



Information Security Policy

Document ID: TP-014-ISP

Version 3.0

Revision History

Version	Release Date	Prepared By	Reviewed By	Approved By	Sec. #	Summary of Changes
0.1	21-Jul-2023	InfoSec	GRC		-	First draft
1.0	26-Jul-2023	InfoSec	GRC		-	Initial Baselined document
1.1	18-Aug-2023	InfoSec	GRC		-	Multiple sections updated
2.0	18-Aug-2023	InfoSec	GRC	CISO	-	Baselined and Approved
2.1	12-Aug-2024	InfoSec	GRC		4.2.8 4.2.10 4.2.22	Updated Doc IDs for Sections Encryption Policy, Data Retention and Data Destruction Network Security
3.0	13-Aug-2024	Infosec	GRC	Chandra J		Baselined

Table of Contents

1	Introduction	4
2	Policy Objectives.....	5
3	Policy Scope	5
4	Policy Statement.....	5
4.1	Security Functions.....	5
4.1.1	Security Awareness Training and Education (SATE).....	5
4.1.2	Security Operations Centre (SOC)	6
4.1.3	Incident Response (IR).....	6
4.1.4	Security Engineering (SE).....	6
4.1.5	Offensive Security (OffSec).....	6
4.1.6	Identity Access Management (IAM) & Privilege Access Management (PAM).....	6
4.1.7	Network & Firewall Security	6
4.1.8	Security Architecture, and Design (SAD)	7
4.1.9	Cloud Security.....	7
4.2	Policies, Plans, and Processes.....	7
4.2.1	Awareness and Education	7
4.2.2	Malicious Software (Malware) Identification & Removal	7
4.2.3	Asset Inventory Management.....	7
4.2.4	User Access Management (UAM)	8
4.2.5	Password Management Policy	8
4.2.6	Acceptable Use Policy.....	8
4.2.7	Mobile Computing and Teleworking Policy.....	8
4.2.8	Encryption Policy	8
4.2.9	Data Classification	9
4.2.10	Data Retention and Data Destruction	9
4.2.11	Vulnerability Assessment & Patch Management (VAPM).....	9
4.2.12	Vulnerability Assessment & Penetration Testing (VAPT)	9
4.2.13	Reporting a Security Incident.....	9
4.2.14	Security Operations Centre (SOC) Process.....	9
4.2.15	Incident Response (IR) Plan.....	10
4.2.16	Data Loss Prevention (DLP).....	11
4.2.17	eDiscovery/Request for Monitoring (RFM)	11
4.2.18	Risk Management.....	11
4.2.19	Security Hardening	11
4.2.20	Endpoint Security	12
4.2.21	Server Security.....	12
4.2.22	Network Security	12
4.2.23	Cloud Security.....	12
4.2.24	Software validation process	13
4.2.25	Change Management Process	13
4.2.26	Backup & Restoration Policy.....	13
4.2.27	Compliance and Audit Process	13
4.2.28	Vendor Management Policy.....	13
5	Policy Exemptions and Exceptions	13
6	Policy Enforcement.....	13
6.1	Policy Violation	14
6.2	Disciplinary Process.....	14
7	Policy Review Cycle	15
8	RACI Matrix.....	15
9	References.....	15
10	Glossary of Terms.....	15

1 Introduction

Techwave is essentially an IT & Engineering Services provider and uses various [Information Systems](#) for providing services to its customers. In doing so, Techwave may store and process confidential and personal information of relevant interested parties, and information relating to its own operations. Consequently, Techwave as an organisation is obligated by local law enforcement agencies, statutory/regulatory bodies and by contractual agreements to ensure Confidentiality, Integrity, and Availability ([CIA](#)) of data in conformance with Data Protection Standards and Governance requirements, while functioning in an efficient manner to provide products and services to customers.

Information systems is inherently prone to [Cyberthreats](#). Dependence on these systems makes any organization vulnerable requiring access controls and other measures to secure them. The interconnecting of public and private networks and sharing of [information](#) resources increase the difficulty of achieving access [control](#). The trend to distributed computing has weakened the effectiveness of central, specialist control.

Moreover, many information systems have not been originally designed to be secure. The security that can be achieved through technical means is limited and should be supported by appropriate management policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. [Information security](#) management needs, as a minimum, participation by all relevant [interested parties](#).

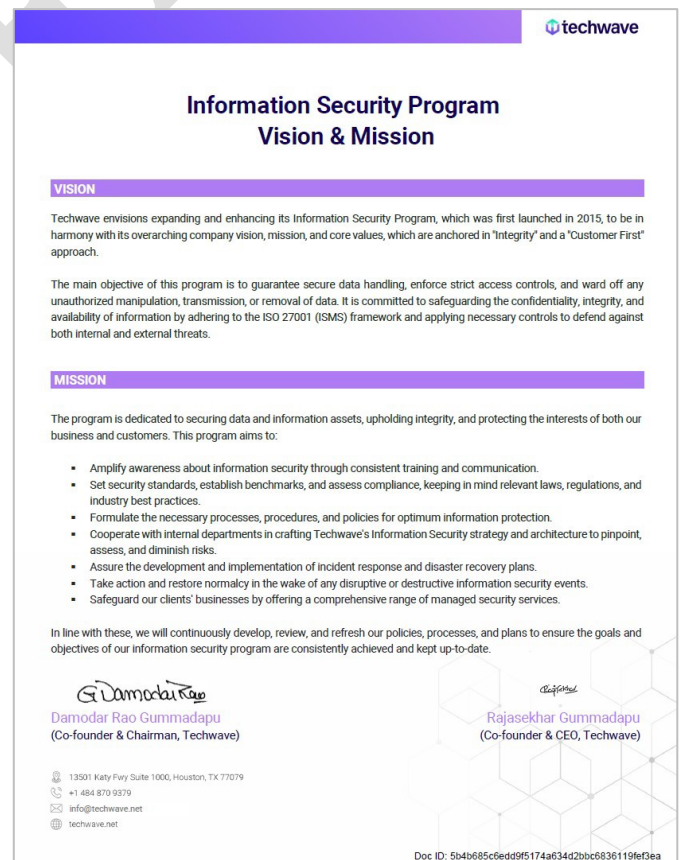
This Information Security [policy](#) provides a [guideline](#) to protect Information related to Techwave business(es), relevant interested parties, clients, previous and current engagements, product/service release plans, internal confidential documents, any copyright information, and information categorized as company secrets or Personally Identifiable Information ([PII](#)).

