ePATH USA
Premier IT Services

Information Security Manual
ISM-01

Version: 1.0 Date: December 13, 2017

Uncontrolled copy if printed/ photocopied (unless specified otherwise)

NOTICE:

Information contained in this document is classified EPATHUSA Confidential Proprietary. No person outside the EPATHUSA shall have access to the information contained in this document unless business needs dictate, otherwise. It is the responsibility of the person knowing the information contained in this document to ensure confidentiality of information contained in it and preventing unauthorized access to this document always.

EPATHUSA Information Security Manual:

Revision History

Rev. No.	Revision Date	Revision Description	Approved By	Effective Date
1.0	December 13, 2017	Baseline document	Hari	December 13, 2017

Document Distribution

Name	Designation / Role
Hari	Management / Chief Information Security Officer (CISO)

TABLE OF CONTENTS

1. Introduction

1.1 Purpose

This document describes EPATHUSA Information Security Management System (ISMS). Although information security is not a core competency of most organizations, it has become a key business enabler, not just an IT option. Without adequately protected enterprise network and other security procedures, the ability of the enterprise to carry out its business is not assured. Any vulnerability could cripple the enterprise preventing it from carrying out its normal business for days and weeks impacting its earnings and profitability. The security threats to business assets are becoming increasingly more sophisticated. Advanced attacks use multiple methods to discover / exploit / propagate network vulnerabilities. It has become a business requirement that a stringent information security management system be put in place.

EPATHUSA deals with protecting its business assets against possible malicious actions targeted on its business assets to negatively impact the business to ensure business continuity.

EPATHUSAISMS concerns with preserving the following three properties of its information base:

- **Confidentiality**:
  Ensuring that information is accessible only to those authorized to have access
- **Integrity**:
  Safeguarding the accuracy and completeness of information
- **Availability:**
  Ensuring that authorized users have access to information when required

EPATHUSA considers ISMS as a key component in its business operations and growth.

The followings are the main executive goals of EPATHUSA ISMS:

- To define and implement processes and policies that protect its business assets including implementing security solutions that support robust and secure network infrastructures to protect the assets and to ensure efficient business operations and business continuity
- To track and keep pace with changing requirements of business and changing threat scenarios.
- To meet statutory & regulatory requirements (compliance, logging, audit, tracing etc.…)
- To implement security solutions that are cost-effective and that afford ease-of-use (easy administration and management) for meeting the above-mentioned goals

1.2 Scope of Certification

ISO 27001 Certification Scope

ISMS manages information security services to internal users of EPATHUSA in accordance with the ISMS Statement of Applicability

The ISMS covers all the business processes and resources associated with the information systems used to provide Software Development, Maintenance and Product Content Services, office located at:

EPATHUSA, LLC
IA

This includes the operation of communications to support the LAN and up to where the “client” links terminate.

1.3 Abbreviations, Acronyms and Definitions

Abbreviation	Description
MRF	Management Review Forum
ISMS	Information security Management System
BU	Business Unit
AMC	Annual Maintenance Contract

1.4 Information Security Policy

We at EPATHUSA, are committed to the operation & continuous improvement of an Information Security Management System relevant to the security risks of the organization to

- Ensure Business Continuity.
- Protect Confidentiality, Integrity and Availability of our information assets.
- Meet Contractual obligations on information security.
- Meet Regulatory and legislation requirements.
- Make employees alert and responsive to information security issues
- Undertake proactive actions and implement relevant information security policies to prevent security breaches

1.5 Management Commitment

The Management of EPATHUSA is committed to the implementation of ISMS to achieve its information security goals. Management shall define the information security goals in conjunction with the business goals.

The Management is keen on promoting security of information assets and shall give due importance to the development and enforcement of a corporate culture, which promotes security. Active participation of the user community and staff members is a must for any security initiative to succeed. The senior management shall endeavour to provide constant support to the staff members and the Information Security Forum to ensure that the security consciousness permeates across all levels of the organization.

Management shall provide all resources required for the definition and effective implementation of ISMS. The management shall participate in the Management Review Meetings and review the effectiveness and suitability of ISMS implementation and take necessary corrective & preventive actions where required.

2 Establishing and Maintenance of ISMS

2.1 Asset Identification & Classification

EPATHUSA information assets can be broadly classified as follows:

Information Assets	Databases, System Documentation, training material, procedures, plans, Information Security records, Contracts, Guidelines, Company Documentation
Software Assets	Application software, System Software, development tools and utilities
Hardware & Infrastructure Assets	Computer equipment, Media, buildings, furniture
People	Personnel
Services	Air –conditioning, power, ISP

EPATHUSA information base is classified as Category 1, Category 2, Category 3 based on the asset value.

Asset Categorization	
Category 3	If the asset value is 1, 2, or 3
Category 2	If the asset value is 4, 5, or 6
Category 1	If the asset value is 7, 8 or 9

The asset value is computed using the asset rating matrix given below:

Asset Type	Rating	Security Parameter		
		Confidentiality	**Integrity**	**Availability**
For all asset types	**No Impact (0)**	Not Applicable (0)	Not Applicable (0)	Not Applicable (0)
Information Assets	**Low (1)**	Disclosure outside organization would be inappropriate and inconvenient (1)	unauthorized modification could cause inconvenience and additional effort to re-establish integrity (1)	Lack of availability could cause delay in execution of business activities, but no external impact (1)
Information Assets	**Medium (2)**	Disclosure inside or outside would cause significant harm to the interest of the organization (2)	unauthorized modification could have monetary impact on the business and require significant additional effort re-establish integrity (2)	Lack of availability could cause significant delay in execution of business activities with external impact (2)
Information Assets	**High (3)**	Disclosure inside or outside would cause serious damage to the interests of the organization (3)	unauthorized modification could have significant monetary impact on the business and loss of reputation and future business (3)	Non-availability could lead to failure in meeting contractual requirements or monetary loss (3)
Software assets	Low (1)	Unauthorized use or violations of license internally, with minimal impact (1)	unauthorized changes to software asset and / or its configuration impacting its usage and requiring additional effort to re-establish integrity (1)	Lack of availability could cause delay in execution of business activities, but no external impact (1)
Software assets	Medium (2)	Unauthorized use or violations of license externally, with moderate impact (2)	unauthorized changes to software asset and / or its configuration affecting its usage, and require significant additional effort re-establish integrity (2)	Lack of availability could cause significant delay in execution of business activities with external impact (2)
Software assets	High (3)	Unauthorized use or violations of license externally, with significant impact (3)	unauthorized changes to software asset and / or its configuration affecting its usage, with monetary impact on the business and require significant additional effort re-establish integrity (3)	Non-availability could lead to failure in meeting contractual requirements or monetary loss (3)

Asset Type	Rating	Security Parameter		
		Confidentiality	Integrity	Availability
Hardware & Infrastructure Assets	Low (1)	Unauthorized physical access with minimal impact on business (1)	Damage to the asset and / or its configuration impacting its usage and requiring additional effort and investment to restore integrity (1)	Lack of availability could cause delay in execution of business activities, with minimal impact on business (1)
Hardware & Infrastructure Assets	Medium (2)	Unauthorized physical access, with moderate impact on business (2)	Damage to the asset or partial / total loss of the asset, impacting its usage and requiring significant additional effort and investment to restore integrity (2)	Lack of availability could cause significant delay in execution of business activities with moderate impact on business (2)
Hardware & Infrastructure Assets	High (3)	Unauthorized physical access, with significant impact on business (3)	Damage to the asset or partial / total loss of the asset, with monetary impact on the business requiring significant additional effort and investment to restore integrity (3)	Non-availability could lead to failure in meeting contractual requirements or monetary loss (3)
Services	Low (1)	Unauthorized access to service with minimal impact on business (1)	Misuse or deficiency of service resulting in inconvenience and minimum business impact (1)	Lack of availability could cause delay in execution of business activities, with minimal impact on business (1)
Services	Medium (2)	Unauthorized access to service, with moderate impact on business (2)	Misuse or deficiency of service resulting in moderate business impact (2)	Lack of availability could cause significant delay in execution of business activities with moderate impact on business (2)
Services	High (3)	Unauthorized access to service, with significant impact on business (3)	Misuse or deficiency of service resulting in significant business impact (3)	Non-availability could lead to failure in meeting contractual requirements or monetary loss (3)

The guidelines for classifying an information asset based on confidentiality are as follows:

Low	Disclosure/ inside or outside organization would not cause any damage or inconvenience
Medium	Disclosure inside or outside organization would be inappropriate and inconvenient
High	Disclosure inside or outside would cause significant harm to the interest of the organization

All assets will have suitable identification EPATHUSA based on the confidentiality level

Asset Classification	Hard Copy	Soft Copy	Physical Assets
Low	None	None	None
Medium	If the information is in the form of a booklet/binding then stamp on the cover page – "Proprietary Information" If the information is in the form of individual sheets then stamp on all pages - "Proprietary Information"	Footer of the document to contain the asset classification "Proprietary Information"	None
High	If the information is in the form of a booklet/binding then stamp on the cover page – "Confidential Information" If the information is in the form of individual sheets then stamp on all pages - "Confidential Information"	Footer of the document to contain the asset classification "Confidential Information"	The asset label shall contain the Asset Classification information – "Critical"

It is recommended that all Highly Confidential information contain a statement indicating only "Persons in the distribution are authorized to access it. If found by anyone other than the ones on the distribution list, it must be returned at once to the owner" It should also contain the distribution list.

