Information Security Management System Policy

"Ensuring the Confidentiality, Integrity, and Availability of Organizational Data"

Satwic Inc.

177 E Colorado Blvd, Suite 200, Pasadena, CA 91105

(818)230-2181

November 2024

Contents

Password Policy 3
Mobile Devices & BYOD Policy 4
Outsourcing & Supplier Relationships Policy 7
Information Exchange Policy 10
Logging & Monitoring Policy 11
Technical Vulnerability Management and Malware Policy 13
Asset Management Policy 15
Information Security Incident Management Policy 19
Legal and other requirements Policy 23
Secure Development Policy 26
Risk Management Policy 29
Clear Desk and Clear screen Policy 35
Business Continuity Management & DRP Policy 37
Teleworking policy 39
Cryptography Policy 41
Capacity Management Policy 43
Capacity Management Policy 44
Network Security Management Policy 45
Back up Policy 47
Media Handling Policy 49
Physical And Environmental Security Policy 52
Human Resource Security Policy 59
IT Access Control Policy 62
Admin Access Control Policy 68
Internet & Email Security Policy 70

Password Policy

1.Policy

To define, implement and maintain a documented policy for setting passwords

2. Definitions:

2.1. Dy CISO –Deputy Chief Information Security Officer
2.2. SA – System Administrator
2.3. LAN – Local Area Network

3. Applicable ISO Clauses / Controls:

A.9.4 System and application access control
A.9.4.3 Password Management System

4. Scope:

Applicable for all the Desktops, Laptops, Servers and Standalones

5. Policy:

5.1. Password strength:-

5.1.1 Password should consist of minimum eight alphanumeric characters.

5.1.2 Acronyms, random letters, non-alphabetic characters, numbers and letter combinations can be used as password

5.1.3 Upper and lower case combination can be considered such as Example

"SatWic@MeD01B"

5.1.4 Numbers, symbols and special characters can be used with combinations.

5.1.5 Password should not be chosen in the way that it can be found easily while typing.

5.2. Password use

5.2.1. Password should not be shared among users / groups, i.e., within the group or outside the group.

5.2.2. Password should not be shared in telephone or email upon any emergency request.

5.2.3. Password should not be written or sticked in the noticeable way.

5.2.4. No logging in on behalf.

5.2.5. Passwords should be used by the users only in the allocated terminals.

5.2.6. Wrong passwords or forgotten cases should be reported to SA / ISO.

5.3. Passwords validity for Users

5.3.1. The passwords maximum age will be 42 days.
5.3.2. The passwords minimum age will be 30 days.

5.4. Password setting

5.4.1. The SA will be responsible for setting up the passwords. In absence of SA, ISO will be responsible.

5.4.2. The first time change of password will be performed by the user.

5.4.3. The use of previous five passwords will be restricted for use.

5.4.4. All employees are communicated to allocate password for the all the possible asset across the organization.

5.4.5. The user id and password generated / provided by the client for their application shall be safeguarded by the user itself. In such case, System Administrator is not held responsible for users not changing the Application Software passwords. If such user id or password is not functioning, respective users will contact Tech lead / Project Manager to resolve the issue.

Mobile Devices & BYOD Policy

1. Purpose:

To define, implement and maintain a documented policy for portable devices security.

2. Definitions:

2.1. DY CISO –Deputy Chief Information Security Officer
2.2. SA – System Administrator
2.3. HR – Human Resources
2.4. PDA – Personal Digital Assistant
2.5. SSID- Server Set identity

3. Applicable ISO Clauses/ Controls:

A.6.2 Mobile devices and teleworking
A.6.2.1 Mobile device policy
A.6.2.2 Teleworking

4. Scope:

Applicable to all the Assets owned by employees or company provided such as Laptop's, phones / smart phones, Tablets, Digital camera and storage media such as Portable hard disk, USB memory sticks, disk drives, Data Card and portable printer, etc.

5. Policy:

5.1. Mobile Devices:

a) Satwic takes special care to ensure that business information is not compromised taking into account the risks of working with mobile devices in unprotected environment.

b) All the mobile devices owned by the company are listed in Asset List maintained by SA.

c) Users required software's are installed on the mobile devices and if required patches are updated during its use. All mobile devices are pre-installed with software to track the download and its usage.

d) Any devices shall be provided for the employees upon the request and authorization from management. CISO/ Manager HR authorizes the request.

e) The SA shall further co-ordinate with CISO for the purchase of devices or using the existing. The handover / takeover report / asset user sheet is completed on the above cases.
f) It is the responsibility of SA to specify all the conditions in writing. The conditions for the usage of laptop shall be provided and agreed with the employees prior to the handover of such devices.

g) SA issues any asset after getting duly signed by the receiver.

h) SA installs necessary applications required for business processes and antivirus programs and advice the user on its usage.

i) SA randomly conducts system audits to ensure the assets provided to employees once in 6 months. In case of any discrepancies are reported to concerned Tech Lead and marking copy to CISO.

j) Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

5.1.1. Physical protection

a) Portable devices are prone to rougher treatment than the desktop computers and therefore the likely damages and breakdown are high. Hence it is the responsibility of the user to take adequate care while handling the portable devices.

b) The portable devices shall not be left unattended in the public places. When the user leaves the portable devices within the office premises, it shall be locked.

c) Portable devices shall be carried as hand luggage and safe guarded where possible when travelling.

d) The user is not advised to leave the laptop in any transportation mode.

e) Users shall report to SA or Tech Lead in case of any damage / corruption / data loss. Users shall not take any action by themselves. SA is authorized to take any actions on repair.

5.1.2. Environmental protection

a) The devices shall not be used in the extreme heat environment. The removable devices shall not be connected continuously for long time and shall be removed after the purpose is complete.

b) The devices shall always be kept in safer mode after its usage. The devices shall not keep connected for long time in public places.

c) The user shall review the user manual for additional care.

5.1.3. Software and data protection

a) The operating system stored in the devices such as Laptop's are protected. Hence installing of any unknown software is risk for the device.

b) SA shall enforce security settings to prevent the installation and use of any unknown software.

c) The recovery programs and license shall be kept within the control of SA.

d) The virus programs / Firewall shall be used to defend the virus attack / Spam's

5.1.4. User responsibilities

a) It is the responsibility of the user to take care of the Mobile devices while it is under their control.

b) The user shall not allow any other unauthorized user to use the mobile devices during their presence or absence.

c) In case some data to be retrieved from such systems in absence of the authorized users, prior approval from Tech lead / MD is required.

d) The users shall be provided with the awareness of security policies, asset usage policies and user manual.

5.2. Bring your own devices (BYOD)

a) Personally owned devices (PODs) are ICT (Information and Communications Technology) devices owned by the employees or by third parties such as suppliers, consultants, contractors, service providers and customers.

b) The PODs are used for making and receiving phone calls and text messages on their own personal cell phones, using their own tablet / computers to access, read and respond to work emails, or working in a home-office.

c) POD's brought by employees must be approved by management before its use in Satwic premises. SA maintains list of POD's declared by employees.

d) SA has allocated IP Numbers for authorized POD users.

e) SA reviews the POD/BYOD users are having suitable antivirus software before it gets connected to Satwic network.

f) BYOD users creating, modifying the data during its usage is instructed to upload the data to the SharePoint. Presently POD used for BYOD will have limited access to emails only.

Outsourcing & Supplier Relationships Policy

1. **Purpose:**

   To define, implement and maintain a documented policy for outsourcing.

2. **Definitions:**

   2.1. ISO –Information Security Officer
   2.2. SA – System Administrator
   2.3. HR – Human Resources
   2.4. PUR – Purchase
   2.5. STR- Stores
   2.6. ADM- Administration

3. Applicable ISO Clauses / Controls:

A.13.2.4 Confidentiality or non-disclosure agreement

A.14.2.7 Outsourced development

A.15.1.1 Information Security policy for supplier relationships

A.15.1.2 Addressing security within supplier agreement

A.15.1.3 Information and communication technology supply chain

A.15.2.1 Monitoring and review of supplier services

A.15.2.2 Managing changes in supplier services

4. Scope:

Applicable to all the Employees, Contractors and Consultants.

5. Policy:

Presently no software development is outsourced. The outsourced processes are Security, housekeeping, statutory compliance auditors, trainers and consultants.

5.1. Appointment of outsourced company/ supplier/ AMC Service provider

a) It is the responsibility of the Managing Director to decide on the appointment of an outsourcing agency.

b) The decision of outsourcing shall not be complete without the security requirements are satisfied.

c) It is the responsibility of the CISO to make necessary site visit and authorize the outsourcing agency before signing formal agreement with the outsourcing agency.

d) Suppliers such as outsourced companies, vendors, contractors, AMC Service providers are listed in Approved Suppliers List. The selection process is detailed in Standard Operating Procedure for Purchase.

5.2. Agreement with outsourced companies / suppliers

A formal confidentiality or non-disclosure agreement shall be signed between the company and the outsourced organization / suppliers / AMC Service providers with the following criteria.

- Validity
- Parties name and signature including the signature of witnesses
- Confidentiality
- Liquidity damages
- Handling of disputes
- Third party rights
- SLA parameters
- Law and jurisdiction

5.3. Monitoring and control

a) While the work is carried out outside the perimeter of Satwic office, the work sheet / visits completed report shall be submitted by the outsourced company.

b) The work sheet / visits completion report will be reviewed by the concerned department. Any deviations pertaining to the information security shall be immediately reported to the CISO for further actions.

c) No work shall be carried out by the outsourcing party without the authorization of work.

d) All suppliers / outsourced process / AMC service providers are evaluated once in 6 months by purchase department in consultation with respective departments. In case of any deviations / lapses, necessary actions are initiated and communicated.

5.4. Third party access

a) The outsourced / suppliers access to the Satwic server / terminal within / outside the company perimeter shall not be permitted without a formal agreement between Satwic and outsourced company / suppliers.

b) The concerned department should intimate the CISO about any planned visit of an outsourcing party within the company.

c) It is also the responsibility of the concerned department to maintain the control over the outsourcing party by adequate supervision.

d) The entry and exit of an outsourcing party shall be recorded in the visitor register book maintained at Front Office / Reception.

e) Any deviations pertaining to the information security shall be immediately reported to the CISO for further actions.

Information Exchange Policy

1. Purpose:

To define, implement and maintain a documented policy for information exchange.

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator

2.3. TL – Tech Leader

2.4. NR – not relevant

2.5. R – read only

2.6. R/WR – Read and write access

3. Applicable ISO Clauses/ Controls:

7.4 Communication

4. Scope:

Applicable to all the Employees of Satwic.

5. Policy:

a) Satwic has defined a systematic information exchange matrix, consisting various type of information and its exchange mode.

b) Based on the business need and criticality of information the exchange matrix for various designations is drafted in below table.

