. shall maintain backup and recovery process for each system/or information, which shall be documented and periodically reviewed.
- Any vendor(s) providing offsite backup storage for SYSTECH SOLUTIONS PVT LTD. must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest SYSTECH SOLUTIONS PVT LTD. sensitivity level of information stored.
- A process must be implemented to verify the success of the SYSTECH SOLUTIONS PVT LTD. electronic information backup.

- Backups must be periodically tested to ensure that they are recoverable.
- Signature cards held by the offsite backup storage vendor(s) for access to SYSTECH SOLUTIONS PVT LTD. backup media must be reviewed annually or when an authorized individual leaves SYSTECH SOLUTIONS PVT LTD..
- Procedures between SYSTECH SOLUTIONS PVT LTD. and the offsite backup storage vendor(s) must be reviewed at least annually.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
    a. System name
    b. Creation Date
    c. Sensitivity Classification [Based on applicable electronic record retention regulations.]
    d. SYSTECH SOLUTIONS PVT LTD. Contact Information

Enforcement

Violation of this policy may result in disciplinary action, including but not limited to performance penalties, employment termination, contract invalidation, civil action, and criminal prosecution. Additionally, violators may lose access privileges to SYSTECH SOLUTIONS PVT LTD. Information Resources.

14.0 PASSWORD MANAGEMENT POLICY

Overview

SYSTECH SOLUTIONS PVT LTD. balances the need for employees to access systems and information with the need to control access for the purposes protecting information confidentiality, integrity, and availability. Account passwords are a mainstay of information security controls. This policy establishes management controls for granting, changing, and terminating access to automated information systems, controls that are essential to the security of SYSTECH SOLUTIONS PVT LTD. information systems.

Scope

All employees who use SYSTECH SOLUTIONS PVT LTD. Information Resources must unique user account information, including passwords for access to various information systems. These procedures apply to accounts on all organizational systems: both in operation and in development.

Roles and Responsibilities

LEADER

- Provides management oversight of the process for administering passwords for SYSTECH SOLUTIONS PVT LTD. systems
- Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords

Information Security Coordinator (ISC)

- Prepares policy guidelines for the creation, safeguarding, and control of passwords
- Approves access of supervisor passwords and passwords for similar privileged accounts used on SYSTECH SOLUTIONS PVT LTD.'s network

IT Manager

- Communicates to the users the system access and password requirements outlined in this policy
- Informs LEADER and ISC when access is to be removed
- Immediately informs LEADER and ISC, on any suspicion that password has been compromised

- Issues and manage passwords for systems and applications under their control in accordance with SYSTECH SOLUTIONS PVT LTD.'s policy described below
- Issues passwords for privileged accounts to the primary system administrator and no more than one designated alternate system administrator; these passwords shall be changed at least every 30 days or when necessary due to employment termination, actual or suspected password compromise

Users

- Understand their responsibilities for safeguarding passwords
- Use SYSTECH SOLUTIONS PVT LTD. data in accordance with job function and SYSTECH SOLUTIONS PVT LTD policy
- Understand the consequences of their failure to adhere to statutes and policy governing information resources
- Immediately notify supervisor if it is suspected that password has been compromised

Policy

Access Authorization Requirements

Access to SYSTECH SOLUTIONS PVT LTD. resources shall be controlled and shall be based on an approved System Access Request Form for each of the systems.

- Individuals shall be granted access only to those information systems necessary for the performance of their official duties; users must receive supervisor's and the IT Manager's approval prior to being granted access to SYSTECH SOLUTIONS PVT LTD.'s information resources. This requirement includes contracted employees and all other non-SYSTECH SOLUTIONS PVT LTD. personnel who have been granted access.
- Passwords shall be used on all SYSTECH SOLUTIONS PVT LTD. automated information systems to uniquely identify individual users.
- Passwords shall not be shared with, used by, or disclosed to others; generic or group passwords shall not be used.
- To preclude password guessing, an intruder lock-out feature shall suspend accounts after three invalid attempts to log on; manual action by a security system administrator is required to reactivate the ID.

Password Parameters

All user and system passwords, even temporary passwords set for new user accounts, should meet the following characteristics:

- Be at least Eight (8) characters in length;
- Consist of a mix of alpha, and at least one numeric, and special characters;
- Not be dictionary words;
- Not be portions of associated account names (e.g., user ID, log-in name);
- Not be character strings (e.g., abc or 123);
- Not be simple keyboard patterns.

In addition, users are required to select a new password immediately after their initial logon. Passwords must be changed at least every 40 days. Previously used 3 passwords may not be re-used.