This is a Program Policy for Techwave's Information Security Program and aligns with **Techwave's Information Security Vision & Mission statement** to protect information systems.

This policy sets the direction for Techwave's Information Security Program, and defines requirements based on [ISO 27001](#) ([ISMS](#)) standard and [NIST](#) Cyber Security Framework ([CSF](#)). It identifies, develops, implements, and maintains adequate, [risk](#) based, cost-effective solutions to protect all data created, collected, processed, stored, transmitted, disseminated, or disposed of by Techwave or its subsidiaries/suppliers/partners/ clients in any form or format.

This policy for all business reasons, replaces the previous Information Security policy and is approved by Techwave Leadership/Management and is supplemented by additional security policy documents, standards, processes, procedures, tools, and training that provide detailed guidelines / instructions / capabilities relating to specific security controls.

In case of any queries/concerns or, want to refer related/referred policies within this document, reach out to your Manager/[HRBP](#)/[InfoSec](#)/[Infra](#)/[QMS](#).



techwave

Information Security Program Vision & Mission

VISION

Techwave envisions expanding and enhancing its Information Security Program, which was first launched in 2015, to be in harmony with its overarching company vision, mission, and core values, which are anchored in "Integrity" and a "Customer First" approach.

The main objective of this program is to guarantee secure data handling, enforce strict access controls, and ward off any unauthorized manipulation, transmission, or removal of data. It is committed to safeguarding the confidentiality, integrity, and availability of information by adhering to the ISO 27001 (ISMS) framework and applying necessary controls to defend against both internal and external threats.

MISSION

The program is dedicated to securing data and information assets, upholding integrity, and protecting the interests of both our business and customers. This program aims to:

- Amplify awareness about information security through consistent training and communication.
- Set security standards, establish benchmarks, and assess compliance, keeping in mind relevant laws, regulations, and industry best practices.
- Formulate the necessary processes, procedures, and policies for optimum information protection.
- Cooperate with internal departments in crafting Techwave's Information Security strategy and architecture to pinpoint, assess, and diminish risks.
- Assure the development and implementation of incident response and disaster recovery plans.
- Take action and restore normalcy in the wake of any disruptive or destructive information security events.
- Safeguard our clients' businesses by offering a comprehensive range of managed security services.

In line with these, we will continuously develop, review, and refresh our policies, processes, and plans to ensure the goals and objectives of our information security program are consistently achieved and kept up-to-date.

Damodar Rao
Damodar Rao Gummadapu
(Co-founder & Chairman, Techwave)

Rajasekhar
Rajasekhar Gummadapu
(Co-founder & CEO, Techwave)

13501 Katy Freeway Suite 1000, Houston, TX 77079
+1 484 879 9579
info@techwave.net
techwave.net

Doc ID: 5b4b685c6edd9f5174a634d2b0c6836115fe3ea

2 Policy Objectives

This policy provides a definitive statement of information security policies to realise the below objectives.

- Acquaint all interested parties with information security risks and the expected ways to address these risks thus creating an information security aware culture within the Organization.
- Clarify responsibilities and duties of interested parties with respect to the protection of information systems.
- Enable interested parties to make appropriate decisions about information security.
- Coordinate the efforts of different groups within Techwave so that information resources are properly and consistently protected, regardless of their location, form, or supporting technologies.
- Maintain confidentiality, integrity, availability, and safety of Information systems.
- Manage risks related to information security, cybersecurity, and physical security.
- Drive [compliance](#) of information security and data privacy controls across all systems.
- Comply with legal, regulatory, and contractual requirements by implementing auditable controls.
- Avoid breaches from internal and external sources.

3 Policy Scope

This Information Security Policy outlines the framework for Management of Information Systems of Techwave by maintaining integrity of data and safeguarding interests of the business and more importantly our customers.

The Information Security Policy, Standards, Processes and Procedures apply to all interested parties, who have access to Techwave's information systems, working from Techwave offices or Remote Home/Client locations.

The Information Security Policy applies to all forms of data which include but is not limited to:

- Written/printed documents.
- Data stored/processed on information systems.
- Communications sent by Email, Post, Courier, fax, etc.,

4 Policy Statement

The policy governs all aspects of information systems, and all interested parties who have access to Techwave Information [assets](#) or processing facilities.

Security is ensured by the Information Security Organization, headed by CISO, and comprises of various core security teams (collectively called the InfoSec team or in short InfoSec) that closely work with other departments within Techwave and with Vendors/Partners/Consultants to perform several [security functions](#) in addition to crafting, maintaining, and implementing related policies, plans, and processes.

Please refer to "[Organization of Information Security](#)" (Document ID: SP-019-OIS) for Information Security Org structure and the roles and responsibilities of various functions within.

