Information Security Policies

DOCUMENT SUMMARY:

AUTHOR	ARUL ARCHANA A	
REVIEWED BY	JAGANNATHAN N	
CURRENT VERSION	2.1	
DATE OF CURRENT VERSION	04-06-2024	
DATE OF ORIGINAL VERSION	05-07-2023	
DOCUMENT TYPE	INFORMATION SECURITY POLICY	
DOCUMENT CIRCULATION	ALL TEAMS	
OWNER	CISO	
APPROVED BY	NAME:	SARAVANA KUMAR S
	DESIGNATION	CHIEF INFORMATION SECURITY OFFICER

REVISION HISTORY

Version	Revision	Issue Date	Changes
1.0		05-07-2023	First Draft
2.0		22-04-2024	Added controls use of privilege utility, Use of cryptography, Secure system architecture and engineering principles, Security testing in development and acceptance and password policy (Data masking) Information Security Project Management,
2.0	1	04-06-2024	In Document summary, Owner changed from MANAGER SECURITY OPERATIONS to CISO and Designation changed from MANAGER SECURITY OPERATIONS to CHIEF INFORMATION SECURITY OFFICER

Table of Contents

1.0 Fourd Information Security Policy

Fourd strives to protect the confidentiality, integrity, availability and privacy and its client's data by taking reasonable and appropriate steps to protect data and control its hardware and electronic media through the entire lifecycle, from initial receipt to final removal. Such control includes reasonably and appropriately protecting, accounting for, safely storing, backing up, and disposing of data, hardware, and electronic media in accordance with specific control procedures. Additional controls around physical and environmental security as well as account specific data protection policies are in place for added information control.

2.0 Purpose

The purpose for this policy is to highlight the terms that are defined with-in the policies and procedures with the intent of Information Security. A secure environment needs quality people, processes, and tools. If any of these requirements are substandard, the potential for a security breach can increase.

The following procedures cover each of these three areas:

2.1 People

An organization needs people who understand how to secure and perform day-to-day tasks for the services they administer.

2.2 Processes

Working in conjunction with an organization's security personnel, procedure should be developed to address the organization's security needs. When developing security policies and procedure, an organization must determine the appropriate balance between ease of use, management, and security, which can be achieved by completing a cost/benefit analysis. While not connecting a business to the Internet is more secure than being connected, almost every organization in today's business climate is connected to internet. These businesses have decided that the risk of not connecting outweighs the risks of connecting.

2.3 Tools

From a technical standpoint, security is best applied in layers, which are often referred to as a "defense-in-depth" strategy. The defense-in-depth strategy entails designing security at every layer of the architecture and minimizing the impact in the event a previous line of defense fails. In general, the defense-in-depth strategy maximizes security, although it adds to the management and coordination.

The following security procedures, provides the rules by which Fourd should operate while handling the Information and information processing facility. This procedure defines, what

involved personnel can and cannot do, and their roles and responsibilities. The Security procedures are designed to assist in the efficient operation. Failure to follow these procedures could lead to a breach of 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) or Availability (the property of being accessible and usable upon demand by an authorized entity).

Departure from these security procedures may lead to disciplinary action. Comprehensive, ongoing training and awareness programs shall be implemented to ensure that the Security Procedures are understood and adhered to. Regular internal and external audits will be conducted to ensure that the procedures are being followed.

3.0 Physical Control

3.1Physical and Environmental Security

The policy of Fourd is to ensure secure physical and environmental areas:

a) An organisation requires administrative, technological, and physical control to carry out business operations smoothly.

b) To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

c) Secure areas need to be protected by the appropriate entry controls to ensure only authorised personnel are allowed access.

3.2 Emergency Evacuation Policy

It is vital that if an emergency situation arises, it is handled effectively and with consideration for all emergencies.

To ensure compliance with National Regulations, the emergency and evacuation procedure must set out

- Instructions for what must be done in the event of an emergency
- An emergency floor plan

Emergency evacuation plans should be practiced and reviewed frequently. Evacuation plans must be displayed in prominent positions near each exit and in the children's environment with a compliant floor plan for ease of reference. The Approved Provider will ensure a risk assessment is conducted also identify potential emergencies that are affecting.

4.0 People Controls

4.1 Screening

Background verification checks on all candidates to become personal shall be carried out after joining the organization (for some cases, we do BGV before joining depends on the criticality of positions/ clients importance like data centre) and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

At the time of job applications verification checks should include the following at a bare minimum. This may be a mix of internal reference checks as well as external agency checks, if required on a case-to-case basis.