It will be the responsibility of the owner of Confidential/Highly Confidential information to ensure that the information is communicated only to the authorized persons on the distribution list.
All practices/functions are required to identify and classify their assets. The inventory of assets is reviewed periodically the Information Security forum along with respective practice/function heads/representatives.
The current list of assets / classification is maintained by the Information Security Officer

2.2 Risk Management Guidelines

The controls applicable at EPATHUSA are based on the current list of assets and the risks identified for the same. Risk identification and mitigation is done according to the EPATHUSA Risk Assessment Process. Reference Document: EPATHUSA Risk Assessment Process

2.3 Statement of applicability

A statement of applicability indicating the applicability of controls indicated in the ISO 27001 part II standard and any other additional controls chosen is prepared by the Information Security Forum. The statement of applicability is reviewed and updated as and when the Risk Plan is reviewed and modified.

Referred Documents: ISMS_EPATHUSA_Statement_of_applicability.xls

2.4 Security Organization and Responsibilities

A security organization shall be formed to define and guide the implementation of security policies and procedures. The various positions in this group are:

- Management Review Forum (MRF)
- Information Security Forum
- Information Security Officer and
- Information asset owner

2.4.1 Management Review Forum

MR shall head the MRF, which consists of all Project Managers/Leaders. The following shall be the broad based duties and responsibilities of the MRF:

- Review and approve the security policy and have overall responsibility for its definition and implementation.
- Approve major information security initiatives.
- Review emerging threats arising out of new technologies and business practices and assess its impact on the organization.
- Mandate periodic audits to review the security of Information assets in the organization.

2.4.2 Information Security Forum

An Information Security Forum consisting of Information Security Officer, Representatives/Project managers from each practice/function shall have the overall responsibility for managing the ISMS. This team shall report to the CEO. The following shall be the broad based duties and responsibilities of the Information Security Forum:

- Review and approve the Asset Lists and Risk Management Plan of all practices/functions
- Define/Maintain, facilitate and monitor the implementation of the organization's ISMS.
- Ensuring that specialized advice and Training on information security is available to Employees, Customers and Third party service providers.
- Approval of new Information Assets
- Responding to security incidents in a calibrated manner

2.4.3 Information Security Officer

The overall responsibility for Information security in the organization shall be allocated to a single officer. This is designed to increase ownership and co-ordination of security management activities. This officer, designated as the Information Security Officer, shall report to CEO. The following shall be the broad based duties and responsibilities of the Information Security Officer:

- Setting up and publication of standards, advice and guidance
- Monitoring of compliance and co-ordination activities necessary to attain the organization's security objectives.
- Informing the CEO of any security incident or threat that could affect the Information Assets and business processes.
- Advising the CEO on outstanding security implementation issues and their associated costs, risks and benefits.
- Responding to security incidents in a calibrated manner.
- Recommending updates to the security policy and procedures (including legislative inputs on information security) to the Management Review Committee.

2.4.4 Information asset owner

All the IT assets in the organization will have an assigned owner. The owner shall be the prime controller for maintaining the assets under his control. Information assets shall remain the exclusive property of the organization. The role of the owner shall be to correctly classify the assets as per the classification norms and to exercise reasonable control over its usage. The following shall be the broad based duties and responsibilities of the Information asset owner:

- Specifying the measures necessary for protecting the Information assets in consultation with the Information Security Forum and the head of practice/function.
- Ensuring good security practices are maintained within their area of responsibility and that policy and procedures laid down to maintain information security is followed.
- Ensuring all staff is made aware of what is expected of them in order to maintain the security of Information assets.

2.4.5 Information asset users

All employees in the organization are responsible for using the organizations information assets in accordance with the Acceptable Use Policy in ISMS. All employees are required to be aware of the policies and procedures in ISMS. All employees are required to notify their supervisor or Information Security officer of any security breaches/incidents.

2.5 Implementation Norms

All practices/functions are required to implement the ISMS policies and procedures. In cases where the business activities require deviations to the ISMS policies and procedures, a request indicating the need for deviation is forwarded by the Practice/Function Head to Information Security Officer. Information Security Officer in consultation with Information Security forum shall review the risks and any additional controls required and approve the same. Information Security officer shall keep track of all such deviations issued.

In cases where the customer has security requirements, which require different/additional controls from those, indicated in ISMS, the requirements are forwarded to the Information Security Officer. ISO in consultation with the Practice head and Information Security forum assists the project team to develop an Information security plan specific to the project/practice.

2.6 Document & Data Control

The ISMS comprises of the following documents:

- Information Security Manual
- Asset List / Risk Management Plan
- Statement of Applicability
- Guidelines
- Templates/Formats

All ISMS documents and records are defined, maintained and controlled in accordance with the defined processes and guidelines

2.7 Internal Audits

Internal audits to verify the compliance of information security practices to ISMS and ISO 27001 requirements are conducted every quarter. Trained internal auditors conduct the audits. Internal Auditors independent of the practice/function being audited are deputed for conducting the audit. The planning and execution of audits are in accordance with the Internal Audit procedures of EPATHUSAISMS.

In addition to these audits, management has decided to be certified for compliance to ISO 27001 requirements. The chosen auditing agency shall depute certified and experienced auditors to evaluate the suitability of the Information Security Policy, ISMS and its implementation vis-à-vis the business requirements/ISO 27001 requirements. Such audits shall provide management with an independent review of information security

Related and support documentation
Information Security Audits Procedure

2.8 Management Review

Management Reviews are conducted once every quarter to review the continuing suitability, adequacy and effectiveness of ISMS. This review shall include assessing opportunities for improvement and the need for changes to the ISMS.

Management Reviews are coordinated by the Information Security Officer and chaired by the CEO. All Practice heads/Function Heads and Information Security Forum members are part of the Management Review Meetings.

The agenda for the Management Review Meetings shall include:

a) Results of ISMS audit and reviews;
b) Feedback form interested parties;
c) Techniques, products or procedures, which cloud be used in the organization to improve the ISMS performance and effectiveness';
d) Status of preventive and corrective actions;
e) Vulnerabilities or threats not adequately addressed in the previous risk assessment;
f) Follow-up actions form previous management review;
g) Any changes that could affect the ISMS; Recommendations for improvement.

The output from the management review shall include any decisions and actions related to the following:

1. Improvement of the effectiveness of the ISMS.
2. Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
    a. Business requirements;
    b. Security requirements;
    c. Business processes effecting the existing business requirements;
    d. Regulatory or legal environments;
    e. Levels of risk and / or levels of risk acceptance.
    f. Resource needs.

The minutes of the meetings are circulated to all the Management Review participants. The Information Security Officer tracks the actions points to closure.

2.9 Training

Employees shall receive appropriate training on the security policy and procedures including security requirements, business controls and disciplinary action, which may result out of non-compliance. The trainings will cover appropriate use of IT facilities, security policy, etc. Employees shall be kept aware of any changes to the security policies and procedures of the organization.
Information Security Training requirements are identified by the practice/function head and ISO/Information Security Forum and communicated to the Training Manager. Planning and execution of the training programs is in accordance with EPATHUSA ISMS.

