Information Security Manual

Version 5.0

Revision History

Version Number	Date	Prepared By	Reviewed By	Approved By	Summary of Changes
0.0	9-SEP-2011	Sai Krishna			Initial Draft
1.0	28-OCT-2011	Sai Krishna	Sairam	Lokesh	• Incorporated review comments • Re-aligned IT Policies
1.1	10-NOV-2011	Sai Krishna	Sai Ram	Lokesh	• Scope section revised • ISMS Effectiveness section added • Removed section 6 "ISO 27001:2005 vs. PRAMATI ISMS Manual"
1.2	29-NOV-2011	Sai Krishna	Sairam	Lokesh	• Updated Scope Section • Removed ISO Asset User role from Section 3.6 "Security Organization and Responsibilities" • Updated Electronic Mail policy with upload/download limit of Attachments
1.3	9-MAR-2012	Mahati	Sai Krishna	Lokesh, Sairam	• Updated Section 4.4: Password Policy with latest implementation details • Added Wireless Access Usage policy • Integrated Pramati HCV HIPAA related ISMS details • Updated Chennai premises address
1.4	18-JUN-2012	Mahati	Sai Krishna	Chandru	• 4.9 Smart Phone & Enterprise Mobility policy

					has been included • 4.11 Corporate social media policy has been included.
1.5	03-Jun-2013	Mahati	Sai Krishna	Chandru	Change of address
1.5	20-Nov-2013	Mahati	Sai Krishna	Chandru	• 4.12 Shredding policy • Network Segregation • Encryption
1.6	03-July-2014	Mahati	Sai Krishna	--	•
2.0	21-Jan-2015	Pavan Nethi	Rajesh Kumar	ISO Team	• Document updated for version 2013 to include expanded meaning of roles, included section for system engineering, references to new terminologies like risk owner made, Key Metrics
3.0	23-02-2016	Pavan Nethi	Rajesh Kumar	ISO Team	• 1. Reviewed and updated ISMS Key Metrics. • 2. Validated the process against current IT process and made the necessary changes
3.1	16 Jan 2017	Pavan Nethi	Pavan Nethi	Draft	• Reviewed and updated locations information.
3.2	7 Feb 2017	Pavan Nethi	Pavan Nethi	Rajesh K	• Included 5.3.11 Interested Parties :section to address the external and internal parties requirement
4.0	7 Feb 2017	Pavan Nethi	Rajesh Kumar	ISO Team	• Baseline and released

5.0	12 Feb 2018	Rajesh K	Prashanth J Anitha Prabhakar Sampath K Ananda K Rajesh K	ISF	Reviewed and updated following sections:. • 8.3.10 Controls against Malicious software / Mobile code • 5.2.10 Wireless Access Usage Policy • 8.5.11 Other forms of Information Exchange • 8.5.27 Terminal Time-out • 8.6.7 Operational Change Controls • Renamed Asset Register with Risk Register • Updated Mail Attachment sizes to 25 MB

Contents

1.0 Introduction

1.1 Purpose

This document describes the Information Security Management System of Pramati Technologies. Although information security is not a core competency of most organizations, it has become a key business enabler, and not just an IT option. Without adequately protected network and other security procedures, the ability of Pramati to carry out its business is not assured. Any Information Security Risk could cripple the company preventing it from carrying out its normal business for days and weeks impacting its earnings and profitability. Hence it has become a business requirement that a stringent Information security management system be put in place.

1.1.1 Pramati Health Care Vertical

HIPAA's scope and compliance is very subjective. This document describes the Information Security Management System of HIPAA implementation at Health Care Vertical of Pramati Technologies as it deals with health care services.

Pramati Technologies is not a Covered Entity but it is a Business Associate for the Clients associated in its Health Care Vertical. This HIPAA implementation is to establish criteria and standards for independent evaluations of the conformance of Processes and Methodologies to all aspects of HIPAA.

2.0 Scope

2.1 Scope of Information Security at Pramati

Information Security covers the organizational Information and information processing facilities of the activities related to design, development testing, service and maintenance of software products and services.

Business Functions such as HR, IT support; Finance & Admin-Facilities are part of the scope.

All Employees, fulltime or part time are part of this information security management system.

Facilities listed below are under the scope of this information security management system.

Corporate Head Quarters
Mid Town 6-3-348,
Road No-1, Banjara Hills,
Hyderabad,
Telangana State, 500034,
India

Chennai Development Center
#7, Perungudi Industrial Estate,
OMR, Chennai, TN 600096
India

Bangalore Development Center
15th Floor, World Trade Center,
Brigade Gateway, Malleswaram
Bengaluru,
Karnataka, 560055
India

2.1.1 HCV Scope

HIPAA Compliant Information Processing facilities covering Design, Development, Testing, Service & Maintenance of Software products and services for healthcare vertical customers of Pramati as a Business associate.

The below facility is covered under scope of HIPAA and treated as Pramati Health Care Vertical:

Pramati Health Care Vertical
3th Floor, Mid Town
6-3-348, Road No-1,
Banjara Hills,
Hyderabad 500034,
Andhra Pradesh, India

3.0 Acronyms / Definitions

Acronym/ Definition	Description
ISMS	Information Security Management System
IS Policy	Information Security Policy
CISO	Chief Information Security Officer
ISO	International Organization for Standardization
BCP	Business Continuity Planning
VAPT	Vulnerability Assessment and Penetration Testing
ERT	Emergency Response Team
AMC	Annual Maintenance Contract
SPAM	Unauthorized and/or unsolicited electronic mass mailings
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to Pramati or its customers' reputation or market standing if the information is leaked / falls into wrong hands.
Virus warning	Email containing warnings about virus or mal-ware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually with intent of frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Pramati who do not have a need to know that information
Sponsoring Organization	Pramati entity/unit/project/function that requested that the external party have access into the Pramati network
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator
Remote Access	Any access to Pramati corporate network through a non-Pramati controlled network, device, or medium
ISP	Internet Service Provider
HIPAA	Health Insurance Portability and Accountability Act
HCV	HealthCare Vertical
EPHI	Electronic Protected Health Information

ISC	Information Security Champ
EHR	Electronic Health Records
EDI	Electronic Data Interchange
External Party	An entity / business unit that is independent of Pramati.
Covered Entity	Health Care provider who transmits any health care Information in electronic form in connection with a covered transaction.
Health Care	Care, services, and supplies related to the health of an individual.
Health Plan	An individual or group plan that provides, or pays the cost of medical care.
Health care clearing houses	A public or private entity that processes or facilitates the processing of non-standard data elements of health information into standard data elements.
Health care Provider	Providers of medical or health care. Researchers who provide health care are health care providers.
Information Security	Preservation of Confidentiality, integrity and availability of information (CIA)
Policy	A policy is a document that states, how the organization readies to protect its information assets. It details specific requirements that shall be established. Policies are generally point-specific, covering a single area; e.g., an acceptable use policy would cover the rules and regulations for appropriate use of the organization's computing facilities
Guideline	A guideline is a collection of recommended best practices that can be system-specific or procedure specific requirements; e.g., guidelines when selecting an outsourcing partner
Procedure	A procedure is a series of steps taken to accomplish a specific task leading to information security governance. e.g., deploying a server into the production environment; the steps include hardening the server and reviewing it for compliance with standards
Confidentiality	To prevent the unauthorized disclosure of information
Integrity	Unauthorized modifications to information by unauthorized personnel or processes
Availability	Ensures access to information or system resources in a reliable and timely manner
Accountability	Provides the capability of identifying each individual and the actions performed by that individual on a system or process. Accountability comprises non-repudiation and

	authentication. Non-repudiation ensures that users cannot deny that a transaction has taken place and that there is sufficient evidence to support the transaction. Authentication establishes the user's identity and ensures that the users are who they say they are.