Being accountable, all Interested parties are required to ensure information is secured and used appropriately by authorized personnel only. To conform to this, they are required to adhere to specific policies for specific areas that ensure information security. These policies collectively form the building blocks of the information security policy. Non-conformity of any nature (minor or serious) will attract disciplinary action – Please refer to "[Disciplinary Process](#)".

4.1 Security Functions

4.1.1 Security Awareness Training and Education (SATE)

The SATE function provides Security Awareness trainings for new hires and periodic refresher trainings, conducts assessments on information security, identifies high-risk groups, works with BU's and loops back to the Security Engineering team for phishing campaigns and additional customized trainings, where deemed necessary.

4.1.2 Security Operations Centre ([SOC](#))

- The SOC function is responsible for safeguarding organization's information systems and ensuring the confidentiality, integrity, and availability of critical information.
- The SOC analysts continuously monitor all information systems to detect potential security breaches and malicious activities.
- This function collaborates closely with IT Support & Infra support team and, other InfoSec functions to ensure effective coordination and response to security incidents.

4.1.3 Incident Response ([IR](#))

- The Incident Response function is responsible for managing and coordinating the response to cybersecurity incidents.
- This function works to identify the root cause, eliminate the threat, and recover from security breaches and other incidents that may impact Techwave's Information Systems.

4.1.4 Security Engineering ([SE](#))

Security Engineering deals with the implementation of security measures based on the design and architecture.

- The SE team performs software validations, POC for security tools, configuring and deploying security solutions, setting up security policies, and integrating security features into applications and systems.
- Security engineering also includes ongoing monitoring, testing, and updating of security measures to adapt to evolving threats and vulnerabilities.

4.1.5 Offensive Security ([OffSec](#))

- Offensive security function identifies and addresses weaknesses in computer systems, networks, applications, and other digital assets before malicious attack vectors exploit them.
- It is a proactive approach that involves simulating attacks and exploiting vulnerabilities in a controlled environment.
- VAPT exercises (both Internal & External) are conducted using a variety of tools and techniques to mimic the tactics, techniques, and procedures (TTPs) used by actual attackers.

4.1.6 Identity Access Management ([IAM](#)) & Privilege Access Management ([PAM](#))

IAM and PAM function resides largely with Infra and IT support teams to manage access to users based on their roles and responsibilities to various resources, systems, applications, and data. Also, some teams manage their own applications to provide access to limited staff.

4.1.7 Network & Firewall Security

This function enforces network security policies to prevent unauthorized access to and from the enterprise network. Techwave implements high availability and failover mechanisms to ensure uninterrupted firewall services in case of hardware/software failures. These are implemented to monitor and control inbound and outbound traffic using firewall rules.

Next-Generation firewalls (NGFWs) are implemented to enable features such as intrusion prevention systems (IPS), application awareness, deep packet inspection, and sophisticated threat detection capabilities. The deep packet inspection and application layer filtering is done to identify and block malicious content within the network traffic and to disable unnecessary services/protocols to reduce the attack surface and minimize the risk of exploitation.

For remote access (e.g., VPN), Techwave ensures MFA to restrict access to authorized users only. VLANs (Virtual LANs) are used to isolate critical network devices from general user traffic to prevent unauthorized access and reduce the impact of potential compromises.

Also, default settings and passwords on all network devices, including routers, switches, access points and firewalls are changed and the firmware, software, and security definitions of network devices are kept up to date.

4.1.8 Security Architecture, and Design ([SAD](#))

SAD function involves in a comprehensive approach to developing and implementing secure information technology systems and networks by comprising various principles, methodologies, and best practices aimed at safeguarding the confidentiality, integrity, and availability of data and resources.

- Security Architecture - involves the design of the overall security framework by establishing how different components and technologies will work together to achieve security objectives.
- Security Design - focuses on creating individual security components and features within the overall architecture with the selection of specific security technologies and tools that will be used to protect the organization's assets.

4.1.9 Cloud Security

- Cloud security ensures the security, compliance, and overall protection of Techwave's cloud infrastructure and services.
- Cloud security team assesses Techwave's cloud architecture to identify potential security weaknesses, misconfigurations, and vulnerabilities.

4.2 Policies, Plans, and Processes

4.2.1 Awareness and Education

- Techwave is responsible for delivering relevant Information security trainings to staff for building awareness around cyber risks and influencing behaviour so that the likelihood of those risks is minimized.
- The methods used to create this awareness include IT Communication articles, InfoSec Office Communications, Employee Induction program and periodic awareness sessions.

4.2.2 Malicious Software ([Malware](#)) Identification & Removal

- Techwave will implement Antivirus (both Traditional & NextGen) and any other tools to monitor all [endpoint](#) devices and other computing devices in detecting and remove/quarantine any known malware or variants of it.
- This will also check any connected devices and alert the InfoSec team to take corrective actions where needed.
- The InfoSec team and/or IT Support team may seek possession of the device to investigate/contain/remediate.
- The IT support team on the direction of InfoSec, may completely format and/or replace the endpoint.
- The relevant interested parties are required to report without delays to IT/InfoSec about any anomalous behaviour or unusual activity on the endpoints.

4.2.3 Asset Inventory Management

- The IT support team will track and manage all Techwave assets. Tangible assets such as Laptops/desktops, printers, hardware equipment's/appliances and Intangible assets like software licenses, digital media etc are recorded in asset inventory.

- The IT team shall manage software licenses and subscriptions to comply with software agreements and optimize software usage.