5.1 Exchange Matrix

Sl No	Type	Department	Exchange mode	Exchange matrix					
				MD	Manager HR	Tech Lead	SA	Admin	Finance Exe
1	Proprietary information	Finance	Electronic	R/WR	NR	NR	NR	NR	R
			Hard copy	R/WR	NR	NR	NR	NR	R
2	Confidential information	Finance	Electronic	R/WR	NR	NR	NR	NR	R/WR
			Hard copy	R/WR	NR	NR	NR	NR	R
		HR	Electronic	R/WR	R/WR	NR	NR	NR	NR
			Hard copy	R/WR	R/WR	NR	NR	NR	NR
		ADMIN	Electronic	R/WR	R	NR	R	R	NR
			Hard copy	R/WR	R	NR	R	R	NR
			Electronic	R/WR	R	NR	NR	R	NR

		IT	Hard copy	R/WR	R	NR	NR	R	NR
		PM	Electronic	R/WR	R	R/WR	NR	NR	NR
			Hard copy	R/WR	R	R/WR	NR	NR	NR
3	**Personal information**	Finance	Electronic	R/WR	R	NR	NR	R	R/WR
			Hard copy	R/WR	R	NR	NR	R	R/WR
		HR	Electronic	R/WR	R/WR	NR	NR	R	R
			Hard copy	R/WR	R/WR	NR	NR	R	R
		ADMIN	Electronic	R/WR	R	NR	R	R/WR	R
			Hard copy	R/WR	R	NR	R	R/WR	R
		IT	Electronic	R/WR	R	NR	R/WR	R	R
			Hard copy	R/WR	R	NR	R/WR	R	R
		PM	Electronic	R/WR	R	R/WR	NR	NR	R
			Hard copy	R/WR	R	R/WR	NR	NR	R
4	**Internal use Documents and records**	Finance	Electronic	R/WR	R	NR	NR	R	R/WR
			Hard copy	R/WR	R	NR	NR	R	R/WR
		HR	Electronic	R/WR	R/WR	NR	NR	R	R
			Hard copy	R/WR	R/WR	NR	NR	R	R
		ADMIN	Electronic	R/WR	R	NR	R	R/WR	R
			Hard copy	R/WR	R	NR	R	R/WR	R
		IT	Electronic	R/WR	R	NR	R/WR	R	R
			Hard copy	R/WR	R	NR	R/WR	R	R
		PM	Electronic	R/WR	R	NR	NR	NR	R
			Hard copy	R/WR	R	NR	NR	NR	R
5	**Deliverables**	Finance	Electronic	R/WR	R	NR	NR	R	R/WR
			Hard copy	R/WR	R	NR	NR	R	R/WR
		HR	Electronic	R/WR	R/WR	NR	R	R	R
			Hard copy	R/WR	R/WR	NR	R	R	R
		ADMIN	Electronic	R/WR	R	NR	R	R/WR	R
			Hard copy	R/WR	R	NR	R	R/WR	R
		IT	Electronic	R/WR	R	NR	R/WR	R	R
			Hard copy	R/WR	R	NR	R/WR	R	R
		PM	Electronic	R/WR	R	R/WR	R	NR	R
			Hard copy	R/WR	R	R/WR	R	NR	R
6	**Daily report**	Finance	Electronic	R/WR	R	NR	NR	NR	R/WR
			Hard copy	R/WR	R	NR	NR	NR	R/WR
		HR	Electronic	R/WR	R/WR	NR	NR	R	NR
			Hard copy	R/WR	R/WR	NR	NR	R	NR
		ADMIN	Electronic	R/WR	R	NR	R	R/WR	R
			Hard copy	R/WR	R	NR	R	R/WR	R
		IT	Electronic	R/WR	R	NR	R/WR	R	R
			Hard copy	R/WR	R	NR	R/WR	R	R
		PM	Electronic	R/WR	R	R/WR	NR	NR	R
			Hard copy	R/WR	R	R/WR	NR	NR	R

Logging & Monitoring Policy

1. Purpose:

Satwic has documented, implemented and maintained Logging and Monitoring Policy to ensure that information systems meet the desired level of confidentiality, integrity, availability and protection.

2. Definitions:

2.1. DY CISO –Deputy Chief Information Security Officer

2.2. SA – System Administrator or IT Head

2.3. HR – Human Resources

2.4. ADM- Administration

3. Applicable ISO Clauses/ Controls:

A.12.4 Logging and Monitoring

A.12.4.1 Event Logging

A.12.4.2 Protection of log information

A.12.4.3 Administrator and operator logs

A.12.4.4 Clock synchronization

4. Scope:

Applicable to all critical IT and Information assets of Satwic.

5. Policy:

a) Incident tickets are initiated as result of monitoring and managed as per Incident Management policy.

b) Access to office premises logs are maintained by HR Department. Attendance logs are recorded in Attendance Register.

c) Clocks of all systems used in satwic are synchronized.

d) Logs related to any attacks are reviewed on monthly basis by System administrator. If critical data is identified as a part of incident, then the same will be retrieved and backed up.

e) Audit logs contains, user IDs, date and time stamps of key events, records of successful and rejected system access attempts, records of successful and rejected data and other resource access attempts, network addresses, alarms raised by the access control system as appropriate. Presently this is not possible since the Firewall Software or any other software are not used in Satwic.

f) The audit logs which contain intrusive and confidential personal data are monitored by SA and CISO. Where required, administrators are not provided with permission to erase or de-activate logs of their own activities.

g) Audit logs are archived and retained minimum one year, where required by law, audit logs are retained and stored permanently.

5.1. Usage logging

The usage logging shall be monitored on regular basis in order to improve the performance of the business processes, identify and investigate prohibited or misuse.

5.2. Access facility

HR Department shall ensure that the access facility will be revoked upon the termination of the employment contracts. The access facility application shall be monitored upon the need basis, where appropriate, based on any incidents reported.

Technical Vulnerability Management and Malware Policy

1. Purpose:

To define, implement and maintain a documented policy for technical vulnerability management.

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator

2.3. HR – Human Resources

3. Applicable ISO Clauses/ Controls:

A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities

A.12.6.2 Restriction on software installation

A. 12.2 Protection from Malware.

4. Scope:

Applicable to all the employees, contractors and consultants; Information and Information processing assets.

5. Policy:

5.1. Management of technical vulnerabilities

a) Satwic shall take proactive steps to identify and minimize the vulnerabilities in the technology environment before they can be exploited.

b) Sophos XG Firewall has been installed to protect from outside treats.

c) Security scanning tools (VAPT Test tool) shall be used on the prescribed basis to identify vulnerabilities that could be exploited by persons performing unauthorized scanning with similar tools.

d) Multiple tools under different technologies shall be used to identify as much vulnerability as possible.

e) The users will be notified before performing the scheduled or unscheduled scanning and the effects on the terminals being used.

f) All approved devices attached to the network and running operating systems and application with identified security vulnerabilities are patched in order to address the known vulnerabilities. In case if a device could not be patched, the vulnerability is mitigated with an acceptable alternate security controls.

g) Software assets inventory shall be maintained in order to ensure that known vulnerabilities are readily identified and mitigated.

h) Computers system shall be patched up to date as per the vendor specification or best practices in order to ensure that operations are not disturbed.

i) Security controls that detect malicious code, vulnerabilities or attack signatures shall use the current versions of their detection database.

j) Mitigation procedures shall be in place in case of any event that vulnerabilities are exploited before they can be removed from the environment.

k) Vulnerabilities shall be prioritized in terms of risk to the resources. High risk reported will be fixed on priority.

5.2. Restrictions on software installations.

a) Satwic has communicated to all laptop / desktop users not to download any software without permission of SA / CISO.

b) SA conducts system audit randomly to verify for such software installations. If found, the same will be un-installed and communicated to users.

5.3 System Hardening Procedure.

a) Patch Microsoft Windows after approval.

b) Use strong passwords or pass phrases for all Windows user accounts on your PC.

c) Use and properly maintain good anti-virus software, and optionally anti-spyware software.

d) Firewall should be enabled.

e) Do not open suspicious email attachments or respond to suspicious requests.

f) If you're not using it, disable the Windows File and Printer Sharing service.

g) Disable any unneeded user accounts.

h) Lock your PC's screen when you step away, and shut down your computer when you'll be gone for more than 6 hours.

i) Where possible, consider using a web browser other than Internet Explorer, and treat "free" software with suspicion.

5.4 Protection from Malware.

Installation and Updates:

a) SAD will install anti-virus software on all the systems.

b) The team will configure each desktop so that antivirus gets updates daily.

Monitoring:

a) Each employee will check antivirus update every day on their machine.

b) SAD team will monitor the computer at the regular interval to ensure that the antivirus updates are latest and virus scanning is done regularly.

c) Any incidents found will be reported as mentioned in Incident Management Log.

Asset Management Policy

1. Purpose:

Satwic has documented, implemented and maintained Asset Management Policy to identify organizational assets and define appropriate protection responsibilities.

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator or IT Head

3. Applicable ISO Clauses/ Controls:

A.8 Asset Management

A.8.1 Responsibility for Assets

A.8.1.1 Inventory of Assets

A.8.1.2 Ownership of Assets

A.8.1.3 Acceptable use of assets

A.8.1.4 Return of Assets

4. Scope:

This policy covers the asset purchase, asset history, asset usage and handling, and asset disposal

5. Policy:

5.1.Inventory of Assets

a) Capacity management: It will be the responsibility of SA and CISO to review the utilization of the existing resources & assets and plan adequately for the future needs.

b) SA is held responsible to review the utilization of existing assets and plan adequately for the future capacity requirements to ensure the required system performance.

c) Any asset purchase requirements pertaining to IT shall be communicated to SA

/ CISO, Managers and MD.

d) The asset history shall be maintained for the IT assets and capital assets separately.

e) It will be the responsibility of Finance executive to maintain the history of Capital Assets and SA to maintain the history of IT assets.

f) The IT assets purchased will be updated in the IT Assets. Asset Management System is audited during internal audits.

5.2. Ownership of Assets

a) IT Assets issued to employees are listed in Asset Management System and access to those assets are recorded in Access Control Matrix.

b) HR personnel provide the prior intimation to the SA regarding the new employee with expected date of joining for IT requirements allocation.

c) Assets such as Cash Box are handled by Finance department.

d) Laptops, Data cards and Mobile Phones are issued as per request approved by concerned Department Heads and MD. Issuance records are maintained by SA.

e) Asset owner or Risk owner of each asset is taken as consideration for conducting Risk Management Study. Asset ownership is reviewed during termination / resignation or long leave or as and when significant changes occur to risk assessment study.

f) Satwic has implemented CCTV at front office of the company to monitor Assets, People, infrastructure or unauthorized person's entry and exit. This is to avoid any security incidents or breaches.

g) If the laptop is lost or stolen, User should notify immediately to System Administrator or Information Security Officer or respective Manager available immediately.

5.3. Asset Numbering System:

All the Assets are identified as discussed below:

a) Asset - SW- IT- LP - XXX

SW : Refers to the company name

IT : Refers to the department

LP : Asset Type

XXX : Asset Number

5.4. Acceptable use of Assets

a) The asset user shall be liable for the assets when it is used by the user while its association with the company and return as and when it is needed by the SA.

b) The user shall oblige and follow the user instructions and report in case of any damage or repair without undue delays.

c) External parties such as Vendors / Suppliers / Contractors / Service providers having access to organizations assets are made aware of information security requirements through NDA's / Agreements and briefing if they are deployed at Satwic premises by SA.

d) Assets will be returned back to SA when not in use or on deputation to client location or on long leave.

e) When the assets are exchanged between users for official purpose the concerned user has to intimate to SA through email.

f) All scrap IT assets are disposed as per Media Handling Policy.

g) Admin in consultation with Manager HR & Finance disposes the assets such as tables, chairs, cupboards, etc.