2.10 Continual Improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

Continuous improvement is achieved through the following means:

- Identification of root causes for non-conformities of the implementation/operation of ISMS and taking appropriate corrective and preventive actions
- Identification of potential non-conformities their causes and implementing appropriate preventive actions
- Defining quantitative security goals and improve the ISMS to achieve the same.

Information Security Officer shall keep track of all corrective and preventive actions, their status and data pertinent to security goals. This data shall be analysed to verify whether satisfactory improvement of ISMS effectiveness is being achieved. The improvement of the effectiveness of ISMS is reviewed during the Management Reviews.

Security Goals

Metrics	Unit	Service level Objectives
Incident Call Resolution Duration		
Catastrophic-S1	Hours	2 hrs
Significant-S2	Hours	8 hrs
Minor-S3	Hours	24 hrs
Incident Call Response Duration		
Catastrophic-S1	Hours	.5 hrs
Significant-S2	Hours	4 hrs
Minor-S3	Hours	8 hrs

Sl. No	Security Metric	Objective
1.	No of Non-Conformance during ISMS Audit per projects or functions	< 4

Security Incident Type	Description
Catastrophic-S1	Unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations leading to substantial revenue/capital loss, third party liability, loss of reputation
Significant – S2	Unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations leading to moderate revenue/capital loss, third party liability, loss of reputation
Minor –S3	Unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations leading to insignificant revenue/capital loss, third party liability, loss of reputation

3 INFORMATION SECURITY POLICIES

3.1 Acceptable use policy

3.1.1 Purpose

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

3.1.2 Scope

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

3.1.3 Policy

3.1.3.1 Acceptable Use

- While EPATHUSA the IT Group desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of EPATHUSA. Because of the need to protect EPATHUSA network, management cannot guarantee the Confidentiality of information stored on any network device belonging to EPATHUSA.
- Employees are responsible for excising good judgment regarding the reasonableness of personal use. Individual functions are responsible for creating guidelines concerning personal use of Internet / Intranet / Extranet systems. In the absence of such policies, employees should be

guided by functional policies on personal use, and if there is any uncertainty, employees should consult their reporting manager.

- EPATHUSA recommends that any information that users consider sensitive or vulnerable be Password Protected/Encrypted.
- For security and network maintenance purposes, authorized individuals within EPATHUSA may monitor equipment, systems and network traffic at any time
- EPATHUSA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- Information Asset owners should identify and implement controls in accordance with ISMS to protect Confidentiality, Integrity and Availability of this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All users are bound by the Policies and Procedures defined in the ISMS while operating/handling information assets in EPATHUSA

3.1.3.4 Unacceptable Use

The following activities are, in general prohibited. Under no circumstance is an employee of EPATHUSA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing EPATHUSA- owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by EPATHUSA.
2. Unauthorized copying of copyrighted material including but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which EPATHUSA or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional exports control laws, is illegal.
4. Introduction of malicious programs into the network or server

   (Ex: Viruses, worms, Trojan horses, e-mail bombs, etc).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a EPATHUSA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile work place laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any EPATHUSA account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption "includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job / duty.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any other user

13. Providing information about, or lists of, EPATHUSA employees to parties outside EPATHUSA.

3.2 Password Policy

3.2.1 Purpose

Passwords are an important aspect of computer security. They are front line of protection for user accounts. A poorly chosen password may result in the compromise of EPATHUSA entire corporate network. As such all EPATHUSA employees (including contractors and vendors with access to EPATHUSA systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their Passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.2.2 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any EPATHUSA Admin, has access to the EPATHUSA network, or stores any non- public EPATHUSA information.

3.2.3 Policy

3.2.3.1 General

- All system – level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- All user–level and system–level passwords must conform to the guidelines described below. And password complexity option is enabled.
- Password Option on all servers shall require passwords to have a minimum of 8 characters and password complexity option is enabled

3.2.3.2 Guidelines for Construction of Passwords

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g. a - z, A - Z)
- Have digits and punctuation characters as well as letters (e.g. 0-9, @#$ %^&*() _+/ ~-=\′ {} :";'<>? /)
- Are at least eight alphanumeric characters long
- Are not words in any language, slang, dialect, jargon, etc?
- Are not based on personal information, names of family, etc.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage words such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc
- Computer terms and names, commands, sites, companies, hardware, software
- The words "EPATHUSA", "EPATHUSA", "OZONE", or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Words or number patterns like aaabbb, qwetry, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e. g., secret 1, secret)

NOTE: Do not use either these examples as passwords!

3.2.3.3 Password Protection Standards

All passwords are to be treated sensitive, confidential EPATHUSA information. The following precautions to be taken to protect the passwords

- Don' t reveal a password over the phone, in front of others or in an e-mail message/chat to ANYONE
- Don't hint at the format of a password (e. g., " my family name")
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don't use the "Remember Password" feature of applications (e.g. Outlook, Netscape messenger).
- Don't 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 any encryption.

3.3 Extranet Policy

3.3.1 Purpose

This document describes that policy under which third party organizations connect to EPATHUSA networks for the purpose of transacting business related to EPATHUSA.

3.3.2 Scope

Connections between third parties that require access to non-public EPATHUSA resources fall under this policy, regardless of technology used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for EPATHUSA or to the Public Switched Telephone Network does not fall under this policy.

3.3.3 Policy

3.3.3.1 Third Party Connection Request

Sponsoring Organizations within EPATHUSA that wish to establish connectivity to a third party are required to give a request accompanied by a valid business justification in writing approved by Practice/Function Head. The sponsoring Organization must provide full and complete information as to the nature of the proposed access and the expected duration of the connection to the Networking team, as requested.

All connectivity established must be based on the least- access principle, in accordance with the approved business requirements and the security review. In no case will EPATHUSA rely upon the third party to protect EPATHUSA network or resources

All new extranet connectivity will go through a security review with the Information Security Officer as well as the Networking Department's head. The reviews are to ensure that all access matches the business requirements in the best possible way, and that the principle of least access is followed.

3.3.3.2 Third Party Connection Agreement

All new connection requests between third parties and EPATHUSA require that the third party and EPATHUSA representatives agree to and sign the Third Party Agreement. This agreement must be signed by the authorized executive of the sponsoring organization as well as a representative from third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the Networking Department.

3.3.3.3 Point of Contact

The sponsoring Organization must designate a person to be Point of Contact (POC) for the extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the Third Party Agreements that pertain to it. Should the POC change; the relevant extranet organization must be informed promptly.

3.3.3.4 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification and are subject to security review by the Support Head as well as the Information Security Officer. Changes are to be implemented via corporate change management process. The sponsoring organization is responsible for notifying the IT Group and Information Security Officer when there is material change in the originally provided information so that security and connectivity evolve accordingly.

3.3.3.5 Terminating Access

When access is no longer required, the sponsoring organization within EPATHUSA must notify the Support Department, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate.

3.4 Router Security Policy

3.4.1 Purpose

This document describes a required minimal security configuration for all routers and Switches connecting to a production network or used in a production capacity at or on behalf of EPATHUSA.

3.4.2 Scope

All routers and switches connected to EPATHUSA production networks or used in a production capacity at or on behalf of EPATHUSA are covered under this policy.

3.4.3 Policy

Every router must meet the following configurations standards:

- No local user accounts are configured on the router. Routers must use TACACS+ for all user authentications.
- The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
- Disallow the following:
    a) IP directed broadcasts
    b) Incoming packets at the router sourced with invalid addresses such as RFC 1918 address
    c) TCP small services
    d) UDP small routing All source routing
    e) All web services running on router
- Use corporate standardized SNMP community strings
- Access rules are to be added as business needs arise.
- The router must be included in the corporate organization network with a designated point of contact.

3.5 Network and VPN Policy

3.5.1 Purpose

The purpose of this policy is to provide guidelines for Network access, Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the EPATHUSA corporate network.

3.5.2 Scope

This policy applies to all EPATHUSA employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing LAN, VPNs to access the EPATHUSA network. This policy applies to implementation of VPN that are directed through a EPATHUSA managed IPSec Concentrator.