4.2.4 User Access Management (UAM)

- The IT Support and Infra support teams manage user accounts throughout their entire lifecycle, from creation to termination. The team shall create access rights and permissions of individuals (users) on endpoints or infrastructure.
- Users will have appropriate level of access based on their roles and responsibilities in Techwave to various information systems.
- Revocation of access rights - In cases where users no longer require access to certain resources or when security concerns arise, the IT Support/Infra support team shall promptly revoke or modify the user access rights.

4.2.5 Password Management Policy

All interested parties of Techwave should follow the guidelines outlined in Password Policy to access any Techwave systems/applications etc., and [staff](#) working on any projects for clients are required to adhere to the Client's Information Security Policy and Password Management policy in addition to Techwave Password policy.

4.2.6 Acceptable Use Policy

Techwave has a clearly defined Acceptable Use policy for safeguarding Techwave information systems. All interested parties are required to adhere to **"Acceptable Use Policy"** (Document ID: TP-002-AUP) and **"Data Storage Device Usage Policy"** (Document ID: TP-013-DSDUP).

4.2.7 Mobile Computing and Teleworking Policy

- The policy is established to govern the use of mobile computing devices and the practice of teleworking (also known as remote work/work from home).
- It aims to provide guidelines on security and usage of mobile computing devices, protection of data, and employee well-being while allowing flexibility in where and how work is conducted.
- For adherence to this policy, please refer to **"Mobile Computing and Teleworking Policy"** (Document ID: TP-008-MTP).

4.2.8 Encryption Policy

Techwave implements the strongest possible data [encryption](#) algorithms for data at rest, and data in transit and data in the cloud to ensure the confidentiality and integrity of data, making it impossible to access/use by unauthorized individuals.

- Data at Rest: Full disk encryption to ensure that even if someone gains physical access to storage media/endpoints, the data remains encrypted and unreadable without the appropriate decryption key.
- Data in transit: Protocols like HTTPS (secure web browsing) and [SSL/TLS](#) (secure socket layer/transport layer security) encrypt data during transmission, ensuring the data remains protected from unauthorized interception.

Cloud Encryption: Techwave implements cloud native encryption and ensures access to this data is also through encryption protocols.

Adherence to this is ensured by Techwave Infra and IT Support teams and, is based on the documented **"Cryptography Guidelines and Controls"** (Document ID: SG-008-CGC).

Techwave IT has designed its **"Encryption Policy for endpoints"** (Document ID: TP-015-EPE) to protect sensitive data stored on devices such as laptops, desktops, and workstations. The policy ensures that data is securely encrypted to prevent unauthorized access in case of loss, theft, or breach.

Techwave Infra Support aims to protect sensitive data stored, processed, and transmitted within the Datacenter, documented in **"Encryption Policy for Datacenter IT Infrastructure"** (Document ID: TP-019-EPDI). It ensures that all data is encrypted according to industry standards, mitigating the risk of unauthorized access or data breaches.

4.2.9 Data Classification

- Techwave will follow the Data Classification, documented in **"Information Asset Classification & Labelling"** policy (Document ID: QP-043-IACL).
- The document owner is responsible to label the document with appropriate classification to ensure the confidential/sensitive data is not accidentally released to unauthorized persons.
- Default deemed classification for all documents is "Confidential".

4.2.10 Data Retention and Data Destruction

- Techwave will follow Data Retention and Data Destruction/disposal, documented in **"Data Retention"** policy (Document ID: TP-017-DRP).
- Data retained must be securely stored to protect against unauthorized access, breaches, and other security threats. Encryption and access controls must be used to secure data during the retention period.
- Data destruction methods should ensure that data cannot be recovered. This can include physical destruction (e.g., shredding, degaussing) or digital methods (e.g., overwriting, cryptographic erasure).

4.2.11 Vulnerability Assessment & Patch Management ([VAPM](#))

- The [Vulnerability](#) Assessment & Patch Management Process for Endpoints address how vulnerabilities will be identified, assessed, and remediated.
- Please refer **"Vulnerability Assessment & Patch Management Process for Endpoints"** (Document ID: SP-022-VAPM).
- Vulnerability assessment involves identifying, quantifying, and prioritizing security vulnerabilities across Techwave's endpoints by using automated tools, manual testing, or a combination of both.
- Patch Management process covers the regularly updating software, applications, and systems with the latest security patches and updates provided by software vendors using automated tools, manual process, or a combination of both.

4.2.12 Vulnerability Assessment & Penetration Testing ([VAPT](#))

- VAPT is a systematic process of identifying and quantifying vulnerabilities in Servers, Networks, Applications, and Cloud environment, etc.,
- Penetration testing process is a controlled and simulated attack on Techwave's critical assets to identify and exploit vulnerabilities actively.
- The process involves using automated tools and manual analysis to scan and evaluate the critical assets for known vulnerabilities and misconfigurations.

4.2.13 Reporting a Security Incident

- Information security management needs, as a minimum, participation by all interested parties of Techwave.
- A security incident must be reported to InfoSec team at the earliest. Failing to do so immediately may attract penalties. Please refer to the ["Policy Enforcement"](#) section.

4.2.14 Security Operations Centre ([SOC](#)) Process

The SOC constantly looks out for security events in Techwave Information systems using a centralized Security Incident and Event Management ([SIEM](#)) tool and/or other monitoring consoles/tools to effectively detect, analyse, triage, and escalate security incidents to the Incident Response (IR) team in a timely manner. Also, SOC acts on any security incidents reported by interested parties.