5.5. Virus Protection of Laptops and Desktops

a) Viruses are a major threat to the company and laptops are particularly vulnerable. If their anti-virus software is not kept up-to date. The anti-virus software MUST be updated automatically (Auto run process) is activated by the user or system administrator. If you can't log-in for some reasons, contact system administrator for support and install anti-virus updates.

b) Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from reliable source.

c) Always scan for virus, any files downloaded to your computer from any external source (CD / DVD, USB, Hard Disks and memory sticks, network files, email attachments or files from the internet).

d) Report any security incidents (Such as virus infections) promptly to the System Administrator in order to minimize the damage.

e) Respond immediately to any virus warning message on your computer, or if you suspect a virus. Please do not forward any files or upload data onto the network, if you suspect your laptop might be infected.

5.6. Data card Usage Policy

a) Data card's issued to employees are listed in IT Asset List maintained by System Administrator.

b) If any employee request for Data card, the concerned person should send request for Data card and obtain necessary approvals.

c) Acceptable use of Data card: The data card issued for authorized employees are made aware of its usage and data card usage limits are monitored by SA.

d) If the data card is lost or unsuitable for use, the same will be immediately reported to System Administrator.

5.7. Return of Assets

a) All employees and external parties are responsible to return the assets after its use or upon termination of their employment or agreement.

b) Assets will be removed from the employees as per the Admin Access Control Policy, IT Access Control Policy and Human Resource Security Policy.

Information Security Incident Management Policy

1. Purpose:

Satwic has documented, implemented and maintained Information security incident management Policy to ensure a consistent and effective approach to the management of information security incidents including communication on security events and weaknesses.

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator

2.3. HR – Human Resources

2.4. ADM- Administration

3. Applicable ISO Clauses/ Controls:

A.16 Information Security Incident Management System

A.16.1 Management of Information security incidents and improvement

A.16.1.1 Responsibilities and procedures

A.16.1.2 Reporting Information security events

A.16.1.3 Reporting Information security weaknesses

A.16.1.4 Assessment of and decision on Information security events

A.16.1.5 Response to Information security incidents

A.16.1.6 Learning from Information security incidents

A.16.1.7 Collection of evidence

A.16.1.8 Reporting Information security events

4. Scope:

This policy is applicable for all the functions / departments / areas and Employees and interested parties such as suppliers, contractors, consultants, customers covered under the scope of ISMS.

5. Policy:

5.1 Responsibilities and procedures

a) Satwic has established a procedure through this policy to ensure a quick, effective and orderly response to information security incidents.

b) CISO has defined, implemented and communicated the incident response planning, logging, reviewing, monitoring, detection, analysis and reporting of information security events and incidents.

c) HR & SA is communicated as point of contact for security incidents detection and reporting.

d) Admin / HR maintains list of contacts with interest groups such as Government organizations, statutory bodies, Police, Fire, Hospitals, etc., to handle the issues related to information security incidents are maintained.

e) ISO ensures incidents (events and weaknesses) are reported and recorded.

f) CISO has constituted a forum called “Information Security Forum” which consists of departments such as HR, Admin, SA, Purchase, Finance, Operations personnel for ensuring actions without undue delay of information security events and weaknesses.

5.2 Reporting information security events

a) CISO has established a system for reporting Information security events through emails incidents@satwic.com, Internal messenger, ISMS forum meetings, Management Review Meetings and reporting forms made available for all employees to ensure a quick, effective and order response .

b) ISMS forum communicates or create awareness to all external agencies such as consultants, contractors and suppliers for reporting information security events as quickly as possible.

c) Information Security Incidents reporting Contact details displayed in Reception / Pantry areas to educate employees.

d) Information Security events are such as;

- Security breach of information integrity, confidentiality or availability expectations.
- Human errors.
- Noncompliance with policies & procedures.
- Breaches of physical security arrangements.
- Uncontrolled system changes.
- Malfunction of software or hardware.
- Access violations.
- Virus Attack
- Theft
- Phishing Emails
- Broken drawer when sensitive details kept.
- Emergency door kept open.

5.3 Reporting information security weaknesses

All employees and external agencies using the organization's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services as quickly as possible in order to prevent information security incidents.

5.4 Assessment of and decision on information security events

a) ISMS forum has classified the events as Incidents based on classification defined in 5.2.

b) ISMS forum assess each information security events reported by employees or external agencies and decide to classify and prioritize the Information security incidents to identify the impact and extent of an incident.

c) SA maintains results of the assessment and decisions in Information Security Incident Management Log.

5.5 RCA and Action taken to resolve incident.

RCA for incident happen should be done. Action taken steps to be updated.

5.6 Response to information security incidents

a) ISMS forum is held responsible to respond to relevant persons of the organization with regard to information security incidents.

b) ISMS forum response includes;

1. Collecting evidences as soon as possible after the occurrence.
2. Conducting information security forensics analysis (if required).
3. Escalation to management, as required.
4. Ensuring all involved response activities are properly logged in Incident Management Log for later analysis.
5. Communicating the existence of information security incident or any relevant details thereof to all concern personnel's;
6. Dealing with information security weaknesses found to cause or contribute to the incident;
7. Once the incident has been successfully dealt with, formal closure and recording in the log.

5.7 Learning from information security incidents

a) The Incidents, actions taken and lessons learnt from the reported incidents will be shared to all personnel's involved to reduce the likelihood or impact of future incidents.

b) The actions taken for incidents are reported and submitted during Management Review Meetings. Minutes of meeting addresses incidents related issues and circulated to concerned employees.

5.8 Collecting information security incidents

a) Satwic has defined and applied procedure for the identification, collection, acquisition and preservation of information which serves as evidence.

b) Satwic classifies the incidents reported and decides if forensic evidences are required for the incident.

c) HR personnel will contact legal appointee to take up further in line with jurisdiction (If required).

d) The evidences collected are maintained by Manager HR and preserved to confirm to the rules of evidence laid down in the relevant jurisdiction.

- Identification is the process involving the search for, recognition and documentation of potential evidence.

- Collection is the process of gathering the physical items that can contain potential evidence.
- Acquisition is the process of creating a copy of data within a defined set.
- Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

Legal and other requirements Policy

1. Purpose:

To define and document legal and other contractual requirements compliance policy to avoid breaches of Legal, statutory, regulatory or contractual obligations related to information security.

2. Definitions:

2.1	CISO	Chief Information Security Officer
2.2	DY CISO	Deputy Chief Information Security Officer
2.3	SA	System Administrator
2.4	HRD	Human Resource Department

3 Applicable ISO Clauses/ Controls:

A.18.1	Compliance with Legal and contractual requirements
A.18.1.1	Identification of applicable legislations and contractual requirements
A.18.1.3	Protection of records
A.18.1.4	Privacy and protection of personally identifiable information

4 Scope:

This policy is applicable to the following

a) Compliance to applicable Legal, statutory and contractual requirements

b) Protection of records

c) Privacy and protection of personally identifiable information

5 Policy Description:

5.1 Identification of applicable legislation and contractual requirements

a) Finance Executive and Manager HR are held responsible for getting information about applicable Legal, Statutory, regulatory, contractual and other requirements by referring to any of the following:

Notification from State / Central Government bodies like Companies Act, IT Act, etc.

- Information in Newspapers and commercial databases
- Subscription / contact with Bureau Indian Standard, Book Supply Bureau, Confederation of Indian Industry, etc.,
- Through visiting web site of government organizations such as Service Tax, VAT, Customs, Central Excise, Sales Tax, etc., to get information on latest updates and also through membership.

b) The application for renewal of Consents / Authorization under Government statutory requirements will be given in advance as specified in the Acts / Rules. Renewal frequency mentioned above may be altered as per Notification / Intimation from the government authorities from time to time. The details are recorded in Applicable Legal and other contractual requirements Matrix.

c) The following are the other requirements, which are to be complied with:

- Customer Specific Requirements- MD and Manager Delivery is responsible for communicating the customer requirements to operations team for fulfillment.
- Statutory requirement by Financial Institutions – some institutions like Banks / Insurance companies may require organization to comply with Statutory norms, for those requirements; Finance Executive is responsible for receiving and responding to ensure fulfillment.
- Agreement with public Authorities – Public authorities like social bodies may require the organization to comply with their requirements. Manager HR is responsible for receiving and responding to ensure fulfillment of such requirements.
- Requirements related to IT- MD / CISO / SA are responsible for received and responding to ensure fulfillment of such requirements.

d) Evaluation of Compliance to Legal & other Requirements:

- The evaluation of Compliance to the Legal, Statutory, Regulatory, Contractual requirement & other requirements is carried out by HR & Finance Department as per the periodicity mentioned in Legal Matrix
- The evaluation covers

a. License, consent, authorization

b. Submissions to respective departments as mentioned in the Matrix.

c. Notifications, publications, communications by Government Authorities and reply.

d. Compliance to other requirements

e. Updating in legal requirement and their compliance.

- The HR Department takes appropriate decision in case of any discrepancy on the above and records the same. HR Department also verifies the records maintained at required areas / operations. The evaluation results are recorded. HR initiates corrective actions based on evaluation report (if necessary).

5.2 Protection of records

a) Satwic has classified the records such as operations records, accounting records, database records, transaction logs, audit logs, specification / drawings shared with interested parties, etc.

b) Records generated as physical hard copies are maintained in racks, cupboard, lockable cabinets and labeled as per Information Classification.

c) Records generated through electronic media are processed and stored in External HDD. Backup of these records are taken as per defined frequency documented in Procedure for System Administration and Backup Policy.

d) In case of records related to Legal, statutory and contractual requirements, respective departments are held responsible.

1. Finance Department is held responsible for records retention, storage, handling and disposal of Finance and Accounting records.

2. HR Department is held responsible for records retention, storage, handling and disposal of HR related records.

3. IT related records such as audit logs/ administrative logs, Server logs are retained till its use.

e) Records stored in Storage media are password protected before it is moved to Bank Lockers.

f) SA is responsible to ensure that data is accessible or readable format to safeguard against loss due to change in technology. Data retrieval or restoration is carried out once a year and records are maintained.

5.3 Privacy and protection of personally identifiable information

a) HR department has implemented the Privacy Act applicable for Satwic. The contents written in privacy act related to the employee personnel information are retained as confidential and not disclosed to others.

b) Protection of personally identifiable information such as name, residential address, family details, personal email ID, Digital Identity such as Aadhar Number, PAN Card, Voters ID, telephone numbers, Appraisals, Salary & benefits details, background verification status, etc., retained as part of Employee Personal file is stored in lockable cabinets. No such information is disclosed to any employees, contractors, suppliers, etc.

c) This is communicated through forums/ meetings/training to all employees of the organization.

Secure Development Policy

1. Purpose:

Satwic has documented, implemented and maintained Secure Development Policy applicable for project management activities.