By default, HR Team will check very basic verification like Prior Employment and Cross verify Name with Aadhar with in 30days.

Below checks will be done against client request case to case basis.:

- For Campus Hires/Freshers:
    - Address Proof (Permanent & Current)
    - Identification Proof
    - Academic Check
    - Court Record Checks
- For Experienced Hires:
    - Employment check [all last employments]
    - Academic Check
    - Address (Permanent & Current)
    - Identification Proof
    - Court Record
- In case of third parties, similar screening process should be carried out. In case of contractors and temporary staff are provided through an agency the contract with the agency should clearly specify the agency's responsibility for screening and notification procedures they need to follow if screening has not been completed or if the results give cause of doubt or concern.
- If background checks are done through a third party, Fourd shall sign an agreement with SLAs/ terms, as well as Confidentiality and Non-Disclosure Agreements with the background verification agency/ service provider. Fourd shall also have a Right to Audit clause inserted, since the background verification agency comes across sensitive employees' data of Fourd.

This ensures all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

4.2 Terms and conditions of employment

Fourd has established employment contractual agreements that clearly state the responsibilities of personnel and the organization for information security.

References: Human Resources Policy

This ensures personnel understand their information security responsibilities for the roles for which they are considered.

4.3 During employment

4.3.1 Information security awareness, education, and training

Fourd has established a program to provide appropriate information security awareness, education, and training to personnel and relevant interested parties. The program includes regular updates of the organization's information security policy, other relevant policies, and procedures, as relevant for their job function. The effectiveness of the program is periodically assessed, and necessary improvements are made.

- Training programs should be conducted to make users aware of new security threats. Periodic training calendar should be maintained and tracked.
- Employees should also be issued alerts whenever required through emails by the IT Team.
- Users should be fully trained in the correct use of IT facilities like logon procedures, use of software packages, acceptable use etc.
- Training awareness programmes are to be documented and tracked, along with employee attendance sign-offs, feedback and evaluation mechanisms for effectiveness of the training.
- User training should include the following:
    - Reporting security incidents
    - Virus protection controls
    - Physical access
    - Internet usage
    - Email usage
    - Password usage
    - File sharing
    - Remote access
    - Removal of property

In addition to the regular InfoSec awareness, Fourd shall also conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on ISO policy and standards. Special focus shall be given to build awareness levels and skills of staff from non-technical disciplines. The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant

Terms and conditions of employment should include:

- Information security related roles and responsibilities.
- Action to be taken if the employee disregards security requirements
- Legal responsibilities and rights, e.g. regarding copyright laws
- Indemnification clause against any loss, claim or damage to a third party caused by the employee
- It should state that these responsibilities are extended outside the organisation's premises and outside normal working hours, e.g. in case of Work from Home / any other places.
- All employees shall sign Confidentiality / Non-Disclosure Agreements at the time of joining.

4.4 Disciplinary process

Fourd has implemented a disciplinary process that is formalized and communicated to all personnel and other relevant interested parties in case they commit an information security policy violation. The process includes appropriate actions that may be taken against violators, depending on the severity and frequency of the violation. The process is documented and made available to all personnel and other relevant interested parties, and regular training is provided to raise awareness of the process and its consequences.

- There should be a formal disciplinary process for employees who have committed a security breach subject to prior verification that a security breach has indeed occurred.
- The formal disciplinary process to ensure correct and fair treatment for employees who are suspected of committing breaches of security.
- The formal disciplinary process should provide for a response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.
- In serious cases of misconduct, the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

This ensures personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.

4.5 Termination or change of employment

4.5.1 Responsibilities after termination or change of employment

Fourd has implemented the control measure where information security responsibilities and duties that remain valid after termination or change of employment have been defined, enforced and communicated to relevant personnel and other interested parties.

- The communication of termination responsibilities should include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment continuing for a defined period after the end of the employee's, contractor's or third-party user's employment.
- The Human Resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the security aspects of the relevant procedures.