4.2.14.1 Security Incident Management Process

[Incident Management](#) (IM) Process is to be followed to effectively handle security breaches, cyberattacks, or other incidents that may compromise the confidentiality, integrity, or availability of Techwave's information assets. Below steps outline the Security Incident Management Process:

- Preparation: This stage focuses on the implementation of an incident response policy and function and the prevention of cybersecurity incidents.
- Detection and Analysis: This stage requires first identifying the type of threat that an organization is facing and determining whether or not it is an incident.
- Containment Eradication & Recovery: This stage of incident response includes isolating the threat and affected systems to make sure it does not proliferate.
- Post Incident Activity: This stage includes "Lessons Learned" and go over strategies for preserving the data collected and evidence gathered over the course of the meeting, and revisit preparation for future cybersecurity threats.

When an incident has an emergency-level outage or loss of service impacting multiple customers or can potentially cause reputational damages it will be considered as a major incident – A major incident is a trigger for Major Incident Management (MIM) Process which requires quick escalation of the incident for greater visibility and involvement of senior analysts, other technical recovery teams, and Management on [Technical Recovery Team](#) (TRT) calls and/or Management Team Meetings (MTMs).

The management/leadership team is empowered to involve consultants/third-party investigating agencies and initiate the Disaster Recovery process. After such incidents, a thorough Root Cause Analysis (RCA) and Post Incident Review (PIRs) is performed and documented as part of [Problem Management](#) (PM).

4.2.14.2 Security Incident Disaster Recovery (SIDR)

In the event of disaster due to security incident, Techwave infosec team will work with third-party security service providers and consultants to investigate, contain the incident, eradicate malicious content, remediate, stop/prevent exfiltration of data, block access to threat actors, assist in recovery operations, and recommend future course of actions.

- Where deemed necessary Techwave will involve [Third Party](#) for tests or investigation, and this may include transferring data for handling Security Cases or perform requisite testing.
- Reach out to Insurance provider and disclose all required details to cover for damages/loss of revenue incurred due to the security incident.

4.2.15 Incident Response (IR) Plan

The IR team follows a well-defined Incident Response Plan to mitigate the threats, contain the incident, minimize the impact, and restore the affected systems securely.

- The IR plan covers the process of conducting a comprehensive post-mortem analysis, by documenting all the actions taken during the incident response, identify lessons learned and areas of improvement to enhance the overall security posture.
- For adherence to this plan, please refer to **"Information Security - Incident Response Plan"** (Document ID: ST-001-IRP).

4.2.15.1 Testing the IR Plan

The InfoSec team will have to perform annual walkthroughs and tabletop testing of the plans to highlight any gaps in the processes.

4.2.15.2 Digital Forensics

[Digital Forensics](#) is part of IR Plan. The IR team will work collectively with third party digital forensics team to perform disk/device/mobile/malware forensics, reverse engineer, analyse logs/memory

dumps/network data, and other data to understand how the attack occurred, identify the attacker, and gather information for possible legal actions.

- The team documents the chain of custody for all collected evidence to maintain its admissibility in legal proceedings.

4.2.15.3 Chain of Custody (CoC)

The Chain of Custody policy ensures the importance of handling evidence (both digital and physical) with integrity, authenticity be verified and protected in line with Techwave's best practices.

- The CoC process refers to the documented chronological record of the custody, control, and handling of evidence collected during an investigation.
- The custody transfer form includes details about the evidence, the names and contact information of the individuals involved in the transfer, date/time of the transfer, and the purpose of the transfer.

4.2.15.4 Asset Forfeiture

- Asset Forfeiture refers to the legal process to seize and take control of assets (Techwave provided or Personal devices) believed to be connected to criminal or illegal activities.
- Forfeited personal devices are replaced with a brand-new device of same or higher capacity.

4.2.15.5 Third Party Testing and Investigations

- Where deemed necessary Techwave will involve Third Party for tests or investigation, and this may include transferring data for handling Security Cases or perform requisite testing.

4.2.16 Data Loss Prevention (DLP)

- The DLP process is designed to identify, monitor, and protect sensitive data to prevent it from being accessed, used, or distributed by unauthorized individuals or entities.
- It is to ensure the confidentiality, integrity, and availability of sensitive information within an organization.

4.2.17 eDiscovery/Request for Monitoring (RFM)

- Techwave HR department is at liberty to request InfoSec team to initiate the eDiscovery process to gather more evidence on relevant interested parties where there is prima facie evidence of wrongdoing/ill-intent.

4.2.18 Risk Management

- Risk management is the process of identifying, assessing, mitigating, and monitoring the risks associated with information systems.
- Risk assessments are conducted to understand the level of risk exposure and make informed decisions to mitigate and manage risks effectively.
- The Enterprise Risk Review meetings occurs once every month with relevant interested parties and all risks are logged in **"Risk Assessment and Risk Treatment Plan"** (Document ID: SR-071-RARTP).
- For detailed process on Risk assessment, please refer to **"Information Security Risk Analysis Process"** (Document ID: SP-009-ISRA).

4.2.19 Security Hardening

- Security hardening is the process of strengthening a system's defence's by minimizing vulnerabilities and potential attacks.
- Techwave disables the unnecessary services, ports, and features to reduce attack surface.
- Strong access controls and user authentication is enforced, limiting unauthorized access.

- Regularly security updates and patches are updated, ensuring known vulnerabilities are addressed.
- Security policies and configurations are tailored to Techwave's needs.
- System configurations are monitored and audited to maintain a secure state.

4.2.20 Endpoint Security

- Techwave protects endpoint devices from various cyber threats such as malware, ransomware, virus, data breaches and unauthorized access.
- Antivirus/Anti-malware security solutions are installed to scan and detect malicious software on the endpoint devices.
- All endpoints must be hardened to reduce the attack surface and enhance the security of the devices.
- Unnecessary services and features on the endpoints must be disabled or removed to reduce the potential attack vectors and minimize the risk of exploitation.
- The endpoint device operating system software and applications shall be applied with latest patches and security updates to ensure vulnerabilities are fixed.