3.5.3 Policy

Approved EPATHUSA employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of LAN/VPNs, which are a "user managed" service. Additionally,

- It is the responsibility of employees with LAN/VPN privileges to ensure that unauthorized users are not allowed access to EPATHUSA internal networks.
- VPN use is to be controlled using a symmetric Key system with a strong pass phrase that is provided by EPATHUSA for site to site VPN.

- VPN gateways will be set up and managed by EPATHUSA Support Department.
- All computers connected to EPATHUSA internal networks via VPN or any other technology must use the most up-to–date anti–virus software that is the corporate standard.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computer that are not EPATHUSA- owned equipment must configure the equipment to comply with EPATHUSAVPN and LAN policies.
- Only IT Group– approved VPN clients may be used.

3.6 Clear Desk/Clear Screen Policy

3.6.1 Purpose

The purpose of this policy is to provide guidelines ensuring that information assets are not made accessible inadvertently to non-authorized resources.

3.6.2 Scope

This policy applies to all EPATHUSA employees, contractors and consultants utilizing EPATHUSA information assets. Information assets include Correspondence, Corporate papers, computer media, manuals, drawings etc

3.6.3 Policy

- All information, other than "Sensitive", shall be locked in cabinets or fireproof cabinets when not in use. This is to ensure that confidential or restricted information is not accidentally left unsupervised in publicly accessible areas such as desks, printers etc.
- Documents should not be left unattended at Printers, Xerox, and Fax Machines and should be collected immediately.
- Users should use the facilities provided by the IT Group to protect unattended screens by use of a power on passwords and password-protected screensavers
- Staff should ensure their desks are clear every evening before leaving

3.7 Access Control Policy

3.7.1 Purpose

The purpose of this policy is to provide guidelines ensuring that access rights are provided on a need basis with minimum possible levels of access.

3.7.2 Scope

This policy applies to all EPATHUSA employees, contractors, and consultants utilizing EPATHUSA information assets / Networking facilities.

3.7.3 Policy

- Information Security Forum and Network administrator shall be responsible for creating and implementing access control procedure as per the configuration management plan.
- Terminals will be identified through unique IP addresses/System name.
- Practice / Function Heads approval is required to authorize issuance of user IDs and resources privileges.
- Only authorized users shall be allowed access to the information systems of the organization.
- Access rights for users shall be granted based on the following aspects:
  a) Sensitivity level of information;
  b) Information dissemination and entitlement policies e.g. "need-to-know" and "need-to-do" principles, segregation of duties, etc
- Access privileges will be individually defined for the different information systems (e.g. operating systems, databases, application systems etc) used in the organization. The access privilege will be based on the organizational needs and the security requirements specific to that information system.
- The Network Administrator shall periodically review the Access control system

- Configuration plan defines the access requirements for individual departments to perform the business functions.
- User should be able to login to their desktop only.

3.8 Electronic Mail Policy

3.8.1 Purpose

The purpose of this policy is to ensure that the employees use e-mail in a secure manner and the information transmitted through the mail network is secure and its use does not expose the organization to any risks.

3.8.2 Scope

This policy applies to all EPATHUSA employees, contractors and consultants utilizing EPATHUSA e-mail accounts.

3.8.3 Policy

3.8.3.1 E-mail usage

- Email ID naming convention and signature will be followed as per the following standards decided by Information Security Forum.

  The name of the Employee will form the basis for his email ID. The E-mail Id creation process is initiated. The Project manager triggers the process by filling in the New Employee Infrastructure Request Form and sending it to the HR who in turn will request the IT Department to create an E-Mail Id.

  E-mail Id is created as: first name followed by period and the last name

- No employee shall be permitted to use any other email account for official communication.
- The users will exercise extreme caution while sending e-mails through the public networks. Guidelines will be issued to educate users on the secure and acceptable use of the corporate e-mail account. http-SSH layer over RPC over http

3.8.3.2 Remote access to e-mail account

Users shall be able to access s their e-mail account from outside the corporate network only after passing through a designated authentication mechanism.

3.8.3.3 Usage of internet-based mail accounts

- Employees should not use any e-mail account other than the corporate account for official communications with external users.
- All exceptions shall need specific authorization by the department head/CEO.

3.8.3.4 Encryption of mails

- Users should not send any confidential information through e-mail unless it is encrypted or the attached document is protected from unauthorized access by means of a password.

3.8.3.5 Monitoring

- The organization may, for reasons of security, intercept or otherwise monitor the mails sent through its mailing system.
- CEO shall have the authority to approve monitoring of corporate mail of employees.

3.8.3.6 Disclaimer information

All e-mail sent from the organization’s mail system shall have a standard “disclaimer statement” attached to it.

3.8.3.7 Unacceptable Email and Communications Activities

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email Spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi or other "pyramid "schemes of any type.
6. Use of unsolicited email originating from within EPATHUSA networks of other Internet / Intranet Extranet service providers on behalf of, or to advertise, any service hosted by EPATHUSA or connoted via EPATHUSA network.
7. Posting the same or similar non-business – related messages to large numbers of Usenet groups (newsgroup Spam).

3.9 Acceptable Encryption Policy

3.9.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those EPATHUSA algorithms that have received substantial public review and have been proven to work effectively.

3.9.2 Scope

This policy applies to all EPATHUSA employees and affiliates.

3.9.3 Policy

Encryption shall be mandatory for site-to-site network traffic on VPN. Encryption of data on FTP servers, E-Mail shall be optional depending on contractual requirements
Proven, standard a EPATHUSA Algorithms 3DES, RSA, DES, SHA should be used as the basis for encryption technologies. These EPATHUSA Algorithms represent the actual cipher used for an approved application. Encryption mechanisms which use a minimum of 56 bit encryption shall be adopted.

3.10 Mobile Computing/Tele-Working/Laptop Policy

3.10.1 Purpose

The purpose of this policy is to define standards for connecting to EPATHUSA network from any host. These standards are designed to minimize the potential exposure to EPATHUSA from damages, which may result from unauthorized use of EPATHUSA resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to critical EPATHUSA internal systems, etc.

Also, Laptop computers, together with their data, are becoming an increasingly common target for thieves and EPATHUSA is keen to protect all its assets and the information these assets might hold. Apart from the financial impact arising from cost of replacement laptops, there are "hidden" costs associated with the following:

- lost productivity
- procurement
- laptop set-up
- data replacement

3.10.2 Scope

This policy applies to all EPATHUSA employees, contractors, vendors and agents with EPATHUSA–owned or personally – owned computer or workstation/Laptops used to connect to the EPATHUSA network. This policy applies to remote access connections used to work on behalf of EPATHUSA, including reading or sending email, and viewing intranet web resources and using Laptops.

Remote access implementation that are covered by this policy include, but are not limited to, dial–in–modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.10.3 Policy

3.10.3.1 General

- It is the responsibility of EPATHUSA employees, contractors, vendors and agents with remote access privileges to EPATHUSA corporate network to ensure that their remote access connection is given the same consideration as the users-on–site connection to EPATHUSA.

- General access to the Internet for recreational use by immediate household members through the EPATHUSA Network on personal computers is permitted for employees that have flat-rate services. The EPATHUSA employee is responsible to ensure the family member does not violate any EPATHUSA policies, does nor perform any illegal activities, and does not use the access for outside business interests. The EPATHUSA employee bears responsibility for the consequences should the access is misused.
- ISMS policies provide details of protecting information when accessing the corporate network via remote access methods, and acceptable use of EPATHUSA network

3.10.3.2 Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication with strong pass-phrases. For information on creating a strong pass-phrase see the password policy.
- At no time, should any EPATHUSA employee provide their login or email password to anyone, not even family members.
- EPATHUSA employees and contractors with remote access privileges must ensure that their EPATHUSA-owned or personal computer or workstation, which is remotely connected to EPATHUSA corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- EPATHUSA employees and contractors with remote access privileges to EPATHUSA corporate network must not use non – EPATHUSA email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct EPATHUSA business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN line configured for access to the EPATHUSA network are only on a case-by-case basis and must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of spilt-tunneling or dual homing is not permitted at any time.
- Non-standard hardware configurations must be approved by the Support Department, and the IT Group must approve security configurations for access to hardware.
- All hosts that are connected to EPATHUSA internal networks via remote access technologies must use the most up – to date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.
- Personal equipment that is used to connect EPATHUSA networks must meet the requirements of EPATHUSA-owned equipment for remote access.
- Organizations or individuals who wish to implement non–standard Remote Access solutions to the EPATHUSA production network must obtain prior approval from the Network administrator as well as the Information Security Officer.
- Applying technology controls (for example authenticated login, password aging and virus checking) to protect access to information on laptops.
- Restricting access so that software cannot be installed by users
- Requiring staff to sign a "Laptop / Mobile Device Loan Form/NDA" to confirm that they will abide by this policy and the guidelines.