Password and Account Security

- Password accounts not used for 90 days will be disabled and reviewed for possible deletion. Accounts disabled for 60 days will be deleted. Accounts for SYSTECH SOLUTIONS PVT LTD. contractors shall terminate on the expiration date of their contract.
- Lockout policy must be implemented for unsuccessful login attempts. As a good practice a maximum of three (3) login attempts should be allowed. The auto-lock policy for locked accounts must be released by the IT Department after a written approval from the respective Process Owner.
- Screen-saver password must be enabled after 3 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.
- Passwords for all users' accounts must be changed on or before the 42nd day.
- Administrative account passwords must be changed promptly upon departure of personnel (mandatory or voluntary) or suspected compromise of the password. User accounts will be disabled promptly upon departure of personnel (mandatory or voluntary). Users should immediately change their password if they suspect it has been compromised.

- Vendor or service accounts will be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation at SYSTECH SOLUTIONS PVT LTD. facilities.
- Passwords may not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.
- Passwords may be not visible on a screen, hardcopy printouts, or any other output device

Password Protection Standards

1. Do not share passwords to ANYONE including your colleagues, administrative assistants, any secretaries, third party vendors or consultants providing service at SYSTECH SOLUTIONS PVT LTD..
2. Don't reveal a password over the phone to ANYONE
3. Don't reveal a password in an email message
4. Don't reveal a password to any team members or colleagues including your boss;
5. Don't talk about a password in front of others;
6. Don't hint at the format of a password (e.g., "my family name")
7. Don't reveal a password on questionnaires or security forms;
8. Don't share a password with family members;
9. Don't reveal a password to co-workers/colleagues while on vacation;
10. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

- If someone demands a password, refer them to this document or have them call someone in the Information Security department or IT Manager.
- All passwords are to be treated as sensitive, Confidential Information of SYSTECH SOLUTIONS PVT LTD..
- All passwords are to be changed once every quarterly, except system-level passwords to be changed once in every forty two (42) days.
- If an account or password is suspected to have been compromised, report the incident to ISMS team and ensure IT Manager takes measures to change all passwords.
- Periodic assessments to be performed on password cracking by ISMS team and report the same to Information Security Coordinator who shall submit the same to the review and approval of the Information Security Officer. During assessment the IT Manager and finds any violation to this

Policy on the Passwords maintained he shall sent a written mail to the respective User to change the password and ensure they change it.

Enforcement

Violation of this policy may result in disciplinary action, including but not limited to performance penalties, employment termination, contract invalidation, civil action, and criminal prosecution. Additionally, violators may lose access privileges to SYSTECH SOLUTIONS PVT LTD. Information Resources.

15.0 PHYSICAL SECURITY POLICY

Overview

Controlling physical access to Information and Information Processing Facilities (referred to herein as "Information Resource") is an extremely vital/ principal function of the SYSTECH SOLUTIONS PVT LTD. security program. This policy sets forth rules for establishing, controlling, and monitoring physical access to Information Resource facilities.

Scope

This policy applies to all individuals within SYSTECH SOLUTIONS PVT LTD. who are responsible for day to day access to information and information processing facilities, installation and support of Information and information processing facilities, members of information security management and personnel, other employees and data owners.

Policy

Information resources must be physically protected in proportion to the criticality, sensitivity, or business importance of their function(s)

General

- All physical security systems must comply with all applicable regulations, including, but not limited to, building codes and fire prevention codes. In the event of rental premises, precautionary measures to be initiated to avoid calamities due to environmental hazards. Training and security awareness to be initiated to all levels in the organization.
- Restricted areas and facilities must be clearly marked. Signage for restricted areas and facilities should contain enough information to be practical, but present minimal discernible evidence as to the nature of the importance of the location.
- Each individual granted physical access to restricted Information Resources or facilities must receive training on emergency procedures for the facility.

Physical access management

- Access to Information Resources must follow the principle of least privilege access. Personnel, including full time and part-time employees, contractors, and vendor service staff, should be granted access only to facilities and systems that are necessary for the fulfilment of their job responsibilities
- Requests for access must come from concerned Department Manager, upon approval, IT Manager shall grant access and include sign-off from an applicable Process Owner or Departmental Manager.
- The process for granting physical access to information and information processing facilities must include the approval of IT Manager.
- Each individual granted physical access to an information and information processing facilities must sign appropriate access, information protection, and nondisclosure agreements
- Administrative Department responsible for biometric or physical security access must remove card and/or key access rights of individuals that leave or change roles within SYSTECH SOLUTIONS PVT LTD.. Appropriate entry shall be entered in the List of User's access and rights retained by the IT Manager.
- IT Manager shall coordinate with the Administration Department to review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Visitors who have not been granted special access privileges must at all time be escorted and monitored in access-controlled areas SYSTECH SOLUTIONS PVT LTD. facilities.