4.2.21 Server Security

- Techwave must ensure all servers be configured, accessed, and maintained by enforcing security policies.
- Strong authentication mechanisms (2FA/MFA) be applied to control user access to servers, by enforcing the principle of least privilege to limit user permissions.
- All server's operating system, applications, and software's shall be up to date with the latest security patches and updates to address known vulnerabilities.
- Encrypt sensitive data at rest and in transit to protect it from unauthorized access.
- Secure communication protocols such as SSH (Secure Shell) must be used, instead of unencrypted protocols like Telnet.
- Remove or disable unnecessary services and software to minimize the attack surface.

4.2.22 Network Security

Network security enhances the security of computer networks and protect against various cyber threats.

- Techwave shall implement strong authentication methods (2FA/MFA) to ensure that only authorized users can access network resources.
- Use strong encryption and authentication methods for Wi-Fi networks and limit access to authorized devices only.
- Virtual Private networks (VPNs) are implemented for secure remote access to the network, especially for remote staff.
- Conduct third-party Vulnerability assessment and Penetration Testing on Critical network assets to identify vulnerabilities and weaknesses in the network.
- For more information about Network Security Policy and Security of network services, please refer to **"CMS_NetworkSecurity_Policy"** (Document ID: TP-016-NSP) and **"Information Communications Management"** procedure (Document ID: SP-003A-COM).

4.2.23 Cloud Security

- Cloud Security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion.
- Techwave manages and secures the Hybrid Cloud platforms for business purposes.
- Cloud security controls are implemented to protect cloud-based resources, data, and services from security threats and risks.

- Best practices are followed to reduce the risk of security breaches and ensure the confidentiality, integrity, and availability of the Cloud environments.

4.2.24 Software validation process

- Techwave performs software validations for all applications that are used internally or for clients to prevent spread of malicious code and/or exfiltration of data.
- All applications to be used by interested parties should adhere to the software validation process.
- Details of initiating a Software validation or checks within the software validation process are outlined in Software Validation Process document.

4.2.25 Change Management Process

- Techwave should follow the [Change Management](#) (CM) guidelines for managing changes related to information security as summarized in ISO 27001 for implementing new tools/create exceptions or exemptions.

4.2.26 Backup & Restoration Policy

- Techwave Infra support team to follow the Backup & Restoration Policy as documented in **"Techwave Infra Backup & Restoration policy"** (Document ID: TP-014-BRP).

4.2.27 Compliance and Audit Process

- Techwave's InfoSec policy aligns itself to local regulatory bodies and compliances.
- The Security program has auditable controls and complies with [ISO 27001](#) & [SOC 2 Type II](#) and, is open to both internal and external audits.
However, during the audit process, confidential information of Techwave cannot be transferred/displayed.

4.2.28 Vendor Management Policy

Where required Techwave is at privilege to follow the Vendor Management Policy for critical vendors and ensures Vendor [Risk assessment](#) for its suppliers where mandated by the customers.

Staff are required to get in touch with respective BU heads to understand where this is required/mandated and do a vendor [risk management](#) in conjunction with Techwave's [GRC](#) team.

5 Policy Exemptions and Exceptions

No individual, team, or group who is a part of the interested parties is fully exempt from this policy. However, exceptions to limited processes within this policy can be made subject to appropriate business justification and approvals.

Some examples:

1. A client may request laptops allocated to their project, to be provided with original configuration from OEM and not Techwave image due to business reasons which must be honoured as per the agreement of engagement.
2. A client may request NOT to install specific software on laptops allocated to their project and instead suggest alternative software due to their own regulatory, statutory, and legal obligations, or technical dependencies or fair-trade practices or avoid usage of their competitor's software.
3. A team requests large displays to be added to the exception list for screen lock policy.

6 Policy Enforcement

The policy is enforced on all Techwave users with immediate effect. Every user must **read, understand**, and **comply** with this policy and is responsible for ensuring the safety & security of Techwave Information

systems. For any queries about this policy and how it applies to you, please seek advice from your manager or, send an e-mail enquiry to InfoSec@techwave.net

InfoSec and IT Support will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and available monitoring tools. Also, if any employee notices users not complying with this policy, they are required to report such cases to the InfoSec team for investigation, otherwise shall be deemed non-compliant with this policy.

6.1 Policy Violation

Any non-compliance is a serious violation of this policy and is to be brought to the notice of InfoSec, who upon verification of facts will involve HR and Legal for further action.

Information security policy violations include but not limited to:

- Sharing passwords
- Unauthorized Access
- Data Breach
- Phishing
- Unauthorized Software Installation
- Data Leakage
- Negligence in Handling Data
- Violation of Data Classification policies
- Failure to report Security Incidents
- Unauthorized Remote Access
- Insider Threats
- Social Engineering
- Violation of Encryption Policy
- Violation of Acceptable Use policy
- Violation of Organization's COBC & Ethics
- Impersonating for any official communication

All Information Security Policy violations will be deemed as non-conformance with Techwave Organization's COBC & Ethics and/or other HR Policies.

6.2 Disciplinary Process

If determined that an employee/staff has breached information security policies, Techwave InfoSec team would conduct a thorough investigation to gather evidence related to breach or violation.