Word **"enterprise", "company" or "organization"** refers to Pramati
Word **"shall"** refers to practices or procedures that are mandatory
Word **"should", "may" or "recommended"** refers to best practices but not mandatory
Word **"User"** means employees, partners and contract services who are allowed access to Company computing and network facilities
The term **"third party"** refers to vendors, contractors, consultants, customers and other non-employees who are allowed access to Company computing and network facilities
The words **"need-to-know"** refer to the security principle that only people who need to know an item of information to perform their contracted work are authorized to read it
The words **"need-to-have"** refer to the security principle that only people who need to have an item of information to perform their contracted work are authorized to work on it
The words **"least privilege"** refer to the security principle that a person shall be given no privileges other than those that are required to perform his or her contracted work. For example, if the person requires an item of information only for reading, he / she shall not be given permissions to modify
Information is an asset which, like other important business assets, has value to an organization and needs protection. Information assets include program source code, binary programs, documents, financial statements, correspondence with customers, etc.
The terms **information processing asset** or **information containers** refer to assets that store, process or transmit information. These terms include Information Technology devices like computers, storage devices, EPBX and communication links etc. They also include other assets like paper, film, people, buildings used to house people and other information processing assets etc.

4.0 Context of the Organization

4.1 Information Security Policy

The key objective of our Information Security Policy is to assist us in constantly ensuring that our esteemed clients are delivered products and services, through effective practices for sensitive information protection, distribution and management, seamlessly and securely.

- We collectively maintain the confidentiality, integrity and availability of sensitive Information in the company and make them available with minimum disruption to employees when critical to their function.
- We would provide information security awareness and training to employees and non-employees (as needed) regularly.
- All our business units and functions would adhere to configuration management process that controls access and protects their work products.
- We are committed to meet all regulatory, legislative and contractual requirements that our business demands.
- Our business continuity process is planned and implemented to counteract interruptions to critical business activities from the effects of major failures.
- We are committed to report any security breach of information, actual or suspected. All reported breaches are investigated to initiate corrective actions and be on the lookout for improvement opportunities.
- We intend to do periodic audits to ensure the effectiveness of the implementation of our information security management system. Our Information Security Forum reviews this policy annually.

(Jay Pullur)
Founder & Chief Executive Officer

This policy is approved by the CEO. This policy is reviewed and revised by the security forum on a yearly basis

4.2 Objective

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

The following are the main executive objectives of Pramati ISMS:

- To protect client data and information.
- To protect Pramati's information assets and intellectual property
- To embrace a robust business continuity process framework to deliver seamless product development and services to clients
- Objective related metrics are referenced in the below section identified as ISMS Key metrics.

4.2.1 Pramati HCV Objectives

In addition to Pramati ISMS Objectives, the following are the additional objectives for HCV:

- To have a secure environment where the Projects at HealthCare Vertical have a streamlined process workflow.
- To protect HealthCare Vertical's information assets and intellectual property
- To prevent fraud and misrepresentation
- To embrace a robust business continuity process framework to deliver seamless product development and services to clients

5.0 Leadership

5.1 Leadership Commitment

The Leadership at Pramati is committed to implement Information Security to achieve its Business objectives. Leadership team shall define the information security objectives in conjunction with the business objectives and Information Security Policy.

The Leadership team is keen on promoting security of information assets and shall give due importance to the development and enforcement of a corporate culture, which promotes information security. Active participation of the user community and staff members is a must for any security initiative to succeed. The Leadership team shall endeavor to provide regular support to the staff members and the Information security forum to ensure that the security consciousness spread across all levels of the organization.

The IS Forum shall ensure employees, vendors and external party users are:

- Aware of security roles and responsibilities and applicable controls
- Security expectations of their role within the organization
- Motivated to fulfill and confirm to security policies of the organization
- Continue to have appropriate skills to manage information security

The IS Forum provides all resources required for the definition and effective implementation of ISMS. The management participates in the Management Review Meetings and reviews the effectiveness and suitability of ISMS implementation and suggests taking necessary corrective actions & facilitates improvement opportunities as required.

5.2 Information Security Policies

Information security is achieved by implementing a suitable set of controls that are addressed in Policies, Practices, Procedures, Organizational Structures and Software Functions. These are established to ensure that the specific security objectives of the organization are met.

5.2.1 Identification Policy

Purpose

The purpose of this policy is to enforce identification cards to avoid unauthorized access to the Pramati's facilities.

Scope

This policy applies to all employees (regular & contract), visiting clients, prospects, vendors, visitors technicians, house-keeping staff, and catering staff.

Policy

- Demonstrating an Identification card (ID card) on person ensures that he /she is an employee /contractor of Pramati and does not need further checks on one's identity. The visitors, vendors, technicians, house-keeping staff, catering personnel are provided with appropriate ID cards that would be displayed on person which identifies them at Pramati. Failure to adhere to this Policy may result in disciplinary action.

- Employees are encouraged to ask visitors if assistance is required, direct that person to a location to obtain assistance. Our efforts should be viewed as presenting a user-friendly environment where visitors are quickly directed to their destinations, while also alerting security to people who do not have a specific destination. This will require the cooperation of all employees since security is everyone's responsibility.
    - Admin function issue ID cards to all employees with necessary details such as employee ID, photo, blood group etc.
    - All employees will wear their ID card at all times in a visible location at or above the waist while they are in the premises of Pramati.
    - The visitors, vendors, technicians, house-keeping staff, catering personnel shall display their respective ID cards at all the times on person in a visible location at or above the waist while they are in the premises of Pramati.
    - In the event an employee's ID card is lost or stolen, the employee can sign the register placed at the reception to gain access into the premises.
    - ID cards are issued for the exclusive use of the named employee and are not to be loaned to anyone. ID cards remain the assets of Pramati and must be surrendered upon demand by HR, or upon termination of employment.
    - Employees must report lost or stolen ID cards to the Admin function and to their reporting manager as soon as possible. The employees are charged for each replacement of a lost or stolen card.

5.2.2 Acceptable Usage Policy

Purpose

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

Scope

This policy applies to all employees (regular & contract) at Pramati, including all personnel affiliated with external parties.

Policy

The use of Pramati’s automation systems, including computers, fax machines, telephones, camera, mobile phones, conference systems and all forms of Internet/intranet access, is for company business and for authorized purposes only. However, the facilities may be used in case of personal emergencies and other critical times where the situation demands and can be justified.

This policy discourages the following;

- Electronic communication used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass coworkers or external parties; or disrupt the workplace.
- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate Company purposes
- Engaging in private or personal business activities, including excessive use of instant messaging

- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant
- Making unauthorized copies of Company files or other Company data
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems
- Misrepresenting oneself or the Company
- Violating the laws and regulations of India or any other nation or any state, city, province, or other local jurisdiction in any way
- Engaging in unlawful or malicious activities
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages
- Sending, receiving, or accessing pornographic materials
- Becoming involved in partisan politics
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which one is assigned, if one leaves such computer or system unattended
- Using company resources for recreational games
- Defeating or attempting to defeat security restrictions on company systems and applications.
- Using Company automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the Company’s Anti-Harassment policies and is subject to disciplinary action.
- The Company's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of India or any other nation or any state, city, province, or other local jurisdiction in any way. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The Company will act as per the prevailing law of the Land and will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.
- A posting by employees from a Pramati’s email address to newsgroups is not permitted due to the scope for spam and hacking. Where it is necessary, user must seek written permission from the Chief Information security officer.
- Unless specifically granted in this policy, any non-business use of the Company's automation systems is expressly forbidden. If these policies are violated, one could be subject to disciplinary action that may include termination.

5.2.3 Privacy Policy

Purpose

The purpose of this policy is to safeguard client's information and Pramati's information.

Scope

This policy applies to all employees (regular & contract) at Pramati, including all personnel affiliated with external parties.

Policy

- The Company owns the rights to all data and files in any computer, network, or other information system used in the Company and to all data and files sent or received using any company system or using the Company's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The Company also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content.
- Employees must be aware that the electronic mail messages sent and received using Company equipment or Company-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by Company authorities at all times.
- The Company has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with Company policies and state and central government laws.
- No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Company official.
- The Company uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on Company electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Company use at any time.
- Further, employees who use Company systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure.
- Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than Company systems or the company-provided Internet access.

5.2.4 Password Policy

Purpose

Secret authentication information or Passwords are the important aspects of computer security. They are the front-line of protection for user accounts. A poorly chosen password may result in the compromise of the entire Pramati corporate network. As such all Pramati employees (including contractors and vendors with access to Pramati 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.