Protection of physical access cards and keys

- Personnel must not share or transfer access cards and/or to other individuals within or external to SYSTECH SOLUTIONS PVT LTD.
- Access cards and/or keys that are no longer needed must be returned to Administration Department. Cards must not be transferred or reallocated to another individual, bypassing the return process
- Lost or stolen access cards and/or keys must be reported to the IT Manager and Administration Department Manager.

- Cards and/or keys must not have identifying information other than a return mail address.
- A service charge may be assessed for access cards and/or keys that are lost, stolen, or not returned.

Monitoring and Documentation

- Physical access to all restricted Information their resources and information processing facilities must be documented.
- All facilities that allow visitors must track visitor access with a sign in/sign out log
- Card access records and visitor logs for access to information resources and information processing facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Administrative Department or a authorized representative must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access

Enforcement

Gross negligence or willful disregard of this standard 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; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of SYSTECH SOLUTIONS PVT LTD. Information Resources access privileges, civil, and criminal prosecution.

16.0 POLICY ON CONTROL OF REMOVABLE MEDIA

Purpose

This document states the Removable Media policy for SYSTECH SOLUTIONS PVT LTD.. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of SYSTECH SOLUTIONS PVT LTD. computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

Scope

This policy applies to all Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to SYSTECH SOLUTIONS PVT LTD. information, information systems or IT equipment and intends to store any information on removable media devices.

Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the SYSTECH SOLUTIONS PVT LTD to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.

- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

Risks

SYSTECH SOLUTIONS PVT LTD. recognizes that there are risks associated with users accessing and handling information in order to conduct official SYSTECH SOLUTIONS PVT LTD business. Information is used throughout the SYSTECH SOLUTIONS PVT LTD and sometimes shared with external organizations and applicants. Securing PROTECT or RESTRICTED data is of paramount importance – particularly in relation to the SYSTECH SOLUTIONS PVT LTD's need to protect data in line with the requirements of the Data Protection. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the SYSTECH SOLUTIONS PVT LTD. It is therefore essential for the continued operation of the SYSTECH SOLUTIONS PVT LTD that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the SYSTECH SOLUTIONS PVT LTD's needs.

This policy aims to mitigate the following risks:

- Disclosure of PROTECT and RESTRICTED information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of SYSTECH SOLUTIONS PVT LTD networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the SYSTECH SOLUTIONS PVT LTD or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the SYSTECH SOLUTIONS PVT LTD or individuals as a result of information loss or misuse.

- SYSTECH SOLUTIONS PVT LTD reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the SYSTECH SOLUTIONS PVT LTD and may result in financial loss and an inability to provide necessary services to our customers.

Policy Statement

SYSTECH SOLUTIONS PVT LTD. will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

Applying the Policy

Restricted Access to Removable Media

It is SYSTECH SOLUTIONS PVT LTD. policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to IT Manager. Approval for their use must be given by Chief Information Security Officer (LEADER).

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by IT Services. Non-SYSTECH SOLUTIONS PVT LTD owned removable media devices **must not** be used to store any information used to conduct official SYSTECH SOLUTIONS PVT LTD business, and **must not** be used with any SYSTECH SOLUTIONS PVT LTD owned or leased IT equipment.

The only equipment and media that should be used to connect to SYSTECH SOLUTIONS PVT LTD equipment or the SYSTECH SOLUTIONS PVT LTD network is equipment and media that has been purchased by the SYSTECH SOLUTIONS PVT LTD and approved by the IT Manager or has been sanctioned for use by the LEADER.

Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for SYSTECH SOLUTIONS PVT LTD purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all PROTECT or RESTRICTED data held must be encrypted.

Users should be aware that the SYSTECH SOLUTIONS PVT LTD will audit / log the transfer of data files to and from all removable media devices and SYSTECH SOLUTIONS PVT LTD-owned IT equipment.

Incident Management

- It is the duty of all users to immediately report any actual or suspected breaches in information security to the LEADER who will initialize process as outlined within the Information Security Incident Management Policy.
- It is the duty of all stakeholders to report any actual or suspected breaches in information security to the LEADER or the ISC.

- Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the LEADER or ISC.

Third Party Access to SYSTECH SOLUTIONS PVT LTD Information

- No third party (external contractors, partners, agents, and the public or non-employee parties) may receive data or extract information from the SYSTECH SOLUTIONS PVT LTD's network, information stores or IT equipment without explicit agreement from the LEADER.
- In the event, any third parties are allowed access to SYSTECH SOLUTIONS PVT LTD information then all the considerations of this policy apply to their storing and transferring of the data.

Preventing Information Security Incidents

- Damaged or faulty removable media devices must not be used. It is the duty of all users to contact IT Department should removable media be damaged.
- Virus and malware checking software approved by the IT Department must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by virus checking software products, before the media is loaded on to the receiving machine.

- Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the SYSTECH SOLUTIONS PVT LTD, other organizations or individuals from the data being lost whilst in transit or storage.

Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the SYSTECH SOLUTIONS PVT LTD or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to IT Department for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the IT Manager.

User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with SYSTECH SOLUTIONS PVT LTD equipment or the network or to hold information used to conduct official SYSTECH SOLUTIONS PVT LTD business **must** only be purchased and installed by IT Department. Any removable media device that has not been supplied by IT **must not** be used.
- All data stored on removable media devices **must** be encrypted where possible.
- Virus and malware checking software **must** be used when the removable media device is connected to a machine.
- Only data that is authorized and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices **must not** to be used for archiving or storing records as an alternative to other storage equipment.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

For advice or assistance on how to securely use removable media devices, please contact the IT Manager.

Enforcement

If any user is found to have breached this policy, they may be subject to SYSTECH SOLUTIONS PVT LTD. Disciplinary Policy and related procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from LEADER.

17.0 DISCIPLINARY PROCEDURE

Purpose and scope

This procedure is designed to help and encourage all employees to achieve and maintain standards of conduct, attendance and job performance. The SYSTECH SOLUTIONS PVT LTD rules (a copy of which is displayed in the office) and this procedure apply to all employees. The aim is to ensure consistent and fair treatment for all in the organization.

Principles

- ✓ Counseling will be offered, where appropriate, to resolve problems.
- ✓ No disciplinary action will be taken against an employee until the case has been fully investigated.
- ✓ At every stage in the procedure the employee will be advised of the nature of the complaint against him or her and will be given the opportunity to state his or her case before any decision is made.
- ✓ At all stages of the procedure the employee will have the right to be accompanied by a trade union representative, or work colleague.
- ✓ No employee will be dismissed for a first breach of discipline except in the case of gross misconduct, when the penalty will be dismissal without notice or payment in lieu of notice.
- ✓ An employee will have the right to appeal against any discipline imposed.
- ✓ The procedure may be implemented at any stage if the employee's alleged misconduct warrants such action.
- ✓ The minimum three-step statutory procedures will be followed if an employee faces dismissal or certain kinds of action short of dismissal.

Procedure

Stage 1 – improvement note: unsatisfactory performance

If performance does not meet acceptable standards the employee will normally be given an improvement note. This will set out the performance problem, the improvement that is required, the timescale and any help that may be given. The individual will be advised that it constitutes the first stage of the formal procedure. A record of the improvement note will be kept for 6 months, but will then be considered spent – subject to achievement and sustainment of satisfactory performance.

Or

Stage 1 – first warning: misconduct

If the conduct does not meet acceptable standards the employee will normally be given a written warning. This will set out the nature of the misconduct and the change in behavior required. The warning should also inform the employee that a final written warning may be considered if there is no sustained satisfactory improvement or change. A record of the warning should be kept, but it should be disregarded for disciplinary purposes after a specified period (eg, six months).

Stage 2: final written warning

If the offence is sufficiently serious, or there is a failure to improve during the currency of a prior warning for the same type of offence, a final written warning may be given to the employee. This will give details of the complaint, the improvement required and the timescale. It will also warn that failure to improve may lead to action under Stage 3 (dismissal or some other action short of dismissal), and will refer to the right of appeal. A copy of this written warning will be kept by the supervisor but will be disregarded for disciplinary purposes after 6 months subject to achievement and sustainment of satisfactory conduct or performance.

Stage 3 – dismissal or other sanction

If there is still a failure to improve the final step in the procedure may be dismissal or some other action short of dismissal such as demotion or disciplinary suspension or transfer (as allowed in the contract of employment). Dismissal decisions can only be taken by the appropriate senior manager, and the employee will be provided, as soon as reasonably practicable, with written reasons for dismissal, the date on which the employment will terminate, and the right of appeal. The decision to dismiss will be confirmed in writing.