The evidence will be shared with the HR & Legal teams who will review and depending on the severity of the violation, may choose to issue a show cause notice to the employee or, set up a discussion with the employee/reporting manager/BU head as outlined below:

- The meetings must be setup by the HRBP between each individual employee, Reporting Manager, and themselves only.
 - Note: Reporting Manager may/may not have prior information on the case depending on any inputs that may have been sought from him/her by InfoSec during the investigation thus far.
- Alongside this, a separate meeting with assigned InfoSec analyst will be scheduled at the same time mentioning the employee's details who will be part of the discussion.
- The meeting will be started by HR and will be quickly joined by InfoSec analyst.
- HRBP will introduce people on the meeting and check on understanding of [COBC](#)/Ethics policy of the employee and pass it on to the InfoSec analyst.
- InfoSec analyst is supposed to check understanding of InfoSec policies and set context (to employee and his/her reporting manager) about the violation, sharing evidence.
- The HR should give the employee a chance to explain his/her actions/in-actions and ask any questions and may choose to agree or disagree.
- InfoSec related questions are to be answered by InfoSec analyst and any questions to HR/Manager should be answered by them, respectively.
- HR will take it forward by informing about any disciplinary action for non-compliance.
- InfoSec analyst will collect any devices if required from the employee as further evidence and follow Chain of Custody process for the collected devices.

As part of the disciplinary process, the HR department would gather and review all relevant evidence & facts and commensurate a potential disciplinary action. Disciplinary measures may include verbal or written warnings, termination, or legal actions if necessary. For more details, please refer to “**Procedure for initiating Disciplinary actions**” (Document ID: HP-002-DISA).

7 Policy Review Cycle

The Information Security Policy, with its supporting guidelines and procedures shall be reviewed at least annually/planned intervals by InfoSec team to ensure its continuing suitability, adequacy, and effectiveness.

CISO will also review and evaluate the policy in response to any changes affecting the basis of risk assessment such as infrastructure changes, technological changes, significant security incidents, new vulnerabilities, etc.,

Formal requests for changes will be raised for incorporation into the Information Security Policy, Processes, and Procedures.

8 RACI Matrix

The below RACI matrix applies to this process:

Responsible - Person(s) responsible for developing and implementing the process	InfoSec
Accountable - Person who has ultimate accountability and authority of the process	CISO
Consulted - Person(s) or groups to be consulted prior to final process implementation	QMS, GRC
Informed - Person(s) or groups to be informed after policy implementation or amendment.	All employees of Techwave

9 References

1. ISO Standards (https://en.wikipedia.org/wiki/List_of_ISO_standards)
2. ISO 27000 family (<https://www.iso.org/standard/iso-iec-27000-family>)
3. ISO 27001 (<https://www.iso.org/standard/27001>)
4. ISO 27002 (<https://www.iso.org/standard/75652.html>)
5. NIST Framework (<https://www.nist.gov/cyberframework>)
6. Information Security (https://en.wikipedia.org/wiki/Information_security)
7. GRC (https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance)
8. All Techwave HR & IT Policies (<https://onewave.techwave.net/#/module/core>)

10 Glossary of Terms

Term	Meaning
API	Application Programming Interface.
Asset	Anything that has value to the organization.
CIA	<p>Short for Confidentiality, Integrity, and Availability. A 1977 NIST publication introduced the CIA triad of confidentiality, integrity, and availability as a clear and simple way to describe key security goals.</p> <p>Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.</p> <p>Integrity: Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.</p> <p>Availability: The property that data or information is accessible and usable upon demand by an authorized person.</p>

CM	Short for Change Management, is a systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies.
COBC	Code of Business Conduct is the set of rules that details an organization's values, ethics, and beliefs alongside the rules that govern legal compliance.
CoC	Chain of Custody
Compliance	Compliance means conforming to a rule, such as a specification, policy, standard or law.
Control	Means of managing risk, including policies, procedures, guidelines, practices.
CSF	Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity risk.
Cyberthreat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Digital Forensics	Digital forensics is a branch of Cybersecurity focused on the recovery, investigation, examination, and analysis of data stored electronically often in relation to Cybercrimes.
DLP	Data Loss Prevention is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.
eDiscovery/RFM	Request for Monitoring
Encryption	Is a process of converting information or data into an encoded form to prevent unauthorized access.
Endpoint	An endpoint device is an internet-capable computer hardware devices on a TCP/IP network. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers etc.,
Security Functions	It defines one or more principles, resources, security operations and required capabilities.
GRC	Governance, Risk, Compliance – GRC function aims to synchronize information and activity across governance, and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities, and avoid wasteful overlaps. Email: GRC@techwave.net
Guideline	A description that clarifies what should be done and how.
HRBP	Human Resources Business Partner team - is an HR professional who can handle everything from hiring and benefits to compliance and employee relations. Email: globalhrteam@techwave.net
Legal	Legal teams align the organization to comply with internal policies, external regulations, and contractual obligations it may have with third parties—regarding security and data handling controls.
IAM	Identity Access Management
IM	Short for Incident Management. It is the process of identifying, managing, recording, and analysing the security threats and incidents related to cybersecurity in the real world.
InfoSec	Information security, sometimes shortened to InfoSec. The various core security teams within the Information Security Organization collectively are referred to as InfoSec. Email: InfoSec@techwave.net
Information	Any data or knowledge collected, processed, stored, managed, transferred, or disseminated by any method.
Information Security	Preservation of confidentiality, integrity, and availability of information.
Information systems	Integrated set of components for collecting, storing, and processing data and may be Physical/On-Prem/Cloud/Hybrid, which include but are not limited to: <ul style="list-style-type: none"> Data Both in physical form (like written or printed documents, books, boards, etc.,) and digital form. People All Interested parties Hardware <ul style="list-style-type: none"> - Computing & Peripheral Devices Servers, NAS, Desktops, Cloud instances, Virtual Machines, Laptops, Mobiles, Tablets, Gaming Consoles, Digital Cameras, Electronic Organizers, Voice Recorders, eReaders, OCR devices, Printers, Scanners, Copiers, Monitors, Projectors, Large Screens, Digital Signage displays, AI Devices, Wearables, IOT devices, etc., - Data storage media and devices Magnetic/Optical/Solid state devices, Storage/Repositories that are Online/Cloud, Pen/flash drives, etc., - Network devices Hubs, Switches, Access points, Routers, Gateways, Firewalls, Internet dongle, hotspot devices, etc., - Communication devices PSTN/POTS phones, Facsimile (Fax) devices, VoIP/SIP phones, GSM/CDMA cellular phones, Pagers, Video conferencing devices, etc.,