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 Pramati facility, has access to the Pramati network, or stores any non- public Pramati information.

Policy

General

- All system – level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) and user-level passwords (e.g., email, web, desktop computer, etc.) Must be changed once at least every 90 days.
- User accounts that have system-level privileged access rights granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard ones like "public," "private" and "system" or any other default strings and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- Passwords should never be written down or stored on-line. Passwords must not be inserted into email messages or other forms of electronic communication.
- Password option on all servers shall require them to have a minimum of 8 characters and their complexity option be enabled
- As per current Password policy implemented, password must have a combination of 1 uppercase, 1 lowercase, 1 numeric character and special characters.
- According to password policy implemented, password should be changed every 90 days. All user–level and system–level passwords must conform to the guidelines described.

Guidelines for Construction of Strong Passwords:

- Passwords are at least eight alphanumeric characters long
- They may contain both upper and lower case characters (e.g. a - z, A - Z)
- They may have digits and punctuation characters as well as letters (e.g. 0-9, @#$ %^&*() _+/ ~-=\' {} :";'<>? /)
- They shall not have words in any language, slang, dialect, jargon, etc. other than in English.
- As a best practice, the Passwords should not be based on personal information like names of family, pet, friends and fantasy characters.
- All passwords /Secret authentication information are to be treated sensitive, confidential Pramati information. The following precautions are to be taken to protect the passwords

Password Protection Standards

- Don't reveal a password to anyone by any means
- Don't even hint its format (e. g., " my family name")
- Don't share a password with family members or near or dear ones

- 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 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.
- If an account or password is suspected to have been compromised, report the incident to IT Support and change all passwords.

Application Development Standards

- Application developers must ensure their programs contain the following security precautions.
- Applications

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- 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.
- Should support with LDAP security retrieval, wherever possible.

Use of Passwords and Passphrases for Remote Access Users

- Access to the Pramati Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

  Passphrases

  - Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
  - Passphrases are not the same as passwords. A passphrase is a longer version of the Secret authentication information and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
  - A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.
  - All of the rules above that apply to passwords apply to passphrases too.

5.2.5 Clear Desk/Clear Screen Policy

Purpose

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

Scope

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

Policy

- All “Sensitive” information shall be locked in secured 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 IT Support to protect unattended screens by use of a power on passwords and password-protected screen savers
- Staff should ensure their desks are clear every end of the day before leaving, and also secure confidential information whether physical or electronic, while they are away from their desk even for a brief period.

5.2.6 Electronic Mail Policy

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 email network is secure and its use does not expose the organization to any risks.

Scope

This policy applies to all Pramati employees, contractors and consultants utilizing Pramati e-mail accounts and /or other approved email accounts being used in tandem with Pramati business.

Policy

- **E-mail usage**
  - Email ID naming convention and signature will be followed as per standards decided by Information Security Forum.
  - 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. Users will be educated during induction on the secure and acceptable use of the corporate e-mail account.
- **Remote access to e-mail account**

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

- **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.

- **Mail Attachment**

- The attached document may also be protected from unauthorized access by means of a password depending upon the information like financial data, etc.
- 25MB is the upload/download limit of email attachments being sent or received. Attachments larger than 25MB will be automatically uploaded to Google Drive. A Download link will be included in the emails.

- **Monitoring**

- The organization may, for reasons of security, intercept or otherwise monitor the mails sent through its mailing system.
- The Function Head of HR can approve monitoring of corporate email of employees.
- Sending unsolicited email messages, including sending of “junk email” or other advertising material to individuals who did not specifically request such material shall be considered to be a Spam email.
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use or forging, of email header information.
- 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.
- Creating or forwarding “chain letters”, “Ponzi or other “pyramid “schemes of any type.
- Use of unsolicited email originating from within Pramati networks of other Internet / Intranet Extranet service providers on behalf of, or to advertise, any service hosted by Pramati or connoted via Pramati network.
- Posting the same or similar non-business – related messages to large numbers of Usenet groups (newsgroup Spam).

5.2.7 Mobile Computing/Tele-Working Policy

Purpose

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

Scope

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

Policy

General

- It is the responsibility of Pramati employees, contractors, vendors and agents with remote access privileges to Pramati corporate network to ensure that their remote access connection is given appropriate consideration and privileged access rights as they would have had if they were to be the users-on–site at Pramati.
- General access to the Internet for recreational use by immediate household members through the Pramati Network on personal computers is not permitted. The Pramati employee is responsible to ensure the family member or the near or dear ones do not violate any Pramati policies, and does not use the access for outside business interests. The Pramati employee bears responsibility for the consequences, should the access be misused.

- IS policies provide details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Pramati network

  Requirements

  - At no time should any Pramati employee provide their login or email Passwords to anyone, not even to family members or near /dear ones.
  - Pramati employees and contractors with privileged access rights to remote locations /sites must ensure that their Pramati-owned or personal computer or workstation, which is remotely connected to Pramati 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.
  - Pramati employees and contractors with remote privileged access rights to Pramati corporate network must not use non–Pramati email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Pramati business, thereby ensuring that official business is never confused with personal business.
  - Routers for dedicated ISDN line configured for access to the Pramati 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 IT Support, and IT Support must approve security configurations for access to hardware.
  - All hosts that are connected to Pramati internal networks via remote access technologies must use the most up to-date antivirus software, this includes personal computers. External connections must comply with requirements as stated in the External Party Agreement.
  - Personal equipment that is used to connect Pramati networks must meet the requirements of Pramati-owned equipment for remote access or should have an explicit approval from the IT Support function or CISO on any specific deviations.
  - Organizations or individuals who wish to implement non–standard Remote Access solutions to the Pramati production network must obtain prior approval from the IT Support function as well as the Chief Information Security Officer.

5.2.8 Licensed/Copyright Software Usage Policy

Purpose

The purpose of this policy is to ensure that the employees take the responsibility for the use of licensed/copy right software other than company supplied/installed items.

Scope

This policy applies to all Pramati employees, contractors and consultants utilizing Pramati computers or devices that are approved to be explicitly used for Pramati Business.

Policy

- The Company has licensed the use of certain commercial software application programs for business purposes. External parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.

- Company provides Employees with all software that is required for performing their job. For software that is not installed and required for execution of work Employee should get approvals from system administration before installing.
- Employee cannot store/copy/carry any music, videos or any data that is protected by copyrights or licenses, on the Company system unless such data is required for work to be done. In such case, Employee needs to take appropriate approvals from the IT managers.
- Any software or licensed or copyrighted content found on Employee system is considered as responsibility of the Employee and any issues arising thereof would not be the responsibility of the Company, but would be the responsibility of the employee /contractor /consultant.

5.2.9 Smartphone & Enterprise Mobility Policy

Overview

Smartphone and Enterprise Mobility offers new ways of gaining business and competitive advantage by creating new services, improving current offerings, enhancing operational access and flexibility. But with all this improvement comes increased security risk .Pramati cannot afford to ignore the risk and must formulate appropriate smart phone policies to manage it effectively.

Purpose

This smartphone security policy establishes the rules for the proper use of Pramati/Office provided smartphone devices for the eligible employees. Also, this establishes to protect the confidentiality of sensitive data, the integrity of data & applications and the availability of services, continuity of business.

Scope

This policy applies to all Pramati employees who utilize company-owned, personally-owned, or publicly-accessible mobile technology to access the organization's data and networks via wireless means. Wireless and mobile access to Pramati network resources is a privilege, not a right. Consequently, employment at the Company does not automatically guarantee the rights to wireless and mobile access privileges. This access is governed by and subject to prevailing Organization's policies and guidelines relating to technology, use of data and security restrictions.

Policy

To comply with this policy, it is expected that IT maintains a log and register of all the company owned smartphones, tablets and other mobile WIFI devices and Gadgets. It also should ensure that all these devices are updated complying with the respective vendor specifications.

Equally responsible are all such respective employees to maintain and safeguard the devices that they use or own for work.

The following are the key points to be considered while using the above mentioned gadgets in Pramati:

- Establish smartphone wireless access security.
- Establish and enforce passwords.
- Vary access levels based on device interrogations.
- Require lost or stolen phones be reported immediately.
- Allow or disallow application use, including Pramati mandated programs for filing reports and such.