2. Definitions:

2.1 CISO- Chief Information Security Officer

2.2 Dy CISO- Information Security Officer

2.3 MR -Management Representative

2.4 SD -Software Development

2.5 HIT -Head Information Technology

2.6 PL -Project Lead

2.7 TL -Team Lead

3. Applicable ISO Clauses/ Controls

A.6 Access Control

A.6.1 Internal Organization

A.6.1.5 Information Security in project management

A.14.2 Security in development and support processes

A.14.2.1 Secure Development Policy

A.14.2.2 System change control procedures

A.14.2.3 Technical review of applications after operating platform

A.14.2.4 Restrictions in changes to software packages

A.14.2.5 Secure system engineering principles

A.14.2.6 Secure development environment

A.14.2.7 Outsourced development

A.14.2.8 System security testing

A.14.2.9 System acceptable testing

A.14.3 Test data

A.14.3.1 Protection of test data

4. Scope:

This Policy covers project management activities as per the Satwic customer requirements to ensure that information security is designed and implemented within the project management lifecycle of information systems.

5. Policy:

NOTE: All activities related to project management lifecycle such as Software development and Managed Support services are performed on client's provided Applications/Servers /Tools.

5.1 Information Security in Project Management (A.6.1.5 of ISO27001:2013)

Information security requirements are addressed during Project Planning phase as part of Risk Management process.

5.2 Secure development policy (A.14.2.1 of ISO27001:2013)

Rules for the development of software and systems are established and applied to development within the project lifecycle. This is detailed in Project initiation phase and the SRS/CRS/Contract document is made available.

5.3 System change control procedures (A.14.2.2 of ISO27001:2013)

Changes to the systems within the development life cycle are controlled by the use of formal change control as per the Change Management procedure (PMS-PPT-04 ServiceNow-Change Management-Satwic.pdf)

5.4 Technical review of applications after operating platform changes (A.14.2.3 of ISO 27001:2013)

In case of any operating platforms changes or the proposed change is reviewed in line with business critical applications and tested to ensure that there is no adverse impact on organizational operations or security.

5.5 Restrictions on changes to software packages (A.14.2.4 of ISO27001:2013)

a. Software development team uses working folder and project dump or any applicable folder structure to upload the developed source code.

b. No team members are allowed for modifications or changes to software other than what is mentioned in the change process as detailed in Change Management.

c. Project Lead / Tech Lead is responsible to ensure no changes carried out to software packages before release to customer. In case of any changes carried out is detailed in Change Management.

5.6 Secure system engineering principles (A.14.2.5 of ISO27001:2013)

Principles of engineering secure systems such as Architecture followed during software development are detailed in planning phase.

5.7 Secure development environment (A.14.2.6 of ISO27001:2013)

Software development is carried out in secured environment such as segregation in working area, test server for testers and access controls defined for the team.

5.8 Outsourced development (A.14.2.7 of ISO27001:2013)

Presently no software is outsourced for development.

5.9 System security testing (A.14.2.8 of ISO27001:2013)

Project Lead / Tech Lead identify the required testing of security functionality as per customer requirements during Project Planning Phase. Testing is detailed. Test results are recorded and maintained in Project folder. Currently Satwic is not handling QA testing

5.10 System Acceptance Testing (A.14.2.9 of ISO27001:2013)

Acceptance testing programs and related criteria are developed as Test Cases and test results are recorded for the development software packages. The test criteria are reviewed for new information systems, upgrades and new versions.

5.11 Protection of Test data (A.14.3.1 of ISO27001:2013)

Any information used for testing the Operational database will be saved in the "Test Server – Client application", access to the test server will be provided only to the authorized implementers approved by concerned Department Head.

Risk Management Policy

1. Purpose:

The Purpose of this policy is to provide need and direction to management in selection, establishment and implementation of safeguards and to define coordinated activities to direct and control the organization with regard to risk.

2. Definitions:

2.1. CISO –Chief Information Security Officer

2.2. SA – System Administrator

3. Applicable ISO Clauses/ Controls

6.1 Actions to address risk and opportunities

6.1.1 General

6.1.2 Information Security Risk Assessment

6.1.3 Information Security Risk Treatment

4. Scope:

This policy applies to all Information System Assets and Information processing assets of Satwic.

5. Policy:

5.1 Risk Assessment Approach

a) Risk Assessment is conducted for all assets defined in Information Security Risk Assessment and Risk Treatment Plan of respective departments/ functions.

b) Risk assessment is a combination of the potential adverse business impacts of unwanted incidents, level of assessed threats, vulnerabilities and the existing/ proposed safeguards.

c) Risk Assessment is carried out by core functional team & ISMS forum.

d) Core functional team comprises of:

- Departmental Heads
- Managing Director (Chief Information Security Officer)
- Manager HR & Admin
- Manager Delivery
- System Administrator (DY Chief Information Security Officer)
- ISMS forum

5.2 Detailed Risk Analysis

5.2.1 Identifying Asset:

- Risk Analysis is performed for all information & Information processing assets.

5.2.2 Assets are categorized for conducting Risk Assessment as follows:

1. Information assets
2. Hardware Assets
3. Software Assets
4. Service Assets
5. People Assets

5.2.3 Owner:

a) Responsibility of owning, protecting and using the Asset must be identified.

b) Owner will be an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the asset.

Ex: Laptops / Desktops

Risk Owner: Head of Department

Data Custodian: Users

5.2.4 Location of the Asset:

- Identify the location of the asset where it is kept.

5.2.5 Asset Value:

All assets are valued in non-financial terms such as Low, Medium and High to the organization based on the cost of obtaining and maintaining the asset and the potential adverse business impacts from loss of confidentiality, integrity and availability.

Asset Value	Explanation
Confidentiality	The Property that information is not made available or disclosed to unauthorized individuals, entities or processes.
Integrity	The property of safeguarding the accuracy and completeness of Assets
Availability	The property of being accessible and usable upon demand by authorized entity

Asset will be categorized based on the asset value as defined below:

Rate each asset for C, I, A on a scale of 1-3 where scale 1 is low 2 is Medium and 3 is High. The valuation will be done based on the importance of the asset to the organization business.

Calculate Asset value as sum of values of C, I and A.

Asset Value = C+I+A

5.2.6 Identifying Threat:

- Histories of incidents / Change managements / Problem managements are utilized as inputs for Threat assessment.
- Threat assessment is performed identifying its sources and the likelihood of their occurrence, ensuring that no relevant threat is overlooked.
- Identify the various threats on each asset. Determine the impact of the threat if it is occurs and the frequency of the occurrence. Rate each on scale of 1-5.

Threat Value = Impact + Probability.

5.2.7 Likelihood calculation:

- Identify and assign the value for likelihood of occurrence of each threat as mentioned in the below table

Likelihood	Explanation	Score
Very Low	An event that is highly unlikely to occur , if ever (or) Rare Occurrence	1
Low	An event that is unlikely to occur, perhaps once every 3 years	2
Medium	An event likely to occur relatively infrequently, perhaps once a year	3
High	An event that is fairly probable, and could be expected to occur several times a year	4
Very High	An event that is highly probable, and could be expected to occur at least every month or more frequently	5

5.2.8 Impact calculation:

- A quantitative value has to be given for each Impact as given in the below table

Impact level	Explanation	Score
Minor	Minor impact but not significant	1
Significant	Tangible harm, extra effort required to repair	2
Damaging	Significant expenditure of resources required and/or damage to reputation and confidence	3

Serious	Extended outage and / or loss of connectivity and/or compromise of large amounts of data or services	4
Critical	Permanent shutdown and/or complete compromise of the enterprise	5

5.2.9 Identifying the Impact:

- Assess and describe the business impacts due to effect of losses on confidentiality, availability and integrity resulting from security failures on each threat.

5.2.10 Identifying Vulnerability:

- Vulnerability assessment is performed to identify weaknesses in the physical environment, organization, procedures, personnel, management, administration, hardware, software or communication equipment that may be exploited by a threat source to cause harm to the assets, and the business they support.
- Vulnerability which has no corresponding threat not considered for implementation of safeguard.
- It is mandatory to list down all vulnerabilities which may lead to threat on an asset
- Identify the vulnerabilities which each threat can exploit and rate it on a scale of 1 to 5 based on its exposer value. Where 1 indicates least and 5 is high

5.2.11 Risk Value:

- Risk value will be identified for each Threat based on the addition of, Asset Value, Threat Value and Vulnerability Value.

Risk Value = Asset Value + Threat Value + Vulnerability Value

5.2.12 Rating of each risk will be given as mentioned in the below table:

6	12	18	24	30	36
5	10	15	20	25	30
4	8	12	16	20	24
3	6	9	12	15	18
2	4	6	8	10	12
1	2	3	4	5	6

Risk Value	Risk Level	Color
1 to 12	Low	Green
13 to 24	Medium	Yellow
25 and above	High	Red

Note: Risk Assessment will not be done for the risks which are at Risk Level "LOW"

5.2.13 Existing Controls:

- Existing controls that are available at Satwic in order to reduce the Likelihood of occurrence or Impact are recorded for each threat

5.2.14 Risk Treatment Plan (Required actions):

- Risk Treatment Plan addresses the required / proposed actions defined by the Departments / functions to reduce risk level.
- All the controls that are required to reduce the value of risk must be listed

5.2.15 Risk Owner:

- Risk Owner approval will be obtained for implementing Risk Treatment Plan.

5.2.16 Risk Treatment Plan Implementation status:

- Status is recorded to ensure actions proposed in RTP are implemented.

5.2.17 Reduce Risk Analysis after RTP Implementation:

- Once the Risk Treatment Plan is implemented, again the Risk Value need to be calculated same as defined in Sec 5.2.11 with the reduced Likelihood, reduced Impact and Revised Vulnerability Value.

5.2.18 New Risk Level:

- Record new Risk level as Low / Medium / High
- Reduce Risk Value

Risk Value = Asset Value + Reduced Threat Value +Reduced Vulnerability Value

5.2.19 Risk Categorization and Management Approval:

- The process of reviewing the risk assessment and its framework is ensured once in 6 months for its adequacy and effectiveness.
- No further actions are required for the risk categorized as Low as per para 5.2.18.
- Medium and High Value Risk identified as per para 5.2.17 will be discussed with departmental heads and categorized as Acceptable Risk and Residual Risk.
- Risk identified as Acceptable will be reviewed once in 6 months or as per the RTP Action Plan in line with controls mapped in the Risk Assessment Sheet to reduce the risk level.

- Risks categorized as Acceptable Risk and Residual risk will be approved by MD.
- Risks that can be transferred to others / vendors will be done with the approval of Management (Transfer).
- Risk assessment report is reviewed once in a Year or significant changes such as revision in standard, incident management, business continuity & process change, etc., occur to ISMS.

Clear Desk and Clear screen Policy

1. Purpose:

To define, implement and maintain a documented policy for Clear desk and Clear Screen to prevent loss, damage, theft or compromise of assets and interruption to the organization operations.

2. Definitions:

2.1. CISO – Chief Information Security Officer

2.2. ISO - Information Security Officer

2.3. SA – System Administrator

2.4. Standalone – Terminal not connected in LAN

2.5. HRD- Human Resource Department.

2.6. ADM- Administration.

3. Applicable ISO Clauses / Controls:

A.11.2 Equipment

A.11.2.9 Clear desk and Clear Screen Policy

4. Scope:

Applicable to all the Laptops, Desktops/Workstation, Printers, Scanners, Printouts, Paper documents, white boards, Mails, Couriers, Fax Messages, etc. handled within Satwic premises.

5. Policy:

5.1. Clear desk policy

5.1.1 While leaving the desk, the users shall ensure that the information categorized as Confidential / proprietary / private / public are locked in their own cabinets / racks / lockable cupboards.