If some sanction short of dismissal is imposed, the employee will receive details of the complaint, will be warned that dismissal could result if there is no satisfactory improvement, and will be advised of the right of appeal. A copy of the written warning will be kept by the supervisor but will be disregarded for disciplinary purposes after 6 months subject to achievement and sustainment of satisfactory conduct or performance.

Statutory Discipline and Dismissal Procedure

If an employee faces dismissal – or certain action short of dismissal such as loss of pay or demotion – the minimum statutory procedure will be followed. This involves:

- Step one: a written note to the employee setting out the allegation and the basis for it
- Step two: a meeting to consider and discuss the allegation
- Step three: a right of appeal including an appeal meeting.

The employee will be reminded of their right to be accompanied.

Gross misconduct

The following list provides examples of offences which are normally regarded as gross misconduct:

1. theft, fraud, deliberate falsification of records
2. fighting, assault on another person
3. deliberate damage to organizational property
4. serious incapability through alcohol or being under the influence of illegal drugs
5. serious negligence which causes unacceptable loss, damage or injury
6. serious act of insubordination
7. Unauthorized entry to computer records.

If you are accused of an act of gross misconduct, you may be suspended from work on full pay, normally for no more than five working days, while the alleged offence is investigated. If, on completion of the investigation and the full disciplinary procedure, the organization is satisfied that gross misconduct has occurred, the result will normally be summary dismissal without notice or payment in lieu of notice.

Appeals

An employee who wishes to appeal against a disciplinary decision must do so within five working days. The HR Manager will hear all appeals and his/her decision is final. At the appeal any disciplinary penalty imposed will be reviewed.

18.0 SOFTWARE INSTALLATION POLICY

Purpose

The purpose of this policy is to address all issues relevant to software installation and deployment on SYSTECH SOLUTIONS PVT LTD.'S computer systems.

Authority

- This policy has full support from the Top Management and human resources department.
- The LEADER administers this policy. This policy is currently effective for all SYSTECH SOLUTIONS PVT LTD., employees and computer systems.

Continuance

This policy is a living document and may be modified at any time by the IT Manager, Human Resources, or the Top Management.

Mission

SYSTECH SOLUTIONS PVT LTD.'s IT objective is to enable its employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs.

Dilemma

Historically, we have not consistently addressed how software is to be deployed to SYSTECH SOLUTIONS PVT LTD.'s computer systems. This lack of a standard policy has adversely affected the IT mission at times. This policy will set protocol as to how software is to be delivered to better enable IT to achieve its objective of delivering stable, well-performing technology solutions.

Installation and support of SYSTECH SOLUTIONS PVT LTD.'s software

The SYSTECH SOLUTIONS PVT LTD., IT department is exclusively responsible for installing and supporting all software on SYSTECH SOLUTIONS PVT LTD computers. This responsibility set includes:

- Office desktop computers;
- SYSTECH SOLUTIONS PVT LTD laptop computers (Used both onsite and offsite);
- Computer lab public desktop computers.

The SYSTECH SOLUTIONS PVT LTD., IT department relies on installation and support to provide software and hardware in good operating condition to SYSTECH SOLUTIONS PVT LTD., employees so that they can best accomplish their tasks.

Current software

SYSTECH SOLUTIONS PVT LTD., IT, in coordination with all other departments, has decided upon the following software standards:

Approved Software list:

The current software can exist in any one of the following scenarios:

- An IT-created “image” or OEM installation on the hardware;

- A SYSTECH SOLUTIONS PVT LTD., IT Department installation procedure that provides for the following:
    - Installation options
    - Upgrade considerations (if applicable)
    - Data conversion (if applicable)
- A shortcut to a network application (not truly an installation)
- An automated installation through an IT-developed solution that may be used in a rapid-deployment scenario or silent-install situation
- A terminal application, Server application, or other thin-client type of application accessible via the SYSTECH SOLUTIONS PVT LTD., intranet page

Software **cannot** be present on SYSTECH SOLUTIONS PVT LTD., computers in the following scenarios:

- An installation not by a procedure
- A piece of software purchased for one's home computer
- A downloaded title from the Internet
- A pirated copy of any title
- A different title from the current software list of this policy
- Any means not covered by the ways that software can exist on SYSTECH SOLUTIONS PVT LTD., computers

Software licensing

Most of the software titles on SYSTECH SOLUTIONS PVT LTD.'s current software list are not freeware; therefore, the cost of software is a consideration for most titles and their deployment.