- Enable compliance mechanisms, such as logs.
- Remotely lock down.
- The project lead should record the movement of the testing smartphone devices provided by the client.
- However, as per client requirement Smart phone usage may be limited and Users shall be able to access their e-mail account after enrollment through an authentication mechanism.

5.2.10 Wireless Access Usage Policy

Purpose

This policy is designed to protect Pramati resources against intrusion by those who would use wireless media to penetrate the network. The wireless usage policy defines the use of wireless devices in Pramati and specifies how wireless devices shall be configured when used.

Scope

This policy applies to all the wireless devices in use at Pramati or those who connect through a wireless device to any Pramati network.

Policy

The Policy mandates the following:

- Authentication: The authentication mechanism of all approved wireless devices to be used, must be examined closely by the IT Support function. The authentication mechanism should be used to prevent unauthorized entry into the network. Hence IT Support Function identifies the mac id and the WPA key encryption to be provided.
- Encryption: The encryption mechanism is Wi-Fi Protected Access (WPA). It is used for all approved wireless devices to protect data from being disclosed.
- Configuration: Laptops (all locations) internet access will be provided by IT team through mac binding.
- For mobiles (Hyderabad only) - users have to authenticate using web.pramati.com
- For mobiles (Chennai and Bengaluru) - users have to request with IT team explicitly for mac binding.
- Access Points: All the wireless access points that are connected to Pramati network are registered and approved by the IT Support Function. All wireless devices are subjected to penetration tests.
- Users need to login to web.pramati.com with their LDAP credentials to authenticate their logins & access internet.
- Allowable wireless Use:
  - Only the approved wireless enabled devices provided with mac id shall access the Wi-Fi.
  - All wireless devices must be checked with proper configuration prior to being placed in to service.
  - All the wireless devices shall access only through the provided access point.
  - The WAP key for all the access points is renewed on mutual agreed upon periodicity.
  - Only such internet / 3G data cards that are approved and provided by Pramati's IT and Admin functions should be allowed to use when required.
  - However wireless access may be limited for some networks as per client/business requirements or as per the Leadership decision

5.2.11 Corporate Social Media Policy

Overview

Whether or not an employee chooses to create or participate in a blog, wiki, online social network or any other form of online publishing or discussion is his or her own decision. However, recognizes that emerging online collaboration platforms are fundamentally changing the way individuals and organizations communicate, and this policy is designed to offer practical guidance for responsible, constructive communications via social media channels for employees.

Purpose

This Policy has been developed to ensure that Employees of Pramati and Consultants to Pramati who choose to participate in social media do so in a responsible manner, and act in a way that protects Pramati interests.

Scope

This policy applies to the use of current & emerging forms of social media including social networking sites, blogs, micro-blogs, online discussion forum, collaborative spaces, and media sharing services. This policy is that the Employee may use social media for Personal use only. And in strict compliance with all other terms of this and other Pramati policies.

Policy

- Social Media is defined in this policy as all online or social media includes any sites that allow a user to contribute content whether that is in the form of article, videos, images, blog entries or comments on any items including forums or chat rooms. Social media sites include but are not limited to:

- Facebook
- YouTube
- LinkedIn
- Twitter
- Google+
- Pinterest
- Tagged
- MySpace

- Employee, Consultants can participate in social media that is unrelated to Pramati as any private citizen would, and without need to reference their role at Pramati. They should do so responsibly, respectfully and in accordance with the rules of any forum in which they participate. However if an employee or consultants makes reference to Pramati, its people, Product, Clients, Business partners, Suppliers or other associates on a social media site they must:

- Identify themselves as a Pramati Employee or Consultant.

- Only disclose and discuss publicly available information.
- Ensure that none of the references, posting or content causes the employee or consultant to breach any other obligations to Pramati or external parties.
- Expressly state on all postings that the stated views are their own and are not those of Pramati.
- Adhere to the terms of use of the relevant social media platform/sites as well as copyright, privacy, defamation discrimination.
- Never use Pramati logos, Trademarks, or other copyrighted or protected intellectual property in postings.
    - However wireless access may be limited for some networks as per client/business requirements or as per the Leadership decision

Roles & Responsibilities:

Directors, employees, consultants with Pramati are responsible for all content they publish on blogs, wikis or any other form of user-generated media and are responsible for:

- Ensuring their participation in social media does not breach relevant Pramati polices such as the System Usage & Security, Release of Information and Code of Conduct.
- Ensuring that they do not publish any of Pramati's confidential, financial, intellectual, business performance, sensitive or proprietary information or similar information obtained as a result of their engagement with Pramati about, our clients, business partners, suppliers or other associates
- Not disparaging Pramati or any of its employees, clients, business partners, suppliers or other associates, or make any statement which does, or is likely to bring Pramati or any of these parties into disrepute or ridicule or otherwise affect their reputation.
- Being mindful that any published content will probably remain in the public domain for many years.
- Using privacy settings whenever appropriate but remembering that nothing posted on the internet is ever truly private.
- Ensuring that their online activities do not interfere with their job or commitments to their customers

Breach of this Policy:

Failure to comply with this policy may result in Pramati exercising its rights under a contractor/consultancy agreement or taking disciplinary action against an employee under the Disciplinary Process at Information Security Policies. This action may result in termination of employment and beyond.

5.2.12 Shredding Policy

Purpose

The Shredding Policy option instructs employees to securely shred all information which is no longer needed for business or required by compliance laws – as opposed to directly placing it in a trash can.

Scope

The Shredding Policy is applicable in the Pramati Premises which includes all Functions (Admin, HR, Finance, IT Systems) and all Projects work areas, Cabins, Conference rooms and Meeting rooms.

Policy

- Every day, House Keeping personnel under the supervision of House Keeping Supervisor will pick orphan papers lying at the printers in all floors.
- Papers placed for shredding in the bin will be collected/picked-up only. House Keeping personnel will not pick any papers from “Re-Usable” bin.
- Administration Manager or Facility Manager during their rounds shall verify whether the paper lying at the printers are properly segregated as re-usable or for Shred and appropriately placed in the bins.
- Apart from the above, if there is any element of doubt regarding the papers placed for shredding papers collected by Housekeeping Boy, Housekeeping Supervisor through his judgment will set such papers aside and will acquire clarity from Facility Manager or Admin Manager.
- Papers which are kept for shredding shall be shredded and disposed off to garbage yard for further disposal to authorized scrap vendor.

5.2.13 Enforcement

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

5.3 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:

- Chief Information Security Officer
- Information Security Forum
- Information Risk Owner
- Information Security Champ
- Business Continuity Planning Team
- Emergency Response Team
- Functional/Delivery Lead
- HR Lead
- IT Support Lead

5.3.1 Chief Information Security Officer

At Pramati, Information Security is everybody’s responsibility including those of contractors, consultants and external party service providers. The overall responsibility for overseeing Information security in the organization is allocated to a single officer. This is designed to increase ownership and co-ordination of security management activities. This officer is designated as the Chief Information Security Officer at Pramati, and the following are the broad based duties and responsibilities of the Chief Information Security Officer:

- Setting up and publication of policies, advice and guidance.
- Monitoring of compliance and co-ordination activities necessary to attain the organization's security objectives.
- Informing the Head of IT Support of any security incident or threat that could affect the Information Assets and business processes.
- Advising the Head of IT Support 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
- To recommend modifications to any of the information related policies as appropriate to the business and organizational context, etc.
- To escalate and place before the Leadership team any issues impeding effective implementation of the ISMS.
- Take such steps as required to stop any noticed / reported violations of the information security related policies and procedures.
- To convene and carry on the Management Review Meetings periodically duly involving the Management Review Committee members.