4.5.1.1 Absconding cases

- An employee habitually absents without prior permission/sanctioned leave or absent without authorization for more than 03 consecutive days or who overstays sanctioned leave without a valid explanation, will render herself/himself liable for disciplinary action. If the employee is not reachable in such cases, it will be considered as Employee Absconds and following procedure will be followed.
  - Show Cause Notice (SCN) will be issued to the employee for the continuous absence (wherever required); if he/she fails to respond within turnaround time, employment shall stand terminated. TAT will be 2 business days. SCN will be issued via mail/ letter to their current address via speed delivery.
  - Date of termination will be the turnaround date of SCN
  - It is Manager's responsibility to inform the HR Team about continuous (if more than 3 consecutive days) absenteeism of employee
  - Employee will not be eligible for any encashment and service certificate from company. Only the salary will be credited against the total number of days worked during the month
  - The salary is recovered if the company assets are due with absconded employees
  - If the employee wants to rejoin after long absenteeism, he/she has to provide the explanation to HR and reporting manager in writing. If there is any discrepancy found in the explanation, management has the right to intervene and investigate.
  - Rejoining will be considered on case-to-case basis

4.5.1.2 Legal/Official procedures

- If the employee absents for more than 03 days without notification, manager will have to notify the HR Team. In turn HR will notify the IT Team to pause the Mail and Slack accesses.
- Post SCN turnaround time Mail and communication/ application accesses will be revoked, and company will try to reach the employee in all possible ways (Personal contact no; Emergency contact no)

- If above possible ways don't help; Office Assistant will be sent to check their current address. These tries will be made to retrieve the given assets as per the Asset Handover form signed during the time of joining.
- If none of the above works, company can send a legal notice (wherever required). If the absconder doesn't respond then the employer can file a civil suit in case the absconder has pending loans and advances, pre-paid dues, company devices etc.
- If the employee absconds from job during the notice period, then employee may have to pay the remainder of the salary for the non-serving notice period.

Absconding from a company is a crime and it is dealt with under section 82 of the Code of Criminal Procedure.

This protects the organization's interests as part of the process of changing or terminating employment or contracts.

5.0 Other aspects of Human resources security

5.1 Confidentiality or non-disclosure agreements

Fourd has identified and documented confidentiality or non-disclosure agreements that reflect the organization's needs for the protection of information. These agreements are regularly reviewed and signed by personnel and other relevant interested parties.

- Employees/ contractors/ consultants' work involving access to organizational information processing facilities should be based on formal contract specifying compliance with all information security controls through confidentiality or non-disclosure agreements
- Human resource shall ensure that Information security undertaking and confidentiality agreements are signed by all employees and contractors working for Fourd

Confidentiality or non-disclosure agreements, along with terms of employment and inductions shall include or take into consideration:

1. General policy on information security - i.e., the Third-party is bound by the principles of Fourd's Information Security policy.
2. Notice, notification and other conditions for termination of contracts.
3. The respective liabilities of the parties to the agreement.
4. Responsibilities regarding hardware and software installation and maintenance.
5. Responsibilities with respect to legal matters e.g. data protection, copyright legislation.
6. Restrictions on copying and disclosing information.
7. Procedures regarding protection of assets.
8. Measures to ensure the return and processing of information and other assets at the end of the contract or employment.
9. The authorisation process for user access.
10. The right to monitor and revoke user access.
11. Permitted access methods and the control and use of user identifiers and passwords.
12. Measures to provide protection against the spread of computer viruses.

13. Any required physical protection measures.
14. User training in methods, procedures and security.
15. Arrangements and responsibilities for reporting and investigating security incidents.
16. Mechanisms to ensure that security measures are followed.

- Each employee shall sign the Confidentiality and Non-Disclosure agreements, which shall be kept in a file by the HR team or documented in the HRMS workflow.
- Confidentiality/ Non-Disclosure agreements shall also have a clause for continuing obligations to maintain the confidentiality post-employment termination or exit.
- Third-party employees are responsible for immediately informing the manager responsible for the contract, of any security breaches, including unauthorized access to or compromise of the data or information technology resources. However, any employee who is aware of security violations by vendors shall also report them to the concerned information owner as well as security administrator.

This maintains confidentiality of information accessible by personnel or external parties.

5.2 Remote working

Remote working that works

To ensure that employee performance will not suffer in remote work arrangements, we advise our remote employees to:

Choose a quiet and distraction-free working space.
Have an internet connection that's adequate for their job.
Dedicate their full attention to their job duties during working hours.
Adhere to break and attendance schedules agreed upon with their manager.
Ensure their schedules overlap with those of their team members for as long as is necessary to complete their job duties effectively.
Team members and managers should determine long-term and short-term goals. They should frequently meet (either online or in-person when possible) to discuss progress and results.
Compliance with Policies

Our remote employees must follow our company's policies like their office-based colleagues. Examples of policies that all employees should abide by are:

- Human Resource
- ISMS Policies and Procedures
- Attendance and Leave
- Social Media/ Acceptable Usage
- Confidentiality and Data Protection
- Code of Conduct and Business Ethics by HR
- Disciplinary Process, Anti-Discrimination
- Dress Code when meeting virtually with customers or partners during video conferencing

Equipment

Where applicable, we will provide our remote employees with equipment that is essential to their job duties. We will install CISCO VPN with MFA and company-required software when employees receive their equipment or work from their own devices, as applicable. We will not provide secondary equipment (e.g. printers and screens.)