It is the goal of the IT department to keep licensing accurate and up to date. To address this, the IT department is responsible for purchasing software licenses for the following software categories:

- Desktop operating system software
- Productivity tools package
- Internet software
- Accessories

The other software categories (workgroup-specific titles) are the purchasing responsibility of the workgroup in which they serve. However, the application(s) are still installed and supported by the IT department.

To control costs, licensing costs are a factor in the decision-making processes that go into client software planning and request approval.

Software Requests

If a user is to request software for their computer, the proper method will be to send a request to the IT manager.

A response is guaranteed within one business day via e-mail. If the Urgent option is selected or an in-person appearance occurs, a solution may be delivered at the first possible time. All in-person or “walk-in” requests are logged by a manual entry into the support request system to track licensing needs and costs.

Summary: SYSTECH SOLUTIONS PVT LTD.’s software installation policy

This policy is designed to let SYSTECH SOLUTIONS PVT LTD., employees achieve their business objectives. Any aberrations from this strategy will require the IT department to redeploy software and/or hardware solutions. Full cooperation with this policy is appreciated so that all goals can be met in accordance with the business objectives.

19.0 POLICY ON USE OF NETWORK RESOURCES AND SERVICES

Background and Purpose:

This document represents the SYSTECH SOLUTIONS PVT LTD-wide guidelines and responsibilities required to maintain acceptable and proper use of all SYSTECH SOLUTIONS PVT LTD. network resources and services. The intent of this policy is to educate users about their responsibilities regarding computing resources and services while identifying certain unacceptable uses of network resources and services.

Scope

This policy covers all computer and communication equipment owned or operated by SYSTECH SOLUTIONS PVT LTD. including all equipment attached to or using SYSTECH SOLUTIONS PVT LTD. resources. Explicit in the above statement is that this policy also includes ANYONE using SYSTECH SOLUTIONS PVT LTD. computer and/or communications equipment and/or ANYONE accessing and/or using SYSTECH SOLUTIONS PVT LTD. resources.

User Responsibilities

Courtesy and respect for rights of others.

The SYSTECH SOLUTIONS PVT LTD. campus community has the responsibility to foster a positive and secure campus community by respecting and valuing the right of privacy and the diversity of the population and opinion in the community. In addition, all are responsible for complying with SYSTECH SOLUTIONS PVT LTD policy and all laws and contracts regarding the use of information.

Use of resources

- Users are responsible for knowing what information resources are available including those shared by the campus community. Users should refrain from all acts that waste or prevent others from using these resources.
- Users have a responsibility to ensure the security and integrity of the computer and network resources and services they use or access. Responsibilities include performing regular data backups, controlling physical access to information and computer equipment, using virus protection software, and keeping the virus definition file (DAT file) up to date. Responsibilities may also include updating Windows Critical Updates as requested by Computer and Information Services.

Information integrity

- Users are responsible for the accuracy, completeness, trustworthiness, timeliness, and relevance of the data they enter into and extract from SYSTECH SOLUTIONS PVT LTD. information systems. Users should not unconditionally depend on information or communications to be correct when they appear contrary to expectations. It is important to verify the integrity of the data entered into SYSTECH SOLUTIONS PVT LTD. information systems because information contained on SYSTECH SOLUTIONS PVT LTD. information systems may be used for reporting at a future date.
- **Users shall not place confidential information on the computer's local hard drive without protecting the information appropriately.**
- Employee, Client and Vendor/Supplier details to be kept confidential. If you store confidential or sensitive information on your computer, you are required to take all precautionary steps to safeguard the information.
- **Users are responsible for adhering to the Internal Network Equipment Policy when connecting any devices to the SYSTECH SOLUTIONS PVT LTD..**
- Devices include, but are not limited to computers, laptops, servers, routers, switches, hubs, wireless devices.

Rules

- **No one shall use any SYSTECH SOLUTIONS PVT LTD network resources or services without proper authorization.** No one shall assist in, encourage or conceal any unauthorized use or attempt at unauthorized use of any of the SYSTECH SOLUTIONS PVT LTD's network resources and services.
- Use of network resources and services without permission is theft of services and is illegal under state and SYSTECH SOLUTIONS PVT LTD law.
- Authorized use of SYSTECH SOLUTIONS PVT LTD.-owned or operated computing and network resources are in use that is consistent with the academic and service missions of the SYSTECH SOLUTIONS PVT LTD.
- **No one shall knowingly endanger the security of any SYSTECH SOLUTIONS PVT LTD. network resource, nor willfully interfere with others' authorized network usage.**
- **No one shall use SYSTECH SOLUTIONS PVT LTD.'s network resources or services to attempt unauthorized use, nor to interfere with others' legitimate use, of any network facility anywhere.**

    - The ability to use a remote computer does not constitute permission.