5.3.2 Information Security Forum

An Information Security Forum consisting of Chief Information Security Officer and the following function heads:

- Human Resources, Administration, Finance and IT Support
- Product Portfolio Management
- Product Development Services
- Process Management

This forum is headed by a senior manager and provides the direction to the ISMS implementation. The following are the broad based duties and responsibilities of the Information Security Forum:

- 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.
- Management review of the ISMS initiative in accordance with the Management Review Procedure in Internal Audit & Management Review Process
- Review and approve the Asset Lists
- 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 External party service providers.
- Approval of new Information Assets

- Responding to security incidents in a calibrated manner

5.3.3 Information Risk owner

- All the information assets in the organization would fall under one or the other function /department and the function head will have the ownership. The owner shall be the prime controller for maintaining the assets under his control and will be the identified risk owner who evaluates the risk associated with the assets. 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. That apart, the risk owner would also have the ownership of any non-tangible assets or valuable information that may likely be discussed as part of business information exchanges for which the risk evaluation should be done. The following shall be the broad based duties and responsibilities of the Information risk owner:

- Specifying the measures necessary for protecting the Information and assets in consultation with the Management Representative for ISMS
- Ensuring good security practices are maintained within their area of responsibility and that policy and procedures are laid down to maintain and ensure information security is followed.
- Ensuring all staff is made aware of the expectations in order to maintain the security of Information and the assets.

5.3.4 Information Security Champ

At HealthCare Vertical, HIPAA practice is the main criteria. The overall responsibility for overseeing information security in the HealthCare Vertical is allocated to a single officer. This is designated to increase the co-ordination of HIPAA management activities. This champion, designated as the Information Security Champ at Pramati HealthCare Vertical.

The duties of the Information Security Champ include, but are not limited to the following:

- Oversee and monitor implementation of the components of the HIPAA Compliance plan.
- Develop mechanisms to receive and investigate reports of breaches and monitor subsequent corrective action.
- Ensuring all the team members are aware of all the implemented HIPAA components, which are expected of them in order to maintain the policies and procedures.
- Specifying the measures necessary for the Healthcare Vertical in consultation with the Chief Information Security Officer.

This role – Information Security Champion is extended to other teams with size > 15. The responsibilities of ISC in non-HCV projects will be same as above in ISO 27001 context.

5.3.5 Business Continuity Planning Team

Ensure planning, communication, coordination and implementation of business continuity arrangements including testing of business continuity arrangements.

5.3.6 Emergency Response Team

Steps in for effective communication and coordination in case of security incidents leading to emergency situations and potential causalities. Ensure safety of human resources and other infrastructure assets critical to organization's business.

5.3.7 Delivery Lead

System / Project owners are identified risk owners of projects or services or products and are business owners of specific information assets systems. The context of Delivery lead also includes a Delivery manager or director.

5.3.8 Facility Lead

Ensures physical security aspects of critical assets of organization are covered. Manages facility related external party services essential for organization's business continuity and identified as a risk owner. The context of facility lead also includes a Facility manager or director.

5.3.9 HR Lead

Ensures information security practices are implemented throughout the pre-employment, employment and post-employment phases of human resources functioning and identified as a risk owner. The context of HR lead also includes a HR manager or director.

5.3.10 IT Lead

Ensures that ISMS policies are communicated to interested parties and employees of organization and provides necessary support to ISMS Team in continual improvement of ISMS. Ensure that the IT infrastructure is maintained in accordance with the business requirements, client's expectation and ISMS requirements. The IT Lead is identified as a risk owner for IT related activities. The context of IT lead also includes an IT manager or director.

5.3.11 Interested Parties

- The needs and expectations of the interested parties (both internal and external) are taken into consideration and will align with the Organization's interests.

    - The internal parties are identified under Security Organization and Responsibilities section and this includes the employees of Pramati. The intended outcome for the internal parties is to adhere to the ISMS framework herein laid out in this manual.
    - The external parties include the clients and suppliers of Pramati. Clients needing data security may require the Company to fulfill their security requirements.
    - The Government with statutory requirements will expect the Company to adhere to those requirements. Suppliers will enter into a non-disclosure agreement and Pramati will do a review of their services to meet the requirements entered in the Supplier agreement.

6.0 Planning

6.1 Asset Identification & Classification

PRAMATI assets can be broadly classified as per the “Asset classification guidelines” document. Please refer the same.

6.2 Guidelines on Confidentiality, Integrity and Availability

Refer to “Asset Classification Guidelines”.

6.3 Risk Management

Risk identification and mitigation is done according to the “Risk Assessment Process”

6.4 Statement of Applicability

A statement of applicability indicating the applicability of controls indicated in the ISO 27002: 2013 standard and any other additional controls chosen is prepared by the Chief Information Security Officer and is reviewed and approved by the Leadership team. The statement of applicability is reviewed and updated as and when the Risk Register are reviewed and modified.

Refer “Statement of Applicability” for applicable and not applicable controls.

6.4.1 Pramati HCV SOA

HIPAA implementation is built upon the existing ISO 27001: 2013 standards. HIPAA Privacy and Security Controls are mapped to the existing SOA of ISO27001.For the applicable and non-applicable controls refer “Statement of Applicability “

6.5 Implementation Norms

All practices/functions are required to implement the Information Security Policies and procedures. In cases where the business activities require deviations to the Information Security Policies and procedures, a request indicating the need for deviation is forwarded by the Function Heads and Managers to the CISO. The CISO in consultation with Information Security forum shall review the risks and any additional controls required and approve the same. The CISO shall keep track of all such deviations issued. However, the Risk Owners would always be the Function Heads.

In cases where the customer has security requirements, which require different/additional controls from those, indicated in ISMS, the requirements are forwarded to the Chief Information Security Officer (CISO). CISO in consultation with the function head and Information Security forum assists the team/function to develop an Information security plan specific to the function/practice. Again, the risks would be identified and owned by the Function Head.

6.6 Document & Data Control

The ISMS comprises of the following documents:

- ISMS Manual

- Risk Registers
- Risk Assessment and Treatment Plan
- Statement of Applicability
- Applicable Procedures / Processes / Guidelines
- Templates/Formats
- Configuration Management Process
- Document management process

All ISMS documented information are defined, maintained and controlled in accordance with the Document Management Process.

7.0 Support

7.1 Internal Audits

Internal audits to verify the compliance of information security practices to ISO 27001:2013 requirements are conducted once in a year as per the **"Internal Audit Process".** Trained internal auditors conduct the audits. Internal Auditors independent of the function being audited are deputed for conducting the audit. The planning and execution of audits are in accordance with the Internal Audit Process of Pramati.

7.2 Management Review

Management Reviews are conducted once in a year 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 Information Security.
Management Reviews are coordinated by the CISO and chaired by the VP - Delivery. All function heads and Information Security Forum members are part of the Management Review Meetings.
The agenda for the Management Review Meeting are as per "MRM Guidelines"

7.3 Training

Employees 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 policies and configuration management, 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 Function Heads and Managers and ISO/Information Security Forum and communicated to the head of HR. Planning and execution of the training programs is in accordance with the Training Process.

7.4 Continual Improvement

The organization continually looks at improving the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective actions, mitigation actions for identified risks by risk owners and suggested improvement opportunities along with management review.

Continuous improvement is achieved through the following means:

- Identification of root causes for non-conformities of the implementation/operation of Information Security and taking appropriate corrective actions and act on improvement opportunities
- Identification of potential risks, their causes and implementing appropriate mitigation actions
- Defining qualitative and quantitative security goals and improve the Information Security to achieve the same. Each business function identifies the necessary service levels and quantifies them for effective tracking and improvement.
- The CISO tracks each service level and reports the same in the management review meeting to identify action plans to improve them.
- CISO shall keep track of all corrective actions and suggested improvement opportunities, their status and data pertinent to IT security goals. This data shall be analyzed to verify whether risk treatment plans are effectively contributing towards satisfactory improvement of ISMS. The improvement of the effectiveness of ISMS is reviewed during the Management Reviews.

8.0 Information Security Procedures

8.1 Physical Security

8.1.1 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 Director, Admin will enter into a contract with a Security Agency, which has been evaluated for their ability to carry-out such activities
- Director, Admin will maintain an approved list of personnel from this agency after scrutinizing profiles (and police records if possible) of these personnel.
- Director, 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

8.1.2 Employee Access

- The Admin shall provide employee ID card to all employees with the help of HR
- All employees are required to wear and display the ID cards when reporting to work
- HR shall intimate the Admin function regarding the new employees who have joined service and the office/area to which access is required. Admin Function shall arrange for a photo ID card and the access control system activated for the new employee.
- On separation of an employee from the organization, HR shall intimate Admin the last working date of the employee. Admin Function shall collect the access card and store it in a secure location until the access card is disabled on the access control system

8.1.3 Non-Employee 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 Security Guard
- Details of any equipment/media being brought by the visitor shall also be identified and entered in the “Material Inward Register”
- Security guard shall call up the employee for whom the Visitor/Guest had come to confirm the appointment/availability
- A visitor ID card shall be provided and shall be worn by the visitor until the visitor leaves the premises
- The guest/visitor 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 visitors/guests 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 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
- External 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.