5.1.2 Any document/ records/ information which is not needed for the user are shredded by respective departments.

5.1.3 The users shall keep track of their work documents while interaction with other users or groups.

5.1.4 If any official document found without attention the same will be reported to the concerned departmental head or respective users.

5.2. White Boards/ Notice Boards

5.2.1 White boards used will be cleaned before leaving the conference / work locations.

5.2.2 User Names and passwords should not be written in white boards / papers.

5.2.3 It is the responsibility of Administration team member to check the notice boards / white boards and ensure that it will be changed / removed / cleaned upon updates.

5.3. Mails / Couriers / Printouts / Other Media

5.3.1 Incoming and outgoing mails / couriers are recorded by Front Office Staff

/ Receptionist.

5.3.2 Every individual is responsible to collect their print-outs immediately from the printer. If any critical print-out left un-attended at the printer, it will be handed over to the concerned department head or members by the employee who finds the print-out.

5.3.3 Movement of materials / equipment including magnetic media coming in or leaving office premises must be entered at the register maintained in front office or receptionist.

5.4. Clear screen policy

5.4.1 While the users leave the terminal, asset or desktop for any amount of time, it is automatically configured to get locked (Session time out activated).

5.4.2 The work documents (if any) kept on the desktop or laptop shall be moved to the appropriate folder by the user. In case the same id noticed by the tech lead or SA, user will be take necessary actions.

5.4.3 Locking the desktop or laptop helps in preventing any unauthorized access of information.

5.4.4 Desktops or Laptops will be locked before interacting with any user or visitor. Ensure that meeting with visitor takes place only in the meeting / conference room.

5.4.5 Common Screen Saver is configured for all users.

Business Continuity Management & DRP Policy

1. Purpose:

To support and define Information Security Continuity Management and redundancies process from the effects of major failure of information systems or disasters to ensure their time resumption. This is done by ensuring that the required Information Technology technical and service facilities can be recovered within required and agreed business time-scales.

2. Definitions:

2.1 DY CISO Information Security Officer

2.2 SA System Administrator

2.3 HR Human Resources

2.4 ADM Administration

3. Applicable ISO Clauses/ Controls:

A.17 Information security aspects of business continuity management

A.17.1 Information Security continuity

A.17.1.1 Planning information security continuity

A.17.1.2 Implementing information security continuity

A.17.1.3 Verify, review and evaluate information security continuity

A.17.2 Redundancies

A.17.2.1 Availability of information processing facilities

4. Scope:

• Any incident which affects Business continuity including Business Operations, Information Technology, Information Security facilities, Power outage, Civil/Public unrest, Staffing, Natural calamities etc

5. Policy:

5.1 Identification of Events and associated assets:

2. Concerned Department identifies the risks associated with the Business process and identifies the assets involved for the business process, Mitigating actions, etc in Risk assessment and Treatment Plan.

3. Disaster event (Result of natural, accidents, equipment failures and deliberate actions) will be identified that can cause interruption.

4. Likelihood:

• Identify and assign the value for likelihood of occurrence of each event as mentioned in the below table

Likelihood	Explanation
Low	Unlikely or Rare Occurrence
Medium	Not so frequent Occurrence
High	Frequent Occurrence

5. Impact:

A value has to be given for each Impact as given in the below table

Impact	Explanation
Low	Negligible or Less impact with less effort to repair
Medium	Tangible harm, extra effort required to repair
High	Significant expenditure of resources required and compromise of the system

6. Business Continuity and Disaster Recovery Plan covers Prevention controls and Recovery or Mitigation Controls, Recovery point objectives, Maximum recovery time objective, DR site, Criteria for Fail over, Escalation Process, Location to convene and Recovery Plan.

6.2 Testing, maintaining and re-assessing

1. Test Plan will be made for the events that can be tested such as UPS, etc and it will be tested as per the frequency defined.

2. Emergency contact list will be prepared and updated for the relevant contact details

3. Business Continuity plan will be communicated to all concerned employees. Project Teams prepare the Business continuity plan for their department and communicated to all the team members.

Teleworking policy

1. Purpose:

To define, implement and maintain a policy to protect information accessed, processed or stored at teleworking sites.

2. Definitions:

2.1 CISO Chief Information Security Officer

2.2 DY CISO Chief Information Security Officer

2.3 MR Management Representative

2.4 SAD System Administrator

2.5 HR Human Resources

3. Scope:

- For the employees who work remotely from outside SATWIC

4. Policy:

4.1 Authorize and control by Management:

4.1.1. Employees, who need to work remotely from fixed location other than SATWIC, must get a prior approval from concerned Department Head.

4.1.2. Based on the approval by Head IT / System Administrator shall configure the required steps to access client server as per client remote procedure.

4.2 Guide to create new Client VPN IDs:

Below is the process each mentor must follow for raising requests:

1) Once new employee has completed his boot camp, his/her manager will fill a new activate Non-Employee Form (Find attachment below) and send to Client Manager.

2) Client Manager will submit a request to create new IDs.

3) Once ID has been created, Client Manger will send account details (user id and password) to Satwic manager.

4) With that User ID and Password, user will login to Client email account and look for account activation link.

5) By following the activation link and the instruction given in the email, user can setup his Client account.

4.3 Protection of Equipment

4.2.1. The concerned employee should take necessary steps to protect the physical security of the assets as defined in Mobile Devices Security Policy.

4.4 Support & Maintenance

4.3.1. Concerned Employee shall raise the ticket for IT Support.

4.3.2. If required the hardware will be handed over to IT Support team for any repair or maintenance, else it will be fixed through remote access itself.

4.3.3. Anti-virus software will be installed in all the system issued by SATWIC.

4.3.4. Patch management will be automatically updated on the individual system.

4.5 Revoking the access rights

4.5.1. At the completion of task or end of contract or termination of employee, the access rights provided to the Concerned will be revoked by IT Support team, as per Access control policy

4.6 Receipt of call from Customer

4.7.1. Customers are provided with SATWIC contact numbers or Video conference numbers.

4.7.2. Through Email support number, Customer shall log their complaints to SATWIC

4.7.3. Support Staff will be available round a clock to answer the Customer Calls.

4.7 Addressing Customer Complaints

4.8.1. Any clarification required by customer on usage of product will be given over the phone, and there won't be any ticket raised on behalf of customer.

4.8.2. In case of any complaints/issue, Customers are requested to raise the ticket in Support portal. If customers are not in a position to raise a complaint, Support staff will raise the same.

4.8.3. Support staff shall interact the Customer over the Phone for any Clarification/updation.

Cryptography Policy

1. Purpose:

The company has documented, implemented and maintained applicable cryptography Policy to

a) Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/ or integrity of information.

2. Definitions:

CISO Chief Information Security Officer

ISO Information Security Officer

SA System Administrator

3. Applicable ISO Clauses/ Controls:

A.10 Cryptography

A.10.1 Cryptographic Controls

A.10.1.1 Policy on the use of cryptographic controls

A.10.1.2 Key Management

4. Scope:

a) Software developed in India for client requirements

b) Key Management- Digital Signatures

5. Policy Description:

5.1 No cryptography techniques are used/ implemented for any Hardware/Software developed, since most of the projects handled are partial development only.

5.2 Electronic storage media

1) Sensitive information shall be protected against unauthorized disclosure when it is stored on the electronic storage media if the information cannot be protected using sufficient physical or logical controls, and the information is at the risk of being compromised or stolen.

5.3 Remote access

2) Accessing databases, containing confidential or proprietary information from remote location, shall be adequately encrypted to prevent unauthorized entry.

5.4 Backup storage media / password

1) Any data sent outside for storage should be afforded the same level of security as within the company perimeter.

2) To protect from unauthorized disclosure or modification or loss the entire electronic storage media, should be protected with password before sending offsite.

3) The offsite backup storage shall be with Ion-mountain/ nationalized banks.

4) The access privileges to backup and restore files and directories shall be limited to Head IT and management.

5.5 Email encryption

1) Any information transmitted by email will be automatically encrypted by Microsoft office 365 server.

5.6 Encryption of passwords

1) To prevent passwords from being disclosed to sniffer attacks, passwords shall always be encrypted when held in storage or transmission over communications systems.

5.7 Key Management

1) Usage of digital signature is provided only to Finance Dept or Top Management in compliance with Legal requirements. Digital Signature is protected with Password for un-authorized usage.

Capacity Management Policy

1. Purpose:

To define, implement and maintain a documented policy for Capacity Management. Capacity Management ensures that Capacity and Performance of the IT Infrastructure in Satwic matches the evolving demands of its business in the most cost-effective and timely manner.

2. Definitions:

3.1. CISO –Information Security Officer

3.2. SA – System Administrator

3. Applicable ISO Clauses/ Controls:

A.12.1.3 Capacity Management

4. Scope:

Applicable to all the core services provided includes internet services, cloud servers and core network equipment.

Capacity Activities

4.1 Monitoring

Capacity Management Planning shall be done on an annual basis. The utilization of each resource and service shall be monitored on monthly basis.

4.2 Analyze

While monitoring, the collected data is analyzed to determine whether threshold need to be readjusted, resources to be tuned or capacity to be increased/decreased. In the event capacity needs to be increased and results in financial implication, it needs to be escalated to CISO.

Sample of resources monitored and analyzed are:

a) Memory usage (Average Threshold 70%)

b) CPU (Average Threshold 70%)

c) Hard disk usage (Average Threshold 70%)

d) Network bandwidth (Average Threshold 70%)

4.4 Change Initiation

Once the threshold is reached (average for the month), analysis must be done & appropriate action must be taken.

Capacity Management Policy

1. Purpose:

To define, implement and maintain a documented policy for Capacity Management. Capacity Management ensures that Capacity and Performance of the IT Infrastructure in Satwic matches the evolving demands of its business in the most cost-effective and timely manner.

2. Definitions:

2.1. CISO –Information Security Officer

2.2. SA – System Administrator

3. Applicable ISO Clauses/ Controls:

A.12.1.3 Capacity Management

4. Scope:

Applicable to all the core services provided includes internet services, cloud servers and core network equipment.

Capacity Activities

4.1 Monitoring

Capacity Management Planning shall be done on an annual basis. The utilization of each resource and service shall be monitored on monthly basis.

4.2 Analyze

While monitoring, the collected data is analyzed to determine whether threshold need to be readjusted, resources to be tuned or capacity to be increased/decreased. In the event capacity needs to be increased and results in financial implication, it needs to be escalated to CISO.

Sample of resources monitored and analyzed are:

a) Memory usage (Average Threshold 70%)

b) CPU (Average Threshold 70%)

c) Hard disk usage (Average Threshold 70%)

d) Network bandwidth (Average Threshold 70%)

4.4 Change Initiation

Once the threshold is reached (average for the month), analysis must be done & appropriate action must be taken.

Network Security Management Policy

1. Purpose:

The purpose of this policy is to establish an overarching framework for network security that provides assurance that:

a) IT and communications resources are managed securely and consistently according to specified standards and practices.

b) Members of staff are aware of their own responsibilities concerning use of and security of the Trust's network, including acceptable and unacceptable use.

c) Reliable (highly available), safe and secure IT environments are provided for storage, sharing and use of the Trust's information. Information security risks are identified and controlled.