Any equipment or licensed software/ application that we provide access to is company property. Employees must keep it safe and avoid any misuse.

For client connectivity, we will use their VPN connectivity or Remote tools (E.g., Any desk, Team viewer, Webex)

Specifically, employees must:

Keep their equipment password protected.
Store equipment in a safe and clean space when not in use.
Follow all data encryption, protection standards and settings.
Refrain from downloading suspicious, unauthorized or illegal software.

5.3 Information security event reporting

Fourd has provided a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

5.3.1 Reporting information security events

Fourd has provided a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

Reporting information security events

- Whenever an IT security incident occurs, the ISSO / System Administrator / ISSM should be informed.
- Reporting of any such Incidents based on suspicion or proof can be directly done via email or a tool. All such reports need to be investigated and responded to within a pre-agreed time period.
- Technical Head / System Administrator should maintain the record of IT security incidents. ISSM should periodically analyse the detailed record of reported incidents and report the same to ISSC.
- A procedure should be formulated for reporting an incident.
- Users shall be made aware of to whom to report an incident as per Incident Management Policy and Procedures

5.3.2 Reporting information security weaknesses

- Technical Head should initiate necessary action in case of any security weakness reported.
- Users should not in any circumstances attempt to prove a suspected weakness.
- Testing weaknesses might be interpreted as a potential misuse of the system.

This supports timely, consistent and effective reporting of information security events that can be identified by personnel.

6.0 Internal Organization of Information security

6.1 Information Security roles and responsibilities

Fourd has defined and allocated information security roles and responsibilities according to the organization's needs. The roles and responsibilities have been documented and communicated to all relevant personnel to ensure that everyone understands their individual and collective responsibilities in maintaining information security and protecting the organization's assets. The roles and responsibilities are regularly reviewed and updated to ensure their relevance and alignment with the organization's evolving needs.

a) Security roles and responsibilities of employees, contractors, and third-party users shall be defined and documented in accordance with Fourd's information security policy.

b) Security roles and responsibilities: Employees shall be made aware of their information security roles and responsibilities.

Refer CL-5.1- Information Security Organisation, Roles and Responsibilities.

6.2 Segregation of Duties

a) Fourd implements a system to segregate conflicting duties and conflicting areas of responsibility to minimize the risk of fraud, errors, and unauthorized access to its systems and data. Roles and responsibilities have been defined, documented, and communicated to all relevant personnel.

b) Regular reviews are conducted to ensure that segregation of duties is effectively maintained, and conflicts of interest are avoided. This reduces the risk of fraud, error and bypassing of information security controls.

c) Information security roles defined as per this manual shall not be overlapping. Employee duties shall be separated to guard against negligent or deliberate system misuse of data and services.

Fourd shall ensure that the followed roles are all distinctly segregated.

- maker-checker and delineation for initiation, approval and execution of changes
- maker-checker for access provisioning (request, approve and execution)
- using and administering third party applications and systems;
- Security management and security audit
- There must be compensating controls to ensure integrity and security where segregation is not feasible.
- No single person should be given single responsibility in such a way that no detection can be done in case of frauds, unauthorized access. The initiation of an event should be separated from its authorization. Following controls can be considered:
- Segregate activities which require involvement in order to defraud. For example, raising a purchase order and verifying the goods have been received.
- In case of any danger of collusion, controls should be revised so that two or more people are involved, thereby lowering the possibility of any kind of fraud.
- The design and access control mechanisms in software should also ensure segregation of duties.

6.3 Management Responsibilities

Fourd requires all personnel to apply information security in accordance with the established information security policy, other relevant policies, and processes of the organization. This ensures the protection of the organization's assets, stakeholders, and reputation. Management shall regularly monitor compliance with these policies and procedures to mitigate the risk of security incidents and ensure the confidentiality, integrity, and availability of its systems and data.

This ensures management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

Management shall support the implementation of information security policies and practices by:

a) Supporting and encouraging employees to adhere to information security policies.

b) Ensuring that Information security roles and responsibilities shall be reviewed when staffing or restructuring public service or contract positions, or when implementing new, or significant changes to, information systems.

c) annually reviewing and validating information security roles and responsibilities in job descriptions, standing offers, contracts and information usage agreements.

d) Ensuring that all users are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems.

e) Ensuring that all users are motivated to fulfil the security policies of the organisation.

f) Management shall ensure that the employees, contractors and third-party users conform to the terms and conditions of their employment / agreement.

g) ensuring that all employees with information security responsibilities continue to have appropriate skills and qualifications.

h) HR shall obtain a sign off on Information Security induction for new joiners confirming that they have understood the roles and responsibilities for information security and safeguards, as part of the management initiative for information security.