8.1.4 Inward/Outward Movement of Equipment

- All equipment/material to be delivered to the organization is received at the Material inward area
- The Security Guard will maintain a Material inward/outward register to log items being brought into the secure perimeter and being taken out
- All equipment/material must be accompanied with a valid Delivery Note/Invoice/Gate pass with necessary details
- 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 VP (Delivery) /CISO and provided to the Security Guard
- Head-Admin shall track the return of equipment which have been moved out on returnable basis
- Equipment/Media being transferred between different premises within the security perimeter shall be suitably packed and transferred along with one of the organizations employee.

8.1.5 Equipment Siting and Protection

- 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

8.1.6 Power Supplies and Cabling Security

- 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
- 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 fit to relevant communication lines, if exists.

8.1.7 Equipment Maintenance

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

8.1.8 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 VP (Delivery) / CISO
- 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

8.1.9 Secure disposal or re-use of equipment

- Equipment before being disposed / reallocated shall be reviewed by Head-IT Support and Head-Admin. 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.

8.1.10 Safeguarding of organizational records

- Organization records of value shall be identified and stored using appropriate security mechanism. Suitable backups will be taken and maintained.
- All organizational 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
- Refer to Configuration Management Process

8.1.11 Information Assets Inventory & Management

- A detailed inventory of Pramati assets will be maintained. The inventory is to contain security classification and Customs bonding status of items.
- IT Support maintains the inventory of all computer systems / printers / computer media / licensed software/UPS/Communication equipment related to networking.
- 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 assets are documented using the Risk Register

8.1.12 Contact with authorities

- Head-Admin maintains the contact details of all law enforcement functions, fire function, emergency services, and supervisory authorities.
- Head-Admin. Function maintains contacts with the appropriate level of personnel in these functions.
- Details of when and by whom these authorities shall be contacted and how security incidents are reported in a timely manner are documented
- Refer to Admin process and Business Continuity Plan

8.1.13 Protection against External and Environmental Threats

- Admin Function ensures that combustible materials are stored at a safe distance from the secure perimeter
- Admin Function ensures firefighting equipment such as smoke detectors; fire extinguishers are installed at appropriate places and are maintained. Emergency/Fire exits shall be marked suitably.
- Admin Function ensures that all the employees are trained to operate the firefighting equipment, evacuation of premises during an emergency. Periodic drills shall be conducted to ensure that employees are alert and aware of these procedures.
- Refer to Admin process and Business Continuity Plan

8.2 HR Function

8.2.1 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.
- External party Background checks will be performed and appropriate report will be obtained.
- 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.

8.2.2 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 organization's Information Security policies shall be the basis for confirmation, promotion and assignment of critical duties.

8.2.3 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 Head of HR
- Refer to HR Process

8.2.4 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 Function. Induction training program includes Information Security awareness as part of the curriculum.

- Respective function heads and CISO shall identify training requirements for information security education/ Information Security implementation awareness
- Training Coordinator 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 process.
- Refer to Training process

8.2.5 Disciplinary Process

- A disciplinary committee is constituted by the Leadership team to examine disciplinary issues related to information security practices.
- The disciplinary committee is headed by the VP - Delivery and includes CISO, Head-HR and the specific function heads / Managers.
- 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 measures and mitigation actions for the associated risk identified.

8.2.6 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
- Audit function for the same function/project
- Systems Administration and Resource Allocation/Network Configuration Approval
- Systems Administration and Operator log verification

8.2.7 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
- Refer to Configuration Management Process

8.2.8 Termination Responsibilities

- HR Function is responsible for managing the termination of employment (whether initiated by client, vendor, external party or by Pramati Management) and works together with the supervising manager of the person leaving to manage the security aspects of the exit procedures

- HR shall communicate relevant employees, customers and vendors of changes to personnel and operating arrangements
- HR shall communicate to the employee responsibilities and duties still valid after termination of employment.
- Refer to HR Process

8.2.9 Return of Assets/Removal of access rights

- HR Function works together with the supervising manager and other function heads for return of all assets (software, documents, data, equipment, mobiles, credit cards, access cards, books and electronic media). In cases where an employee uses their own personal equipment (Such as laptop, PDA), procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.
- HR Function works together with the supervising manager for transfer of information related to the role and responsibilities assigned to the employee to ensure continuity and minimize loss of important knowledge.
- Supervising Manager intimates IT Support/ Admin. Function / Function of the access rights (physical & logical) that needs to be revoked. If a departing employee has known passwords for accounts remaining active, these should be changed.
- Refer to HR Process

8.3 IT Support Function

8.3.1 Specialist Information Security Advice

- CISO / Head IT. Function 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 CISO
- The specialist security advisors can be part of the organization or external consultants/vendors.
- Registration/Subscription with vendors (e.g. Microsoft/Oracle)/forums (Yahoo security groups) shall be taken on need basis.

8.3.2 Liaison with ISPs & Telecom Operators

- IT Function 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
- IT function also takes membership or becomes part of security groups/industry forums to obtain advice in the event of a security incident.

8.3.3 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 CISO.
- These requirements shall be specified in the purchase order.
- Member/s of the Leadership team 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.

8.3.4 Reporting Software/Hardware Malfunctions

- All users of the computing infrastructure shall report software/hardware malfunctions to the on duty systems administrator or escalate to the IT Head.
- All software/hardware malfunctions are recorded and tracked using the Service Request Log (Helpdesk.pramati.com)
- The allocated systems administrator shall resolve all such issues as per the agreed service levels and intimate the user
- The IT Head shall analyze the reported software/hardware malfunctions for assessing risk which can compromise the information security and implement necessary controls

8.3.5 Secure Disposal or re-use of equipment

- Equipment containing data/configuration details shall not be disposed without removing the same. The assigned administrator shall ensure mechanisms such as formatting/safe erase to erase the data.
- Equipment being reassigned shall also be verified for data/configuration details and the same is removed before issue.

8.3.6 External IT Sys

- Head of IT shall ensure that the security controls, service definitions and service delivery levels included in the vendor service delivery agreement are implemented, operated, and maintained
- Head of IT shall ensure that the services provided by the vendor are regularly monitored and reviewed. Where performance doesn't match the agreed service delivery levels the same shall be escalated and resolved with the vendor.
- Head of IT shall ensure adequate review of any changes to the provision of services by the vendors taking account of the criticality of business systems and processes involved and re-assessment of risks
- Head of IT shall establish acceptance criteria for new information systems, upgrades, and new versions and suitable tests of the system(s) carried out prior to acceptance

8.3.7 Information Back-up

- IT Support is responsible for the backup of data and periodic recovery testing.
- All practices/functions are required to give the data backup requirements for their data in writing. The request shall contain the location of the data, names of folders/files, type of backup (incremental/full), periodicity and any other specific requirements.
- IT Support consolidates all such requests and prepares a backup plan.

- IT Support take backups 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 IT Support 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.
- IT Support 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.
- IT Support shall identify the restoration plan for the backups to verify the reliability of the backup process. The backup data is restored as per the restoration plan and appropriate corrective action taken in case of discrepancies and also record any improvement opportunities and act upon them.

8.3.8 Control of operational software

- IT Support is responsible to track the risks existing in software versions and availability of new versions of the software or patches to the same
- IT Support 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/software update activities are recorded in the Service request register

8.3.9 Covert channels and Trojan code

- Refer to the Development process and Review process in PAL for using appropriate coding standards and review of code

8.3.10 Controls against Malicious software/Mobile Code

- Antivirus software shall be deployed at 3 levels [All Servers and Desktop.]
- Inbound and outbound data traffic (for http, ftp and emails) shall be scanned for Virus before its transmission.
- The Antivirus software deployed shall be monitored 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 / DVD's / Pen Drives shall not be used / accessed in a networked PC without prior approval of Practice/Function Head.
- IT Support 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.