- Users are not permitted to run software that searches for means of obtaining unauthorized access (ie. port scans, password crackers, etc.) even if the user does not plan to make unauthorized access after finding an access point.
- Users are not permitted to run software that burdens the network with unnecessary traffic or intentionally degrades the performance of the network. (i.e., unnecessary repetitive pings and trace routes)

- **No one shall connect any computer or network equipment to any of the SYSTECH SOLUTIONS PVT LTD's network resources or services until the equipment has been registered with the IT Infrastructure Department.**
- Users are responsible for adhering to the Internal Network Equipment Policy when connecting any devices to the SYSTECH SOLUTIONS PVT LTD.. One improperly configured computer or network device on a network can cause SYSTECH SOLUTIONS PVT LTD-wide disruption.
- Devices include, but are not limited to computers, laptops, servers, routers, switches, hubs, wireless devices.
- **No one without specific authorization shall use any SYSTECH SOLUTIONS PVT LTD network resource or service for non-SYSTECH SOLUTIONS PVT LTD business.**
- By law, the SYSTECH SOLUTIONS PVT LTD can only provide computer resources and services for its own work, not for private use. Therefore, using SYSTECH SOLUTIONS PVT LTD resources or services to establish, run or support a personal and/or non-SYSTECH SOLUTIONS PVT LTD related business venture (e.g. via email, web site, listserv, etc.) is prohibited.
- Users in need of computing/printing resources for private or personal purposes will need to contact local computer vendors for procurement options.
- **No one shall create, install or knowingly distribute a computer virus or other surreptitiously destructive program on any SYSTECH SOLUTIONS PVT LTD. network resource , regardless of whether any demonstrable harm results.**
- **File sharing software is not permitted.**

Enforcement

These policies and procedures are designed to ensure the integrity, security, and proper effective functioning of SYSTECH SOLUTIONS PVT LTD IT services. All policy and procedure violations will be subject to investigation and appropriate disciplinary action through established channels that may include, for serious violations, letters of reprimand and/or termination of employment.

SYSTECH	**IT POLICIES AND PROCEDURES**	**Document Number**	**ITNOCP01**
		Date	**2/06/24**
		Revision No	**2.1**

20.0 USER REGISTRATION, DE-REGISTRATION PROCEDURES

Summary

The following procedures refer to the preparation required to ensure new employees gain access to network and e-mail facilities as quickly and safely as possible on commencement of employment. It also details the process required when removing an individual from the system (e.g. when an individual leaves their employment with SYSTECH SOLUTIONS PVT LTD.).

User Registration

- The IT Department helpdesk should be contacted at least 2 days before a new user commences employment by the HR Manager.
- Required information will be the user's full name, where they are based, start date, and whether they will need access to any specific systems. When the registration is processed, the IT Department will contact the HR Manager or the individual requesting the new registration, to inform them of the user's username and password.
- The user will be prompted to change his/her password on commencement of employment as they access the system for the first time.
- Upon any requirement where the user shall be working with a new PC, laptop or other device, the Departmental Manager or HR Manager shall ensure that the new PC, laptop or other device is set up/processed by the IT Department. The IT Department should be given at least one week's notice that a PC, laptop or other device requires setting up.
- On commencement of employment, the new user should contact the IT helpdesk to be guided through how to set up their e-mail 'profile'. For users with limited IT experience, another authorized individual can help with this.

De-registration & Asset Recovery

- Network and e-mail access privileges should be removed when an individual leaves employment with SYSTECH SOLUTIONS PVT LTD. (or in some cases before) to ensure system security is maintained.
- Within 24 hours of an individual leaving employment, the individual's Departmental Manager/Administration Manager / HR Department should contact the IT Support Team to inform them of the following:
    - Employee's name :
    - Department :
    - Reporting Manager :
    - Leaving date:
- After receiving the information from Department Manager / HR Dept On the afternoon of the scheduled leave date, the following actions are carried out
    - The ID account is disabled and employee is removed from all distribution list
    - The telephone (ext.) will be disabled (if applicable)
    - The Mobile Phone's Calls will be diverted to their reporting / Departmental Managers
    - The users' Home Directory is disabled
    - The users IT equipment is collected
    - Mails will be forwarded to authorized personnel/Departmental Manager
    - An Auto Response to user email will be inserted

- **Once this process is completed, the below mentioned process will be executed by IT Team on the Asset used by the employee.**
    - User's Data (desktop, My documents, Mails) will be copied to the folder in server
    - All the partitions will be deleted & new partitions are created.
    - Operating system will be reinstalled along with applications according to SYSTECH SOLUTIONS PVT LTD.'s Default software list.