4 INFORMATION SECURITY PROCEDURES

4.1 General Admin Department

4.1.1 Physical Security

4.1.1.1 Security Arrangements

- The security perimeter for the organization is identified and documented
- Areas which require additional physical security (e.g. Server rooms or where sensitive equipment is located) controls are identified and documented
- Security guards shall be posted at all entry points and manned round the clock

- The Head-Admin will enter into a contract with a Security Agency, which has been evaluated for their ability
- Head-Admin will maintain an approved list of personnel from this agency after scrutinizing profiles (and police records if possible) of these personnel.
- Head-Admin will ensure that these agencies send only those personnel who are on the approved list for guard duty
- Access to secure perimeter and additional secure areas shall be through an access control system

4.1.1.2 Employee Access

- Admin Group shall provide employee access card to all employees.
- All employees are required to use their Cyber Lock codes to access the suites.
- HR shall intimate the Admin Group regarding the new employees who have joined service and the office/area to which access is required
    - Admin Group shall arrange for a photo access card and get the access control system activated for the new card
    - On separation of an employee from the organization, HR shall intimate Admin the last working date of the employee
    - Admin Group shall collect the access card and store it in a secure location until the access card is disabled on the access control system
    - Access Control System shall be updated immediately to disable cards of employees who left the organization

4.1.1.3 Visitors/Guests/Prospective Employees Access

- All visitors/guests are to report at the security/reception area
- Details of visitors/guests shall be entered into the "Visitors Register" with the front desk
- Front Desk person shall call up the employee for whom the Visitor/Guest had come to confirm the appointment/availability
- The guest/visitor shall be seated in the reception area until the respective employee authorizes the entry into working area
- The front desk person shall take back the visitor access card and note down the out timing when the visitor leaves the premises
- Employees are expected to accompany visitors/guests to ensure that they are permitted to visit only authorized areas and do not cause damage to organizations equipment or pose security threat

4.1.1.4 Third Party/Vendors access

- Third Parties/Vendors may need to have access to the secure perimeter to deliver material/services
- All such personnel are to report at the security/reception area
- Details of Third Parties/Vendors personnel shall be entered into the "Visitors Register" with the Security Guard
- riskSecurity guard shall call up the relevant department head for whom the Material/Service is being provided to confirm the appointment/availability
- A visitor access card shall be provided and shall be worn until these personnel leave the premises
- The Third Parties/Vendors personnel shall be seated in the reception area until the respective employee authorizes the entry into working area
- A list of people who are authorized to take Third Parties/Vendors personnel into the working areas is identified and provided to the security guard by Head-Administration
- The security guard shall take back the visitor access card and note down the out timing when these personnel leaves the premises
- Employees are expected to accompany Third Parties/Vendors personnel to ensure that they are permitted to visit only authorized areas and do not cause damage to organizations equipment or pose security threat

- Third Parties/Vendors who need to have access to organizations information assets for a longer term are required to sign a Non Disclosure agreement and have their employees deputed to the organization screened as per the requirements specified in "Personnel Screening and Referencing" procedure in this document.

4.1.1.5 Inward/Outward Movement of Equipment

- All equipment/material to be delivered to the organization is received at the security/reception area
- The Security Guard will maintain a Material inward/outward register to log items being brought into the secure perimeter and being taken out
- Security Guard shall inform the relevant employee for whom the material is received
- The employee shall receive the material and authorize the same to be brought into the work area for use/storage
- For moving equipment, gate passes shall be issued at the sending point and checked at the receiving point.
- A list of employees who are authorized to sign the gate passes and their specimen signature shall be approved by the CEO and provided to the Security Guard
- Head-Admin shall track the return of equipment which have been moved out on returnable basis
- Equipment, which is under customs bonding, shall not be moved out of the bonded premises without appropriate permissions from the STPI/Central Excise authorities
- Equipment/Media being transferred between different premises within the security perimeter shall be suitably packed and transferred along with one of the organizations employee.

4.1.1.6 Equipment Sitting and Protection

- Head-Admin shall ensure that equipment which have high value/high risk value (e.g. Servers, Costly hardware, Software) are located at segregated work areas/sites with additional security or stored under lock and key
- The precautions to be taken for such equipment shall include controls which protect from theft/vandalism, unauthorized access and environmental threats/hazards
- Unattended Equipment such as Printers/Fax/Xerox machines/Systems in common places will be suitably protected by mechanisms such as passwords/access key

4.1.1.7 Power Supplies and Cabling Security

- Head – Admin shall ensure that all cabling (Power, Communication, Network related) is done in a secure manner meeting the equipment manufacturers specifications and is protected from tapping, tampering, accidental damage and environmental hazards
- Head – Admin shall ensure that all power switches, power mains are protected from tampering, accidental damage and environmental hazards
- Proper earthling should be provided to all power supplies/racks/work areas where equipment is sited
- All critical equipment are connected to UPS to support continuous running/orderly close down
- A backup generator is installed for supplying power when the power fails for longer periods than which UPS can support.
- Lightning protection filters should be fitted to all external communication lines

4.1.1.8 Equipment Maintenance

- All new/critical equipment under the control of General Administration will be tracked for their warranty/Annual Maintenance Contract using an AMC Tracker
- Equipment which require preventive maintenance/periodic checks (e.g. Generator, UPS, Air-conditioners, Fire Extinguishers etc.) shall be identified and tracked
- Details of Preventive maintenance/periodic checks are tracked using the Preventive Maintenance Tracker

4.1.1.9 Security of Equipment off premises

- Equipment containing data, media should not be taken off premises (excludes transfers between different premises within the defined security perimeter) without written approval from the CEO
- Equipment/Media taken out of premises should not be left unattended in public places without suitable protection measures such as passwords, physical barriers or security guards
- Equipment/Media should be packed and sealed suitably to ensure that they are not damaged/tampered/misused

4.1.1.10 Secure disposal or re-use of equipment

- Equipment before being disposed/reallocated shall be reviewed by Head-IT and Head-Admin departments to assess the risk and take steps to remove data/licensed software
- Equipment being disposed shall be recorded using Equipment disposal register
- Media shall be disposed by using appropriate shredding mechanisms to prevent reuse/restoration.

4.1.1.11 Safeguarding of organizational records

- Organization records of value shall be identified and stored using appropriate security mechanism. Suitable backups will be taken and maintained (including storing of backups offsite)
- All organizational records shall be kept in accordance with the configuration and data management process
- A configuration management plan identifying all the records and access rights to data/applications is available in the Project Management Plan (PMP).

4.1.2 Information Assets Inventory & Management

- A detailed inventory of EPATHUSA assets will be maintained. The inventory is to contain security classification and Customs bonding status of items.
- Head-Admin maintains the inventory of all computer systems / printers / computer media / licensed software/UPS/Communication equipment related to networking
- Head-Admin maintains the inventory of all other capital equipment/material in the organization
- All assets are identified with a unique asset id. Asset id is inscribed on the asset for identification and traceability
- The asset list id documented using the Asset Register

4.2 HR Department

4.2.1 Personnel screening and referencing

- Appropriate measures shall be instituted to verify the history of the applicants and any background information that may be useful for decision-making
- The references given by a candidate shall be used for thorough screening of the individual before recruiting them.
- Suitable investigations shall be carried out if there are triggers or potential misrepresentation.
- At least one background reference check shall be required before recruitment of the person.
- Similar screening procedures shall need to be carried out for the vendors/contractors and temporary staffs that need to have access to critical information assets.
- Firms providing contract employees would be required to provide written agreements stating that appropriate personnel and business references have been obtained and verified.
- Temporary staff will only be allowed limited access to the organization's systems and their activities will be monitored on an on-going basis.

4.2.2 Employee appraisal

- Adherence to the Information security policy shall form an integral part of the employee performance evaluation.