- Mobile code is software that is transmitted from a remote system to be executed on a local system, typically without the user's explicit instruction. Such malicious code shall be intercepted by the Antivirus or the monitoring tool for further action.
- Although mobile code is typically benign, attackers have learned that malicious mobile code can be an effective way of attacking systems, as well as a good mechanism for transmitting viruses, worms, and Trojan horses to users. Workstations. Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript. The monitoring tool should detect such a code and quarantine for further action.
- A cookie is a small data file that holds information about the use of a particular Web site. Session cookies are temporary cookies that are valid only for a single Web site session. Persistent cookies are stored on a computer indefinitely so that the site can identify the user during subsequent visits. Unfortunately, persistent cookies also can be misused as spy ware to track a user's Web browsing activities for questionable reasons without the users' knowledge or consent. The monitoring tool should detect such activity and quarantine for further action.
- All the web browsers are set to medium or higher security levels where the users will be prompted before installation of any cookie or script.

8.4 External Party Access

8.4.1 Contracts

- The organization shall enter into legally binding contracts with all external party service providers.
- Maintaining the security of the organization's information assets will be a part of the contractual commitments
- External 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
- Where appropriate, service levels/response time critical for the services are included in the contracts and shall be monitored
- The responsibility for managing the relationship with external party shall be assigned to a designated individual
- Any changes to external party services shall be reviewed and re-assessed for risks before implementation

8.4.2 Access to internal resources

- External parties' access to the organization's IT facilities would be determined based on the business objectives of the services provided.
- The VP (Delivery) shall approve all requests for access to external 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 external party access provided and controls implemented are recorded

8.4.3 External IT Sys

- Head of IT shall ensure that the security controls, service definitions and service delivery levels included in the vendor service delivery agreement are implemented, operated, and maintained
- Head of IT shall ensure that the services provided by the vendor are regularly monitored and reviewed. Where performance doesn't match the agreed service delivery levels the same shall be escalated and resoled with the vendor.
- Head of IT shall ensure adequate review of any changes to the provision of services by the vendors taking account of the criticality of business systems and processes involved and re-assessment of risks
- Head of IT shall establish acceptance criteria for new information systems, upgrades, and new versions and suitable tests of the system(s) carried out prior to acceptance

8.4.4 Removal of Property

- All equipment to be moved within the premises or outside shall be approved by the risk owner
- All equipment to be moved outside the security perimeter shall be accompanies by a gate pass with details of material and authorization by the right authorities
- Security shall track all equipment being moved out and identify whether the material is returnable or non-returnable
- All returnable equipment is tracked on a monthly basis and where the material is not returned as per the gate pass the same shall be escalated and resolved

8.5 Network Controls

8.5.1 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 equipment 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 Pramati its clients, Internet, group companies, etc.
- Authorized personnel are only allowed access to these documents.

8.5.2 Network security

- Controls shall be implemented to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems.
- Head of IT / CISO shall be responsible for monitoring the security of the local and wide area network including access to external 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

8.5.3 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.
- The media movement will be logged to maintain an audit trail.
- All computer media/equipment shall be disposed off safely and securely when no longer required. IT Support / Admin. Shall review equipment to be disposed off at least once every quarter.
- IT Support 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 with approval from the Management
- Infrared / Blue tooth ports shall be disabled from desktops/laptops/peripherals. Based on need basis access would be provided with approval from the Management
- Refer to Admin. Process and IT Support process

8.5.4 Disposal of Media

- Media before being disposed /reallocated shall be reviewed by Head-IT Support and Head-Admin functions to assess the risk and take steps to remove data/licensed software
- Digital media such as DVD, CD, Pen drives, and Hard disk, that are being disposed shall be recorded using Media disposal register
- Media shall be disposed by using appropriate shredding mechanisms to prevent reuse/restoration.

8.5.5 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 anywhere 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

8.5.6 Information Handling Procedures

- Information assets of the functions and their classification is identified and documented using the Risk 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 labeled as per the Asset labeling guideline

8.5.7 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 function holding such documents

8.5.8 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/functions procedures/plans (e.g. Configuration Management Plan) shall identify the exchange/delivery mechanism and any specific security requirements during the transfer
- The respective project/function head shall be responsible for compliance with the contractual requirements

8.5.9 Security of Business Information Systems

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

8.5.10 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 function
- Where such systems are maintained by external party service providers controls mentioned under external Party Access shall be applicable

8.5.11 Other forms of Information Exchange

- Electronic office systems such as Fax, VOIP, Phone lines shall be secured.
- VOIP lines and Phone lines with direct dialing 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 sensitized to the risks associated with these systems while transmitting confidential data to enable them take suitable precautions

8.5.12 User Registration and Privilege access rights Management

- New employees joining the organization shall be provided with user id/mail accounts based on their role/responsibilities.

- HR shall intimate the respective function, Networking and Admin. Functions of new employees joining details. Details of whether the new employee is a direct employee of Pramati or a contract employee shall be communicated by the HR explicitly.
- IT Support in consultation with the respective function 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 function head shall identify the differential access rights that need to be provided and communicate the same to IT Support
- Subsequent modifications to access rights are made based on written requests sent by the respective function 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 Function Head. Network administrator shall take over the resources after getting a clearance from the respective Function 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

8.5.13 User Password Management & Password Use

- Secret authentication information /Passwords shall be defined and used in accordance with the Password Policy.
- Password policies on servers, application systems shall be in accordance with the Password Policy defined in the ISMS
- Passwords for Servers and Applications/Software Utilities shall be implemented and controlled in accordance with the Password policy
- Password Management for Servers shall be implemented in accordance with the Information Technology process
- Secret authentication information which is system generated may sometimes not comply with the requirements of Pramati Password policy (applications given by client, procured before implementation of ISO 27001, proprietary software). In such instances IT Support shall ensure that passwords are immediately changed to comply with the requirements of the password policy. Where the application doesn't support enforcement of Pramati password policy the owner of the application shall define the specific password policy in the Configuration management plan.
- Refer to IT Support Process

8.5.14 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 internal security audits conducted periodically
- Any deviations are recorded as Non-Conformances and appropriate corrective actions taken. Opportunities around such incidents are identified for continuous improvements.

8.5.15 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

- Hardware Level/OS Level password access
- Lock and Key
- Disabling the system
- Removal of Network/Power connections
- Head of IT and Head of Admin functions shall verify the physical condition of such equipment periodically to identify any tampering/physical loss of such equipment

8.5.16 User Authentication for External Connections

- All external users of the organizations network shall be routed through the VPN and authenticated by the Firewall and Domain Controller before being provided access to the internal network resources
- Requests for external connections shall be approved by the VP (Delivery) and forwarded to Head of IT. All such requests are logged and tracked using the **Service Request Register**.
- All such access rights provided are recorded in the Access Register or in systems portal.

8.5.17 Remote Diagnostic Port Protection

- All ports including remote diagnostic ports shall be scanned periodically using suitable tool/s
- 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
- Segregation in networks
- Network shall be segregated into sub domains to ensure that personnel from one function are not able to log into systems of other functions/projects
- The external networks are segregated from the organizations network by usage of a firewall

8.5.18 Security of network services

- Security features, service levels, and management requirements of all network services shall be identified and included in all internal/external network service agreements

8.5.19 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 equipment 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 Pramati, its clients, Internet, group companies, etc.
- Authorized personnel are only allowed access to these documents.

- Refer Network access policy

8.5.20 Network security

- Controls shall be implemented to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems.
- Head of IT shall be responsible for monitoring the security of the local and wide area network including access to external 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 client's security requirements

8.5.21 Segregation in networks

- Network is segregated into V-Lans where applicable, the external networks are segregated from the organizations network by usage of a firewall
- The external networks are segregated from the organizations network by usage of a firewall

8.5.22 Security of network services

- Security features, service levels, and management requirements of all network services shall be identified and included in all internal/external network service agreements

8.5.23 Automatic Terminal Identification

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

8.5.24 Terminal Log-on procedures

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

8.5.25 User Identification and authentication

- All users shall have a unique domain id for their use only and this shall be the basis of identifying users on the network/information systems

8.5.26 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.