	Software Operating Systems, Office applications, OCR apps, Databases, Chat/Messenger apps, In-house applications, APIs, etc., Networks Access to Local area networks, Wide area networks, Communication networks, etc., Operations Processes & Procedures that enable the business
Infra	Short for Infrastructure, includes On-Prem, Cloud, and Network infrastructure
Infra Support	Refers to Managed Services team - Infrastructure Management Services and Cloud Management Services (IMS & CMS) Email: techwaveinfra.support@techwave.net
Interested parties	<p>Interested parties as per ISO/IEC 27001 (ISMS) includes:</p> <ul style="list-style-type: none"> • Employees (full time/part-time on Techwave payroll) • Contractors (directly contracted by Techwave or via third-party/staffing agencies) • Trainees/Interns • Consultants/Free lancers • Vendors/Suppliers • Partners • Staff deputed by Clients/Customers working on Techwave systems. <p>Interested parties also includes shareholders, government agencies, regulatory bodies, emergency services (police, ambulance, firefighters, etc.,) employees' families, media, publishers, service providers, etc.,</p>
IR	Incident Response
ISMS	Information Security Management Systems is a set of policies and procedures for systematically managing an organization's sensitive data. It a systematic approach for managing the information security of an organization.
ISO	International Organization for Standardization, develops and publishes International Standards.
ISO 27001	The ISO/IEC 27001 standard provides guidance for establishing, implementing, maintaining, and continually improving an information security management system.
IT Support	Refers to Information Technology Support team, which supports IT requirements for users. Email: ITsupport@techwave.net
Malware	Short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Malicious Software
NIST	National Institute of Standards and Technology – standards are based on best practices from several security documents, organizations, and publications, and are designed as a framework for federal agencies and programs requiring stringent security measures.
OCR	Optical Character Recognition
OffSec	Is termed as Offensive Security - is a proactive and adversarial approach to protecting computer systems, networks, and individuals from attacks.
Owner of Information	Is responsible for producing, collecting, and maintaining the authenticity, integrity, and accuracy of information.
PAM	Privileged Access Management
PII	Personally Identifiable Information is any information connected to a specific individual that can be used to uncover that individual's identity, such as their social security number, full name, or email address.
PM	Short for Problem Management. It focuses on preventing or minimizing the impact of one or more Incidents by finding the root cause.
Policy	Overall intention and direction as formally expressed by management.
PSTN/POTS	Public Switched Telephone Network/Plain Old Telephone Service PSTN or POTS refers to interconnected telecommunications network which allows subscribers at different places to communicate by voice over wire which is achieved by switching circuits mechanisms to enable an end-to-end connection. Also referred to as landline phones.
QMS	Quality Management System helps organizations manage and document quality processes that help ensure the products and services meet customer expectations and quality standards. Email: sepg@techwave.net
Risk	Combination of the probability of an event and its consequence.
Risk Assessment	Overall process of risk analysis and risk evaluation.
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk Management	Ongoing process of assessing, controlling, and mitigating the risk to Information systems and technologies.
SAD	Security Architecture & Design
SATE	Security Awareness Training & Education

SE	Security Engineering
SIDR	Security Incident Disaster Response
SIP	Short for Session Initiation Protocol (RFC 2543, 3261) The Session Initiation Protocol is a signalling protocol that enables the Voice Over Internet Protocol (VoIP) by defining the messages sent between endpoints and managing the actual elements of a call. SIP supports voice calls, video conferencing, instant messaging, and media distribution.
SIEM	Security Incident and Event Management - SIEM for short, is a solution that helps organizations detect, analyse, and respond to security threats before they harm business operations.
SOC	Short for Security Operations Centre A Security Operation Centre (SOC) is a centralized function employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analysing, and responding to cybersecurity incidents. The SOC acts like the hub or central command post, taking in telemetry from across the organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside.
SOC 2 Type II	System and Organization Controls (SOC), (also sometimes referred to as service organizations controls) as defined by the American Institute of Certified Public Accountants (AICPA). A SOC 2 Type II report is an internal controls report capturing how an organization safeguards customer data and how well those controls are operating.
SSL/TLS	Secure Socket Layer/Transport Layer Security
Staff	Employees, contractors, trainees, interns, consultants, and free lancers
Technical Recovery Team	It involves teams from various departments like IT, Infra (Servers/Networks/Cloud), InfoSec etc., for recovery and resolution of Major Incidents.
Third Party	Person or body that is recognized as being independent.
Threat	Potential cause of an unwanted incident, which may result in harm to a system.
UAM	User Access Management
VAPM	Vulnerability Assessment and Patch Management
VAPT	Vulnerability Assessment and Penetration Testing
VoIP	Voice over Internet Protocol
Vulnerability	Weakness of an asset that can be exploited by one or more threats.