- HR/Reporting Manager shall refer to disciplinary actions taken against the employee as one of the evaluation parameter during appraisal
- The ability of the employee to conform to organizations ISMS policies shall be the basis for confirmation, promotion and assignment of critical duties.

4.2.3 Terms and condition of employment

- Adherence to security policy and participation in security initiatives shall be included in the terms and conditions of employment for all employees.
- In particular, all information system users of the organization will sign-off on a commitment to adhere to the Information security Policies as defined by the organization.
- All employees, temporary staff and consultants shall be required to sign confidentiality and/or nondisclosure agreement binding them not to disclose any information about the organization without prior written permission.
- All employee information will be kept strictly confidential and will be shared only on need basis with specific approval from CEO
- Recruitment Process

4.2.4 Training Procedure

- Role based training is provided to an individual before the assignment to that role.
- Induction training is mandatory for all newly joined employees, and is organized by the HR Department. Induction training includes ISMS awareness as part of the curriculum.
- Respective department head and Information Security officer shall identify training requirements for information security education/ISMS implementation awareness
- Executive - HR consolidates the training requests received and prepares a training calendar. This is reviewed periodically and updated to ensure that the requirements received subsequently are addressed.
- The training requirements are addressed in accordance with the Training Procedure of EPATHUSA ISMS.

4.2.5 Disciplinary Process

- A disciplinary committee is constituted by the CEO to examine disciplinary issues related to information security practices.
- The disciplinary committee is headed by the CEO and includes ISO, Head-HR and the specific department head.
- The disciplinary committee collects and examines necessary evidence through System Logs, Log trails, e-mails and any other suitable mechanism. Evidence collected shall confirm to permissible evidence requirements of law of the land
- The disciplinary committee is convened whenever a security incident warrants disciplinary action as part of the corrective and preventive measures.

4.2.6 Segregation of duties

- All sensitive duties shall be segregated so as to guard against negligent or deliberate misuse of data systems or services.
- As a good practice, it will be ensured that the following responsibilities are allocated to different personnel
  - a) Audit function for the same department/project
  - b) Systems Administration and Resource Allocation/Network Configuration Approval
  - c) Systems Administration and Operator log verification

4.2.7 Data protection and privacy of personal information

- Personal records shall be identified and stored using appropriate security mechanism. Suitable backups will be taken and maintained (including storing of backups offsite)

- All personal records shall be kept in accordance with the configuration and data management process
- A configuration management plan shall be prepared identifying all the records and access rights to data/applications

4.3 Networking Department

4.3.1 Specialist Information Security Advice

- ISO/Head-Admin identifies areas which require specialist security advices
- A list of security advisors and the areas on which they could provide advice shall be documented and maintained by the ISO
- The specialist security advisors can be part of the organization or external consultants/vendors.

4.3.2 Cooperation with information service providers and telecommunications operators

- Head-Admin maintains a list of critical service providers and their contact details
- Where required service levels are negotiated and documented as part of the service contracts
- Head Networking also takes membership or becomes part of security groups/industry forums to obtain advice in the event of a security incident.

4.3.3 Acquisition of Information Assets/Outsourcing

- Security and control features shall form part of every Information Assets (Hardware/Software) acquisition process.
- The indenter for the Information Asset shall be responsible for the effective planning and monitoring of inclusion of security requirements as one of the key requirements in the acquisition process.
- The indenter shall identify the security requirements by discussing the same with the Network Administrator and the Information Security Forum.
- These requirements shall be specified in the purchase order.
- Sr. Management shall approve material request as well as the purchase order before the purchase is done.
- Information Assets will be accepted only if they meet the criteria specified in the purchase order.

4.3.4 Third Party Access

4.3.4.1 Contracts

- The organization shall enter into legally binding contracts with all third party service providers.
- Maintaining the security of the organization's information assets will be a part of the contractual commitments.

4.3.4.2 Access to internal resources

- Third parties' access to the organization's IT facilities would be determined based on the business objectives of the services provided.
- CEO shall approve all requests for access to third parties
- A risk analysis would be carried out to assess the security implications of giving access to internal IT resources.
- Appropriate controls shall be identified and implemented to ensure that the risks identified are sufficiently mitigated
- The details of third party access provided and controls implemented are recorded using the Third Party Access register

4.3.4.3 Monitoring mechanisms

Information Security Officer shall be responsible for monitoring implementation of the identified controls.

4.3.5 Reporting Software/Hardware Malfunctions

- All users of the computing infrastructure shall report software/hardware malfunctions to the Head-Admin/Project manager or the on duty systems administrator

- All software/hardware malfunctions are recorded and tracked using the Service Request Log
- The allocated systems administrator shall resolve all such issues as per the agreed service levels and intimate the user
- Head-Admin shall analyse the reported software/hardware malfunctions for identifying vulnerabilities/weakness which can compromise the information security and implement necessary controls

4.3.6 Incident Management and Learning from Incidents

- All users of information systems in the organization shall be trained to identify and report security incidents and security weaknesses
    - **Security incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system
    - **Security weakness** means the unidentified vulnerabilities and threats that could lead to unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system
- A mail id @EPATHUSA shall be created where all users are required to report security incidents
- Contact numbers of Information Security Forum members are available in organization contact sheet
- MR/ISO shall receive the copy of incidents reported to the above mail id
- MR/ISO shall log all security incidents into the Incident Tracker. MR/ISO in consultation with the Asset Owner and Management shall identify immediate actions and Corrective/Preventive actions to be implemented
- The action points, responsibility and the planned completion schedule shall be logged in the Incident Tracker
- MR/ISO tracks all the action points to satisfactory closure
- Causal Analysis of security incidents are done on a monthly basis by the MR/ISO and appropriate controls are identified and implemented to prevent recurrence of such incidents or mitigate the impact of such incidents
- Causal Analysis findings and action taken are disseminated to all Information Security Forum Members and discussed during the Management Review meetings

4.3.7 Secure Disposal or re-use of equipment

- As described in Section 4.1.1.10

4.3.8 Removal of Property

- As described in Section 4.1.1.6

4.3.9 Operational Change Controls

- Changes to Network/Hardware/OS/Application Software configurations shall be initiated based on the business requirements by the respective department head and approved by the CEO
- The approved changes shall be communicated to the Head-Admin for implementation
- All such service requests shall be logged and tracked using the Service Request Tracker
- All changes to Network/Hardware OS/Application Software configurations shall be evaluated for impact/new security risks and appropriate actions taken

4.3.10 Separation of development and operational facilities

- Development and operational servers for internal applications shall be configured on different systems. Where such segregation is not feasible the development and operational areas may be segregated using appropriate access control mechanisms
- Source Code, Documents, Test Data and any other work products shall be protected from unwarranted changes using appropriate access control mechanisms/configuration management tools such as VSS.
- The access control mechanism and the access rights for such work products are defined in the Configuration Management Plan.

4.3.11 External IT System

- As described in Section 4.3.4 and 4.1.1.4

4.3.12 Capacity Planning

- Computer and network capacity requirements shall be regularly monitored to ensure that the business does not run the risk of failure due to inadequate capacity.
- Capacity planning shall also be conducted for all new systems being acquired. The performance of systems shall be periodically monitored to ensure that they meet the business expectations of service Information Security.
- Management shall identify annually the facilities required for future business functions.

4.3.13 Controls Against Malicious software

- Antivirus software shall be deployed at 3 levels [Gateway, All Servers and Desktop.]
- Inbound and outbound data traffic through Gateway shall be scanned for Virus before its transmission.
- The Antivirus software deployed shall be reassessed every half year for its effectiveness.
- Information on incidence of virus shall be shared with the Information Security Forum members.
- Freeware and unsolicited software shall not be used without prior permission of the Practice/Function Head.
- CD's and floppies shall not be used / accessed in a networked PC without prior approval of Practice/Function Head.
- The IT Group shall ensure that all servers and workstations have anti-virus software installed on them.
- The anti-virus software will be periodically updated with the latest patch released by the vendors.