8.5.27 Terminal time-out

- External connections to the organizations network and Telnet services shall be limited to a maximum connectivity time of 2 hour at a time

8.5.28 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

8.5.29 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
- All log files shall be protected from tampering and unauthorized access

8.5.30 Monitoring System Use

- Critical logs for all Information Systems shall be identified and enabled.
- IT Support shall monitor the logs for understanding the system usage pattern and identify any misuse.

8.5.31 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.

8.5.32 Clock Synchronization

- All systems clocks will be synchronized with a NTP server to enable reflection of accurate time & date

8.5.33 Encryption

- Encryption is limited only to Castlight project members.
- Encryption of Mac Book’s Hard disk is performed by IT Team.
- Mac's internal encryption tool is used for the same.

8.5.34 Non-repudiation service

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

8.5.35 Customers Supplied Assets & Connectivity

- IT Support or Delivery Lead shall ensure that all customer supplied assets are protected in accordance with the asset management policies of the organization and the other controls applicable to organizations assets
- Customer requests for access to Pramati Network and vice-versa shall be authorized by VP (Delivery) /Head-Development and the configuration and duration of such connectivity is logged and tracked by IT Support.
- Refer to IT Support Process

8.6 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 ISO shall review the security requirements identified before they are finalized where specific assistance is requested by the Project Manager/Business Sponsor.
- 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 stages 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.
- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know other's password
- Application shall provide the appropriate level of data integrity checking, both at input stage and also when data are processed
- Where data is entered manually the application should reject incorrect values such as out of range, invalid characters and incomplete data
- 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 & ISF will ensure that all systems acquired are implemented along with the required controls identified.

8.6.1 Information Systems

- Information systems are used in Projects and Support Functions for planning, monitoring and analyzing their various activities. These are critical to the organizations' business continuity and hence needs to be secured.
- Business risks arising out of the Information System being used by the project/function are recorded in their Risk register and appropriate controls are identified and implemented
- Backend access to Information systems shall be controlled and the access rights/controls shall be defined in their respective configuration management plans
- Where the password management system can be integrated with the domain password system the same shall be implemented. Where not feasible, controls for password strength and its renewal are established and implemented

8.6.2 Security in Development and Support Processes

- Refer to Configuration Management process for security to Development environment in case of software solutions developed by Pramati

8.6.3 Change Control Procedures

- Refer to Configuration Management process and review process in PAL for changes to Operating System/Development environment in case of software solutions developed by Pramati.
- An approval process as part of change management will be followed before any code is moved to Production or any other environment. Such approvals will be made by the Delivery lead/manager or the client as per the business requirement.

8.6.4 Technical review of operating system changes

- Refer to Configuration Management process and review process in PAL for changes to Operating System/Development environment in case of software solutions developed by Pramati

8.6.5 Restrictions on changes to software packages

- Refer to Configuration Management process in PAL for changes to software work products in case of software solutions developed by Pramati.

8.6.6 System Engineering Principles

- Delivery teams will follow agile methodology or the software development life cycle defined by the client
- Projects will have a defined delivery process or Standard operating Procedures as per the client needs
- Typical four week sprints may be planned in projects where Agile methodology is followed

- Releases may follow development and testing cycles in the sprints
- System testing is done in test environment. Projects will be tested on the security requirements gathered and provided by clients or identified in product development
- Change control procedures are applied before a release can be deployed to the next environment or the production environment. However in some projects, the client's change control procedures may be followed.

8.6.7 Operational Change Controls

- Changes to Network/Hardware/OS/Application Software configurations shall be initiated based on the business requirements by the respective function head and approved by the Leadership team
- The approved changes shall be communicated to the Head of IT for implementation
- All such service requests shall be logged and tracked using the Service Request Tracker (Helpdesk.pramati.com)
- All changes to Network/Hardware OS/Application Software configurations shall be evaluated for impact/new security risks and appropriate actions taken

8.6.8 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.
- An approval process as part of change management will be followed before any code is moved to Production or any other environment. Such approvals will be made by the Delivery lead/manager or the client as per the business requirement.
- The access control mechanism and the access rights for such work products are defined in the Configuration Management Plan.

8.6.9 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 quality.
- Pramati Leadership shall identify annually the facilities required for future business functions.

8.6.10 Protection of system test data

- As per configuration management process

8.6.11 Access control to program source library

- As per configuration management process

8.7 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 Information Security Risks 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 ISMS@Pramati.com is created where all users are required to report security incidents
- CISO shall receive the copy of incidents reported to the above mail id
- CISO shall log all security incidents into the Incident Tracker. CISO in consultation with the Risk Owner and Management shall identify immediate corrective actions. Improvement opportunities covering all such risk areas should be worked out and a feedback mechanism designed such that any scope for such incidents are identified in advance and acted upon.
- The action points, responsibility and the planned completion schedule shall be logged in the Incident Tracker
- CISO tracks all the action points to satisfactory closure
- Causal Analysis of security incidents are done on a monthly basis by the MR/CISO 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 and discussed during the Management Review meetings

8.8 Business Continuity Management

- The organization shall ensure that the BCP be derived with active involvement of the Leadership team member/s as part of the Information Security Forum to ensure its wider 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.
- Chief Information Security Officer shall ensure that plans are developed which allow the recovery of business process within a defined time frame.
- The plans shall have to address the following issues:
  - Identification and prioritization of critical business processes
  - The potential impact of various types of disaster on business processes
  - Accommodation and communications arrangements
  - Responsibility and authority for invocation and 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 external party service providers will include requirements of business continuity and disaster recovery of the organization’s data where feasible.
- Refer **Business** Continuity Plan

8.9 Compliance with Legal Requirements

- The Information Security Officer 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.
- Chief 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.
- Lists of applicable legislative and regulatory requirements are maintained by the CISO.
- IT Support maintains a track of software licenses acquired by the organization and their utilization.
- All functions shall identify the applicable legislative, regulatory and contractual requirements and the interfaces with which organizations personnel should interact. This shall be communicated to Chief Information security officer

8.9.1 Reviews of security policy and technical compliance

- Risk owners/Function 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 action. Improvement opportunities shall be identified, recorded and acted upon by the Risk Owners/Function Heads
- In addition Technical compliance and risk review shall be done for identified critical systems through the use of external security experts.

8.9.2 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

8.9.3 Documented Operating procedures

- All IT Support activities specified in the above sections shall be performed in accordance with the IT Support process
- In addition IT Support shall develop and use additional procedures, plans, guidelines and checklists and procedures for individual activities as required and shall be referred from IT Support Process
- Refer to IT Support Process

9.0 ISMS Key Metrics

Definition	Data Source	Period (months)	Target	Actual
Number of security incidents which leads to loss of business or critical assets.	Incident Report	12	0	
Number of causes re-occurred and resulting in non-conformities during audits	Audit Report	12	0	
Number of major disciplinary actions taken	Incident Report	12	0	
Number of virus outbreaks	Incident Report	12	<2 - minor 0 - major	
Planned Vs. actual availability of infrastructure critical for service provision	BCP Test Plan BCP Test Reports	6 - 3 planned for each location	100%	

Domain Name	Category Description	Domain Level Measurement	Target	Actual
Security Policy	Information Security Policy Document	# of times information security policy is reviewed in a year	1	
Organization of Information Security	Internal Organization	# of management reviews in a year	1	
Access Control	Business requirements for access control	Number of NCs found during audit for access control	0	
Business Continuity Management	Aspects of business continuity management	% of BCP Testing carried out	100%	
Communications and Operations Management	Third Party Service Delivery Management	# of times of review of third party services	1	
Operational procedures and responsibilities	System Planning and Acceptance	Number of incidents due to failure of capacity planning	<=1	
Protection from malware	Protection against Malicious and Mobile Code	Number of malware incidents reported	0	
Equipment	Infrastructure availability	Failures at device level leading to loss of infrastructure availability	<=1	
Network Security Management	Security of network services	Number of security vulnerabilities found in Vulnerability Assessment and Penetration Testing	<=10-12	