21.0 INTERNET USE MONITORING AND FILTERING POLICY

Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within SYSTECH SOLUTIONS PVT LTD. 's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

Scope

This policy applies to all SYSTECH SOLUTIONS PVT LTD. employees, contractors, vendors and agents with a SYSTECH SOLUTIONS PVT LTD. owned or personally-owned computer or workstation connected to the SYSTECH SOLUTIONS PVT LTD. network.

This policy applies to all end user initiated communications between SYSTECH SOLUTIONS PVT LTD. 's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

Policy

A. Web Site Monitoring

The Information Technology (IT) Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for sixty (60) days.

B. Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to the Information Technology Department. Members authorized by the Departmental Manager or Top Management for overseeing incidents under Incident Management Policy and the Information Security

Coordinator shall have access to all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside only upon written or email request to Information Systems from a Human Resources Representative.

C. Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for SYSTECH SOLUTIONS PVT LTD.'s corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging (Exempted: Skype & Google Talk)
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email with exemption stipulated under Email Security Policy

D. Internet Use Filtering Rule Changes

The Information Technology (IT) Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

E. Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

Enforcement

The IT Manager will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Terms	Explanation
Internet Filtering	Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.
User ID	User Name or other identifier used when an associate logs into the corporate network

IP Address	Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.
SMTP	Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers
Peer to Peer File Sharing	Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts
Social Networking Services	Internet sites such as MySpace and Facebook that allow users to post content, chat, and interact in online communities.
SPAM	Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.
Phishing	Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.
Hacking	Sites that provide content about breaking or subverting computer security controls.

22.0 EMPLOYEE PRIVACY POLICY

Purpose

This policy will outline how SYSTECH SOLUTIONS PVT LTD. handles employee privacy.

Scope

This policy shall apply to all employees handling personal information of employees stored with SYSTECH SOLUTIONS PVT LTD.

Exceptions

There is no specific exception authorized under this policy. This policy is applicable for all employees whose work is reviewed safeguarding their privacy that is owned during their time at work.

Privacy Rights

Without limitations to any other policy or procedures followed in SYSTECH SOLUTIONS PVT LTD. and any applicable legal requirements, all employees of SYSTECH SOLUTIONS PVT LTD. can expect a reasonable amount of privacy during the work day. The organization and management trust employees to work on SYSTECH SOLUTIONS PVT LTD business while at work with the exception of break periods or observed lunches.

During work, an employee may receive phone calls, email messages, or communications that are not related to work. If these do not interfere with the regular performance of job duties for that employee they are allowed.

Electronic Communication And Documents

- SYSTECH SOLUTIONS PVT LTD. reserves the right to retain and review all communication sent through the communication networks or equipments, as well as any documents created and stored on SYSTECH SOLUTIONS PVT LTD resources such as servers, desktops or lockers.

- All messages that are not work related are forbidden to be sent to the SYSTECH SOLUTIONS PVT LTD mail account. Any message that is identified for or required and the employee with the prior permission sends such document or information to the requirement process owners, measures are taken to protect the sensitivity of such information disclosed by the employee.

- All documents stored on SYSTECH SOLUTIONS PVT LTD resources are subject to review. It is not to be assumed that personal documents will not be used, read, or obtained by SYSTECH SOLUTIONS PVT LTD., if they are stored on SYSTECH SOLUTIONS PVT LTD. owned information systems or equipment.

- Constant use of a personal email account that interferes with regularly assigned duties will result in disciplinary action where appropriate, up to and including termination. Checking personal email or voicemail during scheduled breaks or briefly during the workday, as long as this does not affect performance, is allowed by employees using the SYSTECH SOLUTIONS PVT LTD.'s information system.

Use of Internet Access

Using the Internet during SYSTECH SOLUTIONS PVT LTD time when not required by job duties for research or other purposes should be limited to break periods. Any use for non-work purposes that interferes with productivity and performance will not be allowed. Such usage shall adhere to the Internet Usage Policy requirements.

Ejilson Nelson

Digitally signed by Ejilson Nelson
Date: 2024.11.14 12:07:12 +05'30'