4.3.14 Information Back-up

- The IT Group is responsible for the backup of data and periodic recovery testing as per Back up Recovery policy which includes plan for the same.
- The IT Group takes backup in accordance with the backup plan and maintains records of backup taken.
- Data that is no longer required on the file servers (e.g. after completion of project, obsolete data) is archived.
- A request for archival is sent to The IT Group in writing by the Project Manager/Function Head indicating the location of the data, names of folders/files to be archived and the duration for which the data needs to be retained.
- The IT Group will archive the data using suitable media and handover the same to the Practice/Function Head.
- Media used for backup will be suitably labeled. The date from which the media is being used and the expiry date beyond which the media can't be used will be tracked.

4.3.15 Operator Logs

- All Systems administration activities (including but not limited to User registration, access rights management, Hardware/Software/Network installation, configuration and trouble shooting) shall be performed only after due authorization and logging the service requests in the Service Request Register. Evidence of approvals, where required is maintained.
- In addition event logs activated on all key systems/applications shall provide evidence of Systems Administration activities in addition to the business activities performed. Refer to Section 4.3.43

4.3.16 Network Controls

4.3.16.1 Network Documentation

- The Logical and Physical network diagram along with data and electrical cable layouts of all offices shall be documented.

- These diagrams shall clearly indicate the logical connections and physical locations of the equipments on the network including hosts, hubs, routers, bridges, servers
- A clear description of the security attributes of all network services used by the organization shall be provided. The documentation shall also highlight various network links between EPATHUSA its clients, Internet, group companies, etc.
- Authorized personnel are only allowed access to these documents.

4.3.16.2 Network security

- Controls shall be implemented to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems.
- Information Security Officer shall be responsibility for monitoring the security of the local and wide area network including access to third party and/or public networks across the organization.
- Periodic testing and reviews shall be conducted to assure the management of the security of the corporate network. Computer and network management activities shall be closely coordinated to ensure that security measures are consistently applied across the Networking & IT infrastructure.
- Network may be segregated into sub-networks based on business requirements and clients security requirements

4.3.17 Management of Removable Computer Media

- Only authorized staff shall have access to the removable storage media (DAT, DLT etc.).
- All data storage media will be stored in a safe, secure environment. All storage media will follow a uniform labeling scheme to ensure that the correct unit is easily identifiable when needed.
- All movement of storage media outside of its original location must be duly authorized as explained in 4.1.1.5.
- The media movement will be logged to maintain an audit trail.
- Storage media such as DAT/DLT etc should be tested for readability at regular intervals.
- All computer media/equipment's shall be disposed off safely and securely when no longer required. The IT Group/Facilities Group shall review equipment to be disposed off at least once every quarter.
- IT Group will disable all removable storage media like floppy drives, cd drives, and USB ports from desktops/laptops/peripherals. Based on need basis access would be provided.
- Infrared / Bluetooth ports shall be disabled from desktops/laptops/peripherals. Based on need basis access would be provided.

4.3.18 Disposal of Media

- Media before being disposed/reallocated shall be reviewed by Head-Admin and Head-Admin departments to assess the risk and take steps to remove data/licensed software
- Media being disposed shall be recorded using Computer-Media Removable Disposal Form.
- Media shall be disposed by using appropriate shredding mechanisms to prevent reuse/restoration.

4.3.19 Security of media in Transit

- Any media such as DVD/CD/Hard Disks or any other removable media and systems containing data shall be packed and sealed using appropriate mechanism before being shipped any where outside the secure perimeter
- NDA with vendors who will be required to handle/service/transport such media shall be obtained
- Encryption /Password protection options may be used where required

4.3.20 Information Handling Procedures

- Information assets of the departments and their classification is identified and documented using the Asset Register
- Storage location, access rights and handling procedures if any (other than the document and data control procedure) shall be defined in the Configuration Management Plan
- All information assets shall be labelled as per the asset labelling guideline

4.3.21 Security of System Documentation

- Documentation pertaining to application systems, operating systems and any application software used by the organization shall be identified and listed e.g. User and Installation Manuals, Design documents etc.
- Storage location, access rights and handling procedures if any (other than the document and data control procedure) shall be defined in the Configuration Management Plan of the respective department holding such documents

4.3.22 Information and Software Exchange Agreements

- In cases where exchange/delivery of information/software to the clients is stipulated contractually the same are documented in the contract/agreement with the client
- The projects/departments procedures/plans (e.g. Configuration Management Plan) shall identify the exchange/delivery mechanism and any specific security requirements during the transfer
- The respective project/department head shall be responsible for compliance with the contractual requirements

4.3.23 Security of Electronic Office Systems

- Electronic office systems such as Fax, VOIP, Phone lines shall be secured. Fax machine shall be located in a locked cabin with supervision
- VOIP lines and Phone lines with direct dialling facilities are provided on a need only basis.
- Mail/Courier being received /sent is registered using the Mail register and forwarded to the addressee. Acknowledgement of receipt is obtained
- Users of electronic office systems shall be sensitised to the risks associated with these systems while transmitting confidential data to enable them take suitable precautions

4.3.24 Publicly Available Systems

- Publicly available systems such as company's web site, FTP and mail servers shall be protected from unauthorized modifications/hacking
- Content to be placed on such servers and access to the content is provided on need only basis. Access rights for such systems are defined in the Configuration Management Plan of the respective department
- Where such systems are maintained by third party service providers controls mentioned under Third Party Access shall be applicable

4.3.25 other forms of Information Exchange

- As per section 4.3.23

4.3.26 User Registration and Privilege Management

- New employees joining the organization shall be provided with user id/mail accounts based on their role/responsibilities.
- HR shall intimate the respective department, Networking and Admin Groups of new employees joining details. Details of whether the new joiner is a direct employee of EPATHUSA or a contract employee shall be communicated by the HR explicitly.
- IT Group in consultation with the respective department head shall identify the access rights to the various servers/application systems (includes but not limited to operating system, data base management system and each application) and provide the same. In case of contract employees, the department head shall identify the differential access rights that need to be provided and communicate the same to IT Group
- Subsequent modifications to access rights are made based on written requests sent by the respective department head. Where common user id's have to be used for business purposes appropriate controls such as transaction logging/monitoring shall be enabled.
- Where fixed user id's are provided to application systems or servers due to business reasons, access rights are reviewed and passwords modified before they are reallocated to another employee.

- Whenever an employee leaves the organization, his/her user id and mail account shall be disabled/deleted/reallocated with immediate effect upon receiving intimation from the Department Head. Network administrator shall take over the resources after getting a clearance from the respective Department Head and shall take a backup of the data as instructed.
- All requests for user registration/modification/removal shall be logged and tracked using the Service Request Register

4.3.27 User Password Management & Password Use

- Passwords shall be defined and used in accordance with the Password Policy 3.2.3.2.
- Password policies on servers, application systems shall be in accordance with the Password Policy defined in the ISMS

4.3.28 Review of user access rights

- User access rights to various servers, systems and applications are in accordance with the Configuration Management Plan.
- Actual User access rights vis-à-vis the definition in the Configuration Management Plan are reviewed during the ISMS internal audits conducted periodically
- Any deviations are recorded as Non-Conformances and appropriate corrective and preventive actions are taken

4.3.29 Unattended User Equipment

- Unattended user equipment (including equipment installed and not allocated to anyone) shall be secured using one or more of the following controls
  a) Hardware Level/OS Level password access
  b) Lock and Key
  c) Disabling the system
  d) Removal of Network/Power connections
- Head-Admin shall verify the physical condition of such equipment periodically to identify any tampering/physical loss of such equipment

4.3.30 Enforced Path

- All local network connectivity/access are routed through Linux Server (Samba server). Linux Server authenticates and authorizes the use of network resources as per the defined access rights.
- All WAN connections are routed through the gateway. Gateway authenticates and authorizes the network traffic as per the defined access rights on the firewall.

4.3.31 User authentication for external connections

- All external users of the organizations network shall be routed through the VPN and authenticated by the Firewall and Linux Server (Samba Server) before being provided access to the internal network resources
- Requests for external connections shall be approved by the CEO and forwarded to Head-Admin. All such requests are logged and tracked using the Service Request Register.
- All such access rights provided will be recorded in the Access Register.

4.3.32 Node authentication

- As per Section 4.3.30 / 4.3.31

4.3.33 Remote diagnostic port protection

- All ports including remote diagnostic ports shall be scanned for periodically using suitable tool
- Ports which are not required to be open are disabled
- USB, Parallel and Serial ports not required to be operational on systems/servers shall also be disabled

4.3.34 Segregation in networks

This is not applicable as Domain Controller is not used at EPATHUSA.