2. Definitions:

2.1. CISO –Chief Information Security Officer

2.2. DY CISO- Deputy Chief Information Security Officer

2.3. SA – System Administrator

2.4. HRD – Human Resources Department

3. Applicable ISO Clauses/ Controls:

A 13.1 Network Security Management

A.13.1.1 Network controls

A.13.1.2 Security of network services

A.13.1.3 Segregation in networks

4. Scope:

This procedure covers access to secure network area.

5.1 Access to networks and network services

5.1.1 Network controls

a) Network access will provided to employee as per the their nature of work.

b) Wireless connectivity is provided to all employees working in Satwic premises.

c) In case of external parties, wireless connectivity will be provided based on confirmation received from CISO or Manager HR.

d) SA monitors the network and network services. Access to Portal will be provided based on the nature of work and need basis, after getting the approval from concerned Department Head / Tech lead.

e) In case if there is any change in access rights, the same should be approved by CISO.

f) Removal of Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, will be disabled or removed manually.

5.1.2 Local Area Network (LAN)

a) It will be the responsibility of System Admin to determine the need for installation, operation, and management of all various Local Area Network deployments.

b) Network is pooled independently for teams and access of information within the teams is restricted to only concerned personnel.

c) Network cabling diagram indicates the current network infrastructure. Network diagram includes Cable Diagram and Fire Extinguishers located point.

d) System Admin shall authorize the need for access by users through LAN.

e) Users / staff may not deploy access points or extend the coverage without the written consent of ISO.

f) In case of any significant issues, usage shall be limited or ceased.

g) All access to wireless network must be authenticated using login account and password.

6. Security of network services:

a) Sophos firewall has been implemented to secure network access.

b) Firewall update will be carried out n-1.

c) The Trust's networks shall be designed, securely configured and maintained to withstand and recover from threats to their availability, integrity and confidentiality.

d) Access to the Trust's networks shall be controlled, subject to appropriate approval from Tech lead.

e) The network/system password shall not be shared within groups or out of groups for any purpose.

7. Segregation in networks

a) Satwic segregated network access as per the employee role.

b) Segregation of network as per Network diagram (IT_F_13- Network Diagram)

Back up Policy

1. Purpose:

To define, implement and maintain a documented policy for Information Backup.

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator

3. Applicable ISO Clauses / Controls:

A.12.3 Backup

A.12.3.1 Information Backup

4. Scope:

Applicable to all the Cloud Servers, Desktops, Laptops, CCTV and standalones.

5. Policy:

5.1. Data backup

5.1.1 All the data will be backed up based on the criticality wherever applicable.

5.1.2 The incremental backup will be taken on the External Hard disk for the critical users and retained with MD Home.

5.1.3 Email backup from all the systems on monthly basis on office 365 server.

5.1.4 On the SharePoint Server, respective users name folder is created. All Users are instructed to transfer the working data to the folders available in the Server.

5.2. Backup restoration

5.2.1. The backup restoration will be done atleast once in a Six Months in order to ensure the integrity of the data.

5.3. Backup register

5.3.1. Backup register will be maintained. The date, time, mode, description of backup will be recorded in the backup HDD register.

5.4. Offsite storage

5.4.1. The External Hard Disk will be stored in the MD's home and replaced as and when it is overwritten.

5.4.2. The External Hard Disk will also be restored atleast once in Six Months for Integrity.

5.5. CCTV

5.5.1. CCTV is monitored for its operation by executive administrator on daily basis.

5.5.2. CCTV footages are reviewed daily by the Administration team member and System Administrator. If the data is critical, the same is backed up and retained by System Administrator.

5.5.3. CCTV footages overwrite once in 30 days..

Media Handling Policy

1. Purpose:

To define, implement and maintain a documented policy for media handling to prevent unauthorized disclosure, modification, removal or destruction of information storage media.

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator

2.3. HR – Human Resources

2.4. ADM- Administration.

3. Applicable ISO Clauses / Controls:

A.8.3 Media Handling

A.8.3.1 Management of removable media

A.8.3.2 Disposal of media

A.8.3.3 Physical media transfer

4. Scope:

Applicable to all the Hardcopy, Hard disk, Compact disks, Pen Drives, DVD, and for media disposal.

5. Policy:

5.1. Management of removable media

Satwic has implemented the management of removal media in accordance with the below classification defined in Scope of this document.

5.1.1. Hardcopies

a)Hardcopies will be shredded before moving to the dustbin.

b)Respective department's personnel's will be responsible to decide on shredding / tearing the documents / records.

c) No printed paper shall be disposed without shredding/tearing.

d) Any document retained for the purpose of Statutory, regulatory and legal requirements will be managed by HR team.

e)Disposal of any important or critical documents are reviewed and approved by the MD before its disposal.

5.1.2. Hard disk

a) Data will be removed and Hard disk will be formatted before giving it to Warranty Replacement / Repair / Handover.

b) Incase if the Data retrieval is not available / possible, data will be recovered by authorized agency, provided NDA signed by such agency.

c) The data will be removed completely before its disposal in any circumstances.

d) System Administrator in consultation with the concerned department representative or user will be responsible for any disposal along with the approval of MD if needed.

5.1.3. Compact disks , Digital Versatile Disks and Pen Drives

a) The data will be checked; if possible backup will be taken and destroyed permanently.

b) Any CDs / DVDs taken for testing purpose has to be returned back to either System Administrator or concerned department representative.

c) Except System Administrator, nobody is authorized to dispose the Disks, In case any incident happens it is considered as Security Breach.

d) System Administrator will make the disk unreadable before its disposal.

e) Pen drives will be broken / trashed before its disposal.

5.1.4. Disposal of Media

a) Media should be disposed of securely when no longer required, using formal procedures.

5.1.5. USB Drives / Removable Medias / Tablets provided by Company

a) All employees must return back the assets at the time of reliving from the organization / Long leave / after completing the usage of it.

b) At the time of returning back the USB Drive / Removable Media, all the information available must be removed by the user. In case if the information is not removed, it is the responsibility of System Administrator to remove the information before it has been issued to next person. Backup will be taken if necessary based on the criticality of the data.

c) In case of repair / damage to pen drives / External Media, the concerned person must immediately report System Administrator and immediately shall be handed over to SA, SA will check and remove the data if possible or format the pen drive. In case the data can't be retrieved and the device has no value, then SA will proceed with disposal process.

5.1.6. Disposal methodology

a) Physical force destruction will be adopted.

b) The System Administrator in consultation with Chief Information Security Officer will be responsible for any devices that are to be disposed.

c) Any computers or peripherals disposed will be recorded in the Remarks Column of Asset List.

5.1.7. Physical media in transit

a) Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

b) Wherever applicable the media transferred to another location / company owned facility / data center / customer data shall be protected with password and hardware is encrypted.

c) Media is sent through authorized courier / logistics service provider. The service provider for logistics / courier used is listed in Approved Suppliers List.

d) Media with contents disposed is recorded in Asset List and in case of any transfer, the details are recorded in outgoing register maintained by Admin Department.

Physical And Environmental Security Policy

1. Purpose:

To define, implement and maintain a documented policy for Physical and Environmental Security to.

a) Prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

b) Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

2. Definitions:

2.1. DY CISO – Deputy Chief Information Security Officer

2.2. SA – System Administrator

2.3. HRD– Human Resource Department

2.4. ADM - Administration

3. Applicable ISO Clauses / Controls:

A. 11. 1 Secure Areas

A.11.1.1 Physical Security perimeter

A.11.1.2 Physical entry controls

A.11.1.3 Securing offices, rooms and facilities

A.11.1.4 Protection against external and environmental threats

A.11.1.5 Working in secure areas

A.11.1.6 Delivery and loading areas

A.11.2 Equipment

A.11.2.1 Equipment siting and protection

A.11.2.2 Supporting utilities

A.11.2.3 Cabling Security

A.11.2.4 Equipment maintenance

A.11.2.5 Removal of Assets

A.11.2.6 Security of equipment and assets of premises

A.11.2.7 Secure disposal or re-use of equipment

A.11.2.8 Unattended user equipment

4. Scope:

a) This policy applicable to all Satwic Employees, Visitors, suppliers, Information processing facilities and buildings.

b) Equipments such as Computers, Laptops, Printers, electronic gadgets, UPS, Air conditioners, LCD Projectors, EPABX, Switch Racks, Server Racks, Land Phones, etc.

5. Policy:

5.1 Secure Areas

5.1.1 Physical Security perimeter

a) The perimeter of building or site containing information processing facilities is well protected and guarded by company outsourced security staff. The same is monitored by admin department.

b) The entry of any personnel will be under continuous surveillance through manned Security and reception.

5.1.2 Physical entry controls

a) The access to office premises is restricted to employees of the Satwic only.

b) Access to external personnel from agencies such as couriers, transportation, logistics, etc. are allowed up to Front office / Reception for delivery or any queries.

5.1.3 Employees entry and exit

a) The employees should enter the timings of entry as soon as they enter the workplace. Presently Access and Biometric Detection System is provided for employees for accessing the workplace. This system is used to access the office doors.

b) Employees are provided with unique identification card and Front Office Receptionist / Security personnel's monitor all employees wearing the card all the time.

c) In case of loss or damage of ID cards, it should be reported to the Admin Staff immediately and obtain the temporary ID cards till they get the new card.

d) Respective department notifies HR Department to remove the access privileges for the terminated or employee resigned from the organization.

e) HR & Admin shall check the identification card / access rights atleast once in a year for its usage and during termination or resignation of employees.

5.1.4 Visitor's entry and exit

a) The public entry will be under continuous surveillance through manned reception and CCTV at front office / reception area.

b) The visitor's entry and exit should be entered in the Visitor Register.

c) The front office receptionist / security staff requests the visitor to declare their personal assets such as Laptops / Tablets with serial number, Mobile devices, data card, storage devices, USB, etc., in Visitor Register.

d) The visitors should be accompanied with the reception staff until he / she is handed over to the concerned person / department.

e) The visitors shall not be entertained to meet the office staff without the permission of the Front Office / Reception within the office premises.

f) The visitor will be inspected on their belongings, checked for any photo capturing devices and valid ID proof. All visitors are provided with visitor card.

g) The meeting with the visitor shall take place in the conference room/meeting room or MD cabin as per need. The workplace shall strictly not be used for meeting with the visitor.

h) The visitor's equipment shall not be connected to the LAN or Broadband connections with or without permission. If so connected, necessary permissions will be obtained from CISO.

5.1.5 Securing Offices, rooms and facilities

5.1.5.1 Opening and closing – Office

a) The office keys will be under the custody of HR Manager/ Accounts department only. It is the responsibility of Admin personnel/ security to obtain the keys from HR Manager / Accounts department for opening and closing the office.

b) The office will be kept open for the regular housekeeping with the presence of Admin department personnel and appointed Security Agency.

c) The Master Keys of all the doors will be maintained by HR Department.

d) Respective Department / team members are issued keys of rooms / racks

/ cupboards and issuance records are maintained.

e) In case of holidays, no visitors / public entry is allowed inside the premises. Allowed only in case of office maintenance activities with the presence of respective department personnel such as IT, Admin and HRD.

f) Admin and HR departments ensure that no sensitive information such as telephone contact details of customers or employees are not readily accessible by the public includes visitors / contractors, etc.

5.1.5.2 Server room

a) The entry and exit of server room will be recorded in the server room log / register.

b) The SA and CISO are authorized to enter the server room for any official purpose. Other staffs are not permitted to the server room.

c) The window provision or openings will be locked permanently or closed with adequate provision at all the time.

d) The server room temperature shall be set within 18-24 degrees Celsius and SA shall monitor frequently.

e) The server room is equipped with applicable type of fire extinguisher.

f) The server room keys will be maintained with SA during office hours and kept in the IT desk lockable cabinet.

5.1.5.3 Protecting against external and environmental threats

Office premises are installed with adequate Fire Extinguishers and smoke detector. The Fire drills are conducted once a year and all fire extinguishers are refilled as per the due date.

5.1.5.4 Working in Secure areas

a) Admin staff ensures vacant secure areas / rooms are physically locked and periodically checked.

b) Employees are not permitted to enter with Electronics Gadgets such as CD, DVD, External Hard Disk or USB Drives within the Company premises. Employees permitted to bring smart phones, Tabs inside the premises after obtaining necessary authorization as detailed in Bring your own device Policy.

c) Admin Staff is held responsible to check the office premises during housekeeping or routine checks for any potential security threats.

5.1.5.5 Delivery and Loading areas

a) All external doors are secured and closed when not in use.

b) External personnel from agencies such as Courier / Supplier are allowed up to Front Office / Reception only.

c) Incoming materials and outgoing shipments are recorded in Inward / Outward Register with the concern personnel approval.

d) Incoming materials are inspected for potential threats before the material is moved from the delivery to point of use. Admin and SA are held response for Inspection.

e) Random checks of visitor's baggage are conducted at front office by the receptionist / security to ensure there is no unauthorized incoming / outgoing material without prior approval from management.

5.2 Equipment

5.2.1 Equipment and protection

a) Satwic has sited and protected the equipments to reduce the risk from environmental threats, hazards and opportunities for unauthorized access.

b) Access to equipment/s is restricted to respective departments such as to Admin, Operations, System Administrator and approved Vendors / AMC Service providers.

c) AMC service providers who attend the calls as per plan provide maintenance records to Admin & SA.

d) Information processing facilities handling operations data are protected to reduce the risk of information being viewed by unauthorized persons during their use.

e) Admin department ensures storage facilities for any assets are secured and locked to avoid unauthorized access.

f) Satwic has segregated eating and drinking area separately from Information Processing facility. All employees are required to follow the work place ethics of not eating and drinking.

g) Temperature and humidity indicator installed in Server room monitors the temperature and environmental conditions.

5.2.2 Supporting utilities

a) UPS and Airconditioners installed in Office premises are maintained by AMC Service provider. The breakdowns are recorded and reported to concerned service providers to attend the same.

b) In case of any electricity failures / cable fault caused within the Satwic office premises (internal), approved service provider will be intimated immediately and necessary action will be taken. In the issue is identified outside the Satwic premises the same will be reported to Building owner by Admin department.

5.2.3 Cabling Security

a) Office and Cabling Diagram is maintained by System Administrator.

b) Telecommunication cables such as Network wires carrying data or supporting information is protected and monitored by System Administrator.

c) Telephone gadgets including wire and instrument will be maintained by System Administrator.

d) Network cables are protected and concealed from unauthorized interception or damage, connections to each user is identified in network diagram which is maintained by System Administrator.

5.2.4 Equipment maintenance

a) Admin Department coordinates with the building owner to ensure water supply is stable inside the company. In case of any breakdown, admin reports to building owner for rectification.

b) Equipment/s such as UPS, Split Air conditioners and Fire Extinguishers available in office premises, maintenance are carried out based on the need by service provider. Records of maintenance are maintained by Admin.

c) All equipments are covered under Insurance Policies and adequate Preventive Maintenance Program. Insurance Policies are maintained by Finance Department.

5.2.5 Removal of Assets

a) Admin and System Administrator ensure that equipment, materials or software are not to be taken offsite without prior authorization.

b) HR ensures that employees are made aware of removal of assets without prior authorization through review meetings, trainings, ISMS Do’s and Don’ts displays / communication through mail and also spot checks verification.

c) Random checks verification process is carried out based on approvals from Department Heads authorization.

5.2.6 Security of equipment and assets off-premises

a) SA issues laptop's to employees on getting the approval from Department Head and updates the Asset List.

b) The equipment/s owned by Satwic are used on behalf of the Satwic only by the employees who will undergo authorization process.

c) Equipment/s such as Laptops, Tabs, Data cards, etc., provided by the company for official use are taken offsite are made aware of its protection such as:

- Lock the laptops / Tabs away out of sight when you are not using it.
- Always shutdown, log off or activate password protected screen saver before walking away from the machine.
- If the laptop is lost or stolen, notify immediately to SA, respective manager and MD.
- Do not loan your laptop or allow it to be used by others such as family and friends.
- Report any security incidents (Such as virus infections) promptly to the SA in order to minimize the damage.

5.2.7 Secure disposal or re-use of equipment

a) SA ensures that equipment/s containing storage media are verified that any sensitive data and licensed software are removed or securely overwritten prior to disposal or re-use of equipment.

b) After getting approvals from department heads, the storage media will be destroyed / deleted or overwritten using any suitable techniques. If not able to destroy / delete, the storage media will be dismantled and scrapped.

5.2.8 Unattended user equipment

a) Users are made aware about the security requirements through ISMS Do's and Dont's displayed for protection of unattended equipments and its implementation.

b) Lock the laptops away out of sight when you are not using it.

c) Log-off from application or network or activate password protected screen saver before walking away from the machine.

d) Switch off the printer, when not in Use.

e) Session time out or sleep mode gets activated after 15 minutes for all computers.

Human Resource Security Policy

1. Purpose:

To define, implement and maintain a documented policy for Human Resource security.

2. Definitions:

2.1. DY CISO – Deputy Chief Information Security Officer

2.2. SA – System Administrator

2.3. HR – Human Resources

2.4. ADM- Administration

3. Applicable ISO Clauses/ Controls:

A.7.1 Prior to Employment

A.7.2 During Employment

A.7.3 Termination and change of employment

A.8.1.4 Return of Assets

A.9.2.6 Removal or adjustment of access rights

4. Scope:

a) Background verification and screening of employees and contractors

b) Terms and conditions of employment

c) Disciplinary process

d) Training on information security and management responsibilities,

e) Termination or change of employment responsibilities

f) Protection and usage of assets,

g) Removal of Assets

5. Policy:

5.1 Prior to Employment

5.1.1 Background verification and screening

a) The candidates appeared for interview will be subjected to complete background verification prior to their employment.

b) The background verification includes verification of educational records, reference checks, criminal conviction records, and work experience with all the companies.

c) The verification comments will be recorded in the background verification sheet. Certain cases the verification certificates are obtained from the schools / colleges as required.

d) The third party verification agency shall be appointed upon the need basis. Primary verification of the candidate during screening process will be done by Recruitment Agencies / in-house recruitment team.

e) Background verification of prospective suppliers/ subcontractors/ vendors will be done by the respective departments.

1. HR Departments will conduct for Recruitment companies, Trainers, HR related statutory consultant, AMC Service providers, Housekeeping & Security personnel's;

2. Finance Department will conduct for Legal consultants / Auditors,.

f) Background Verification details such as experience in the industry, financials, reputation, previous supplies to other industries, customer feedback results, etc., are recorded in Supplier Registration Form.

5.1.2 Terms and Conditions of employment

a) All employees, suppliers, contractors and consultants will enter into a Confidentiality or Non-disclosure agreement with the company and oblige the terms and conditions mentioned therein.

b) The employee's appointment letter covers the aspects such as maintenance of confidential information with the company, disciplinary action, conflict of interest, termination or change of employment, return of information / assets etc.

5.2 During Employment

5.2.1 Management responsibilities

Satwic ensures that the employees, suppliers, contractors and consultants are briefed about their roles, responsibilities towards information security before access granted to confidential documents

/ records or information systems. The effectiveness is reviewed through internal audits, Supplier audits / mails correspondence, Management review meetings, etc.

5.2.2 Information Security awareness, education and training

a) All employees, suppliers, AMC Service providers, contractors and consultants (where relevant) are made aware of security policies, procedures and responsibilities before making them accountable for any tangible or intangible assets.

b) Refresher trainings shall be conducted upon the updates of policies, procedures and responsibilities.

c) The ISMS DO's and DONT's are displayed at prominent places for communication to all the employees for information security by HR.

d) All employees, suppliers, AMC Service providers, contractors and consultants (where relevant) should be made aware of information security incidents and report to the concerned Departmental Head / HR if any such incident occurs.

5.2.3 Disciplinary process

a) The Disciplinary process is documented in HR policy, Appointment letter and communicated during induction training program.

b) HR will take actions against employees who have committed Information Security Breach. In case of any security breach, management will be initiating actions without notice period.

5.3 Termination and change of Employment

5.3.1 Termination or change of employment responsibilities

The termination or change of employment is defined in Employees Appointment Letter, Confidentiality or Nondisclosure agreement, Purchase Order / Work order for Suppliers / Vendors / Contractors / Consultants.

5.4 Return of Assets

a) Head HR in consultation with respective tech lead and Information Security Officer Advice / discuss upon any termination action against employee, contractors or consultants in removing the access rights.

b) The assets shall be revoked within notice period from the date of resignation. In case of termination the assets will be revoked immediately or any period as decided by the Management and HR.

c) The access facility, identification cards, mobile phones and SIM Cards shall be revoked at the time of relieving without any delays.

d) The identification cards issued to contractors, suppliers, vendors, AMC Service providers, consultants are returned to receptionist / front office staff on the same day of issuance.

e) The access rights will be removed on obtaining the concurrence from the HR Manager / Accounts department. It is the responsibility of system admin to remove the access rights upon the concurrence.

5.5 Removal or adjustment of access rights

The access rights will be removed on obtaining the concurrence from the Departmental Heads. It is the responsibility of System Administrator to remove the access rights upon the concurrence for employees, suppliers, contractors, consultants and AMC service providers who have provided access to information systems.

IT Access Control Policy

1. Purpose:

Satwic has documented, implemented and maintained Access Control Policy applicable for IT controlled assets to

a) Limit access to information and information processing facilities

b) Ensure authorized user access and to prevent unauthorized access to systems and services

c) Make users accountable for safeguarding their authentication information.

d) Prevent unauthorized access to systems and applications.

2. Definitions:

2.1. CISO –Chief Information Security Officer

2.2. DY CISO- Deputy Chief Information Security Officer

2.3. SA – System Administrator

2.4. HRD – Human Resources Department

3. Applicable ISO Clauses/ Controls:

A.9 Access Control

A.9.1 Business requirements of access control

A.9.1.1 Access Control Policy

A.9.1.2 Access to networks and network services

A.9.2 User Access Management

A.9.2.1 User registration and de-registration

A.9.2.2 User access provisioning

A.9.2.3 Management of privileged access rights

A.9.2.4 Management of secret authentication information of users.

A.9.2.5 Review of user access rights.

A.9.2.6 Removal or adjustment of access rights

A.9.3 User responsibilities

A.9.3.1 Use of secret authentication information.

A.9.4 System and application access control

A.9.4.1 Information access restriction

A.9.4.2 Secure log-on procedures

A.9.4.3 Password management system

A.9.4.5 Access control to program source code

4. Scope:

This procedure covers access to server room, access during emergencies, internet / emails, software applications, printers / scanners, terminals / standalones, and review of access rights.