4.3.35 Network connection control

- As per Section 4.3.30/ 4.3.31

4.3.36 Network Routing Control

- As per Section 4.3.31

4.3.37 Security of network services

- As per Section 4.3.16.1

4.3.38 Automatic Terminal Identification

- All terminals are identified with a unique IP address. /system name

4.3.39 Terminal Log-on procedures

- All servers/systems/applications shall be accessible only after an appropriate logon and authentication has been performed.

4.3.40 User Identification and authentication

- As per Section 4.3.26

4.3.41 Password Management System

- Passwords for Servers and Applications/Software Utilities shall be implemented and controlled in accordance with the Password policy
- Passwords which are system generated may sometimes not comply with the requirements of EPATHUSA Password policy (applications given by client, procured before implementation of ISO 27001, proprietary software). In such instances IT group shall ensure that passwords are immediately changed to comply with the requirements of the password policy. Where the application doesn't support enforcement of EPATHUSA password policy the owner of the application shall define the specific password policy in the Configuration management plan.

4.3.42 Use of System Utilities

- Only authorized users shall be given access to system utilities that allow "super user" or "administrative' functions like backup, network monitoring etc.
- The activities of all such power users and system utilities shall be closely monitored and extensively logged.

4.3.43 Terminal time-out

Not applicable

4.3.44 Information Access restriction

- As per Section 4.3.26 and 4.3.28

4.3.45 Sensitive System Isolation

- Sensitive systems/hardware such as Servers, Routers and Switches are segregated and kept in Server Rooms
- Server rooms shall have additional secure perimeter and access is restricted through lock and key/access control mechanisms

4.3.46 Event Logging

- The log files for all critical servers/equipment (Operating Systems) and applications systems shall be enabled to track the activities /transactions performed on the system
- The systems for which logs shall be maintained, the retention period and the review frequency/responsibility shall be defined in the System Logs Tracker

4.3.47 Monitoring System Use

- As per section 4.3.46

4.3.48 Clock Synchronization

- All systems clocks will be synchronized with a central system to enable reflection of accurate time & date
- Windows Times Service on Domain Controller shall be used to synchronize all the desktops clocks with the server clock
- The Domain controller clock shall be synchronized with one of the Internet Time Service

4.3.49 Mobile Computing & Teleworking/Laptop

- As per Mobile Computing & Teleworking Policy as per 3.10

4.3.50 Systems Development and Maintenance

- Security and control features shall form part of every systems acquisition process.
- A business sponsor shall be identified for all new systems developments. He/she shall be responsible for the effective planning and monitoring of inclusion of security requirements as one of the key issues in the systems development process.
- The business sponsor is to understand the security requirements before the development of any system shall carry out user requirement analysis.
- The Information Security Forum shall review the security requirements identified before they are finalized.
- The business sponsor shall identify agree, and sign-off on specific security functionalities and security requirements of the system before commencement of the development process.
- Business Sponsor shall designate resources for testing at relevant EPATHUSA during the systems development and shall include security testing of the system.
- Rules for the migration of software form development to operational status shall be defined and documented (Acceptance Criteria).
- Application developers must ensure their design/programs contain the following security precautions where applicable.
  a) Should support authentication of individual users, not groups.
  b) Should not store passwords in clear text or in any easily reversible form.
  c) Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password
  d) Application shall provide the appropriate level of data integrity checking, both at input EPATHUSA and also when data are processed
  e) Where data is entered manually the application should reject incorrect values such as out of range, invalid characters and incomplete data
  f) Where appropriate message authentication is performed
- In case the application system proposed to be acquired does not satisfy the requirements of effective security and controls, mitigating controls shall be built in the application itself or in the business processes governing its use
- A formal change control procedure shall be followed to facilitate changes proposed to the finalized requirements.
- An appropriate authority should authorize all change requests.
- Adequate testing will be conducted before implementing any change on the 'live' system and test data will be protected against corruption and deletion. All relevant systems documentation will be updated to reflect changes made to the systems.
- The Network Administrator & Information Security Officer will ensure that all systems acquired are implemented along with the required controls identified.

4.3.51 Encryption

- The SSL encryption technology shall be used for encrypting messages exchanged thru email.

4.3.52 Non-repudiation service

- Clock Synchronization, Server Logs, Application software logs shall provide evidence of transactions/activities

4.3.53 Control of operational software

- The IT Group tracks the patches being released to the various operating systems and application software used by the organization. The updates for the same are obtained either through automatic mechanisms or manually as deemed appropriate. Where installation of such patches can have adverse impact on the business activity the same are tested before installation.
- The patch update activities are recorded in the Service request register

4.3.54 Protection of system test data

- As described in Section 4.3.10

4.3.55 Access control to program source library

- As described in Section 4.3.10

4.3.56 Security in Development and Support Processes

- Change Management will be carried after review and authorization.
- Access control policy defined as per 3.7.
- Software applications used for conducting the business operations are evaluated for undesirable code. If software is not evaluated the same may contain undesirable code/results for production systems

4.3.57 Business Continuity Management

- The organization shall ensure that the BCP be derived with active involvement of Management Review Committee to ensure its wide acceptance.
- The criticality of a computer application or business systems in use to support business process and services should be used to determine the necessity and priority for recovery of an application system.
- Information Security Officer shall ensure that plans are developed which allow the recovery of business process within a defined timeframe.
- The plans shall have to address the following issues:
  a) Identification and prioritisation of critical business processes
  b) The potential impact of various types of disaster on business processes
  c) Accommodation and communications arrangements
  d) Responsibility and authority for invocation and
  e) User awareness.
- The organization shall ensure that the documents of continuity and recovery plans and backups of all critical applications and data are available to the staff responsible for implementation of BCP during a business disruption or a disaster.
- The 'offsite' for such BCP documents will be set up at a location, which can be easily accessed during any emergency.
- A copy of the most critical software, application programs, data, documentation, and other contingency/disaster records should also be kept off site.
- Copies of the continuity/recovery plans, critical documents, records and manuals should be kept offsite in printed form by the personnel responsible for invocation of continuity plan during a disruption.
- The contract or service level agreement with the third party service providers will include requirements of business continuity and disaster recovery of the organization's data where feasible.

  Refer to Business Continuity Planning

4.3.58 Compliance with Legal Requirements

- The Information Security Forum in consultation with the Practice/Function Heads shall identify the legislative as well as the regulatory requirements to be met by the organization
- These shall include requirements pertaining to Intellectual rights, copyrights also.
- Information Security Officer shall be responsible for ensuring that the organization complies with all legal and statutory requirements pertaining to information security as and when they are in force.
- A list of applicable legislative and regulatory requirements are maintained by the Information Security Officer
- The IT Group maintains a track of software licenses acquired by the organization and their utilization.
- All departments shall identify the applicable legislative, regulatory and contractual requirements and the interfaces with which organizations personnel should interact. This shall be communicated to the Head – Administration & Finance. Head – Administration & Finance shall keep a list of all such contact details and publish them to be accessible to ISF members & ISO

4.3.59 Reviews of security policy and technical compliance

- Asset owners/Department heads are responsible for ensuring compliance to the technical controls identified in the ISMS
- Technical compliance shall be verified during the periodic Internal/External Audits. Non-conformances shall be addressed immediately with appropriate corrective and preventive actions by the Asset Owners/Department Heads
- In addition Technical compliance /vulnerability checks shall be done for identified critical systems through the use of external security experts.

4.3.60 System Audit considerations

- Internal Audits, Process Implementation Verifications shall be conducted as per the defined audit schedule
- Audits shall be conducted by qualified internal auditors who are also bound by the Non-Disclosure agreements
- Information provided to auditors is collected back on completion of the audit
- Temporary access provided to systems as part of the Audit Checks shall be removed on completion of the audit
- Tools, Systems used for conducting Audits shall be protected from unauthorized access

4.3.61 Documented Operating procedures

- All IT Department activities specified in sec 4.3.1 to 4.3.60 shall be performed in accordance with the Project Management Process
- In addition IT Department shall develop and use additional plans, guidelines and checklists and procedures for individual activities as required and shall be referred from the Project Management Process