5. Policy:

5.1 Access Control

a) The access control addresses both physical as per Admin Access Control Policy and Logical as per IT Access Control Policy.

b) The access to the server room shall be restricted to all employees, contractors and consultants at any point of time, except to the authorized users.

c) Server Room shall be accessed by Contractors / Consultants / employees with the prior consent of System Administrator or CISO and the same is recorded in the Server room in & out Log / register.

d) Admin personnel and Security Staff (in case of emergency crisis) are allowed to enter the Server Room and the same is logged in server room register.

e) No temporary access w.r.t network provided to external parties unless it is approved by CISO for accessing Satwic Information systems.

f) The printer access shall be provided to all employees of Satwic and System admin will monitored for any un-attended printouts left on the printer for longer time.

g) The control of the scanner shall be with Finance and Admin Team only. Any need for scanning will be handed over to Finance department nominated personnel.

5.2 Access to networks and network services

5.2.1 Wireless

a) Wireless connectivity is provided to all employees working in Satwic premises.

b) In case of external parties, wireless connectivity will be provided based on confirmation received from CISO or Manager HR.

c) SA monitors the network and network services. Access to Portal will be provided based on the nature of work and need basis, after getting the approval from concerned Department Head / Tech lead.

d) In case if there is any change in access rights, the same should be approved by CISO.

e) Removal of Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, will be disabled or removed manually.

5.2.2 Local Area Network (LAN)

a) It will be the responsibility of System Admin to determine the need for installation, operation, and management of all various Local Area Network deployments.

b) Network is pooled independently for teams and access of information within the teams is restricted to only concerned personnel.

c) Network cabling diagram indicates the current network infrastructure.

d) System Admin shall authorize the need for access by users through LAN.

e) Users / staff may not deploy access points or extend the coverage without the written consent of ISO.

f) In case of any significant issues, usage shall be limited or ceased.

g) All access to wireless network must be authenticated using login account and password.

5.2.3 Internet / email usage

a) Internet and email usage shall be used by employees for the business and work only.

b) All data transmitted through email / internet is the property of Satwic and bounded with laws in case of any unauthorized copying or misuse.

c) The email facility shall be used in a lawful, professional and ethical manner.

d) Employee shall communicate with department head during his long leave or vacation and handover the password for any immediate action on emails.

e) The department head shall advice the CISO / SA for the auto reply message with appropriate contact information.

f) Any information that is marked as proprietary, confidential shall not be sent outside company through email by any means. Unauthorized intentional or unintentional of such material shall result in severe disciplinary action with penalties or both.

g) The password shall not be shared within groups or out of groups for any purpose.

5.3 User registration and de-registration

a) New email id will be created by the SA based on Email / Application received for Email ID creation from HR Department. Same will be share to new users to their personal email ID. The email facility shall be created for Satwic employee’s only.

b) Provision of internet facility is limited for the employees. Employees at managerial position shall be provided with data card for internet access.

c) Provision of email / internet for contractors or consultants, with or without permission shall be restricted.

d) Any new employee's joined Satwic, SA creates email ID and temporary password will be allocated and communicated to new employee through their personal email ID.

e) Concerned Department Head sends email for requesting SA for provide access rights to software applications, web ports, etc. Based on email approval, necessary access rights will be allocated for the users.

f) SA once in 6 months or any significant changes occur for hardware / Operating system / Software applications / data integrity issues, etc., reviews the users access rights in consultation with Tech lead and CISO.

g) Upon termination / resignation / user has been moved to other offices, de- registration will be done based on request received from concerned department representatives.

h) SA ensures that redundant user ID's are not issued to others or new employees.

5.4 User access provisioning

a) User access provisioning process is implemented to assign or revoke access rights granted to user ID's allocated by SA for all users.

b) Access rights granted with authorization details are maintained by SA.

c) SA verifies the levels of access rights granted to users to access information systems and services are in line with present jobs assigned in the organization.

d) SA reviews the user access rights once in 6 months or any significant changes occur such as users have changed their job roles, transferred to other facilities and termination as per the agreement.

5.5 Management of privileged access rights

a) The allocation and use of privileged access rights are restricted and controlled by SA.

b) The privileged access rights are provided on need-to-use basis for the users based on their job or functional roles. The privileged access rights request is to be approved by CISO.

c) SA records the privileges provided details in the access rights matrix. Privilege access rights are not granted by SA till authorization process is completed.

d) SA changes the Passwords for the User ID's and access rights are restricted for privileged users in case of change in functional role or employee resignation information received from HR.

5.6 Review of user access rights

SA reviews the access rights matrix as detailed in the above paragraphs. SA in consultation with CISO is held responsible and authorized to make changes in the privileges access rights or access rights matrix technically upon receiving any advice from concerned department representatives.

5.7 Removal or adjustment of access rights

a) SA will remove or adjust the access rights based on the request received from HRD or Tech Lead.

b) The access rights of external parties are removed upon termination of their employment, contract, and agreement or adjusted upon change.

c) System backup of the relieving person will be taken by SA as defined in Backup policy.

5.8 Information access restriction

a) Access to information and application system functions are restricted in with sl.No.5.1 of Access control policy. Restrictions to access will be provided based on individual business application requirements.

b) Access restriction includes isolating sensitive applications and data processed by the Departments.

5.9 Secure Log-on procedures

Access to Desktops / Laptops by the user shall be protected with passwords. It is the responsibility of the user to access their systems with the passwords. Logging on behalf shall not be entertained.

5.10 Password management

Password allocated for Laptops / Desktops and server are in line with Password Policy.

5.11 Access control to program source code

a) Operation team ensures the documents / source code processed is moved to project folders maintained on server. Project teams will upload the source code in the project folder.

b) For all IT assets, the access matrix is maintained by SA.

c) Regular backup is taken for the applications and executables as per Backup Policy.

Admin Access Control Policy

1. Purpose:

Satwic has documented, implemented and maintained Access Control Policy applicable for HR & Admin controlled assets

a) to limit access to information and information processing facilities

b) to ensure authorized user access and to prevent unauthorized access to systems and services

2. Definitions:

2.1. ISO –Information Security Officer

2.2. SA – System Administrator

2.3. HR – Human Resources

3. Applicable ISO Clauses/ Controls:

A.9 Access Control

A.9.1 Business requirements of access control

A.9.1.1 Access Control Policy

A.9.2 User Access Management

A.9.2.1 User registration and de-registration

A.9.2.3 Management of privileged access rights

A.9.2.6 Removal or adjustment of access rights

4. Scope:

Access provided to employees, temp staff, visitors/contractors/suppliers and monitoring access rights provided to HR & Admin Department staff.

5. Policy:

5.1 Access control

a) HR and Admin staff are allowed to access office building during office working hours and non-working hours for official purpose or in case of any emergency situations.

b) Access to auditors / consultants who are visiting on daily basis to Satwic premises shall be given by Security / Front Office Staff. The identification badges issued are recorded in Visitor Register.

c) Admin Department monitors regularly for the access provided to external service providers such as security staff, housekeeping staff, etc., who has an access to work areas. In case of long absenteeism or resignation, the cards will be handed over to Admin Department.

d) If any employee did not carry company ID, the same shall be reported to Administration. Temporary access card will be issued; the same has to return at the end of the day.

e) Any loss or damage of access cards shall be reported to Administration immediately without fail.

5.2 Access during emergencies

a) HR & Admin team shall have the control of office buildings during emergency situation.

b) Activities of police department / fire station or any source shall not take place without the presence of manager HR and CISO during emergency situations.

c) Manager HR is held responsible until the mitigation completes and further any litigations.

d) Employees and external parties such as contractors or consultants shall be informed and restricted for entry, during emergency situations.

e) All the Main doors shall be closed to prevent the entry of outsiders during emergency situations. Doors are provided with Access Control mechanism.

5.3 User registration and de-registration

a) Any new employee's joins, HR department forwards necessary details to

1) SA to create domain name and temporary password allocation.

2) Admin department for issuance of unique identification badge, Access card

/ Biometric detection details and Business cards (approval to be obtained from Manager HR / MD).

b) Employees working for HR & Admin department will be provided with privileged access rights such as Access to Social Networking websites, full software access, etc based on the business need and approval.

5.4 Removal or adjustment of access rights

a) In case of employee resignation / Termination / Transfer mail will be triggered from HR department to the SA, Admin and Finance department regarding the date of relieving of an employee.

b) HR department shall ensure relieving formalities to be completed with employee after receipt of ID card, Access Card and other assets used by employee.

c) Relieving employee must get a final clearance advice from HR, SA, Admin and Finance at the date of relieving.

Internet & Email Security Policy

1. Purpose:

To define, implement and maintain a documented policy for internet and email security.

2. Definitions:

2.1. DY CISO – Deputy Chief Information Security Officer

2.2. SA – System Administrator

2.3. HR – Human Resources

3. Scope:

Applicable to all the Employees, contractors, service providers, AMC provider and consultants.

4. Policy:

4.1. Provision and removal of internet and email access

a) New email id will be created by the SA based on Email / Application received for Email ID creation from HR Department. The email facility shall be created for Satwic employee's only.

b) Provision of internet facility is limited for the employees.

c) Employees at shall be provided with data card for internet access as applicable.

d) Provision of email / internet for contractors or consultants, with or without permission shall be restricted.

e) Manager HR / CISO shall advice the SA for the removal of email facility.

4.2. Internet / email usage

a) Internet and email usage shall be used by employees for the business and work only.

b) All data transmitted through email / internet is the property of Satwic and bounded with laws in case of any unauthorized copying or misuse.

c) The email facility shall be used in a lawful, professional and ethical manner.

d) Employee shall communicate with department head during his long leave or vacation and handover the password for any immediate action on emails.

e) The department head shall advice the CISO / SA for the auto reply message with appropriate contact information.

f) Any information that is marked as proprietary, confidential shall not be sent outside company through email by any means. Unauthorized intentional or unintentional of such material shall result in severe disciplinary action with penalties or both.

g) The password shall not be shared within groups or out of groups for any purpose.

4.3. Illegal copying

a) Employees shall not illegally copy material protected under copyrights law or make materials available for others for copying.

b) Employees are responsible for complying with copyright law and other applicable licenses that may apply to software, files, graphics, documents, messages, or any material marked for copyrights and shall not send or wish to send with the provided facility.

4.4. Frivolous use

a) Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all employees connected to the network have responsibility to conserve the resources.

b) Employee shall not perform acts that waste computer resource or unfairly monopolize resources to the exclusion of others. These acts include not limited to, sending mass mailings or chain letters or otherwise creating unnecessary loads on network traffic associated with non-business related uses of email facility.

c) The email facility shall not be used for personal gain or personal commercial use by any employee.

d) Frivolous use of emails for transmitting non work related messages, pictures, jokes, programs etc., shall be strictly prohibited. The employees shall be made aware appropriate usage of emails.

4.5. Broadcast emails

Employees shall not broadcast emails to larger group outside the organization in any case.

4.6. Monitoring and enforcement of privacy

a) Employees shall have no expectation of privacy in anything they create, store, send or receive using email.

b) Employees expressly waive any right of privacy in anything they create, store, send or receive using email.

c) Satwic has the right to monitor and log any or all aspects of its email transactions including, but not limited to, monitoring and / or viewing all emails sent, received, stored, replied or forwarded and archived by employees.