7.0 External Contacts

7.1 Contact with authorities

Fourd has established and maintains contact with relevant authorities to ensure that it stays abreast of the latest security threats and risks. The organization regularly shares information and collaborates with relevant authorities to develop effective strategies and responses to potential security incidents. By maintaining strong relationships with relevant authorities, Fourd is able to enhance its overall security posture and protect its assets, stakeholders, and reputation.

Appropriate contacts with authorities (utilities, law enforcement, emergency services, electricity suppliers and health and safety, e.g., fire departments, telecommunication providers and water suppliers), regulatory and supervisory bodies and mode of contact shall be maintained by ISM to:

a) Take proper advice in the event of security incident.

b) Exchange the latest security information.

c) Be a member of security groups and industry Groups

A list of such persons/ organizations/ authorities as well as the person responsible for the same shall be kept available with the organization.

7.2 Contact with special interest groups

Fourd has established and maintains contact with special interest groups, specialist security forums, and professional associations to stay up-to-date on the latest security trends, technologies, and best practices.

1. The organization shall participate in relevant events, workshops, and conferences to share knowledge and learn from industry peers. By engaging with these groups and associations, Fourd is able to enhance its expertise, stay ahead of emerging threats, and continuously improve its information security program.

2. ISSM should be the focal point for consolidating the in-house experience and expertise on information security.
3. ISSM should also take inputs from Internal Audit Department.
4. ISSM should obtain specific information security advice from external consultants when required.
5. The organization is to collate and collect the experience certificates, qualification credentials, attendance records for webinars, seminars on InfoSec and also stay appraised on the security trends through subscriptions to journals, newsletters.
6. Information security advice is also obtained from vendors, legal advisors, and technical experts on security matters to maximize the effectiveness of the ISMS.
7. Information security specialists shall maintain their knowledge of information security industry trends, best practices, new technologies, and threats or vulnerabilities by:
8. Participating in information exchange forums regarding best practices, industry standards development, new technologies, threats, vulnerabilities, early notice of potential attacks, and advisories;
9. Maintaining and improving knowledge regarding information security best practices; and
10. Creating a support network of other security specialists.

This ensures appropriate flow of information takes place with respect to information security.

8.0 Other aspects of Information security

8.1 Threat Intelligence

Fourd collects and analyzes information relating to information security threats to produce threat intelligence. This includes monitoring internal and external sources for indicators of compromise and staying up-to-date on the latest threat intelligence reports. The threat intelligence is used to proactively identify and respond to potential security threats, and to continuously improve the organization's security posture. Regular reviews are conducted to ensure that the threat intelligence is up-to-date, relevant, and aligned with the organization's objectives.

a) The collection, processing and reporting of threat intelligence shall be vital to Fourd's ability to assess risk and react to the threats it faces to its information security.

b) Fourd shall ensure its commitment to ensuring that effective methods are employed to ensure the accuracy, completeness and timeliness of the threat intelligence it uses.

c) The process shall set out the major steps involved in collecting and processing intelligence about threats at the strategic, tactical and operational levels.

d) Threat intelligence control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Fourd's assets.

e) Threat intelligence shall be gathered and reported at three levels: strategic, tactical and operational.

Threat intelligence levels description

A. Strategic Focused on the collection and analysis of high-level information regarding groups of attackers, their motivation, typical targets, types of attack and current levels of activity.

B. Tactical Concerned with specific attackers or types of attackers and the tactics, techniques, and procedures (TTPs) that they are currently using to gain access to systems or otherwise pose a threat to our organization.

C. Operational Relating to specific and potentially ongoing attacks, including indicators of compromise (IOCs) which may allow us to identify cases where we have suffered a breach.

Clear objectives shall be defined for threat intelligence in general and for the specific topics for which information is to be collected and analysed. These objectives shall consider the context of the organization, in terms of our industry, locations, technology and interested parties.

The IT and Information Security departments are responsible for performing threat intelligence across Fourd through sources like vulnerability scanning and threat intel data from vendors and shall also communicate on the threats to the organization or relevant teams through suitable channels.

Fourd shall document and assess its internal and external sources for threat intelligence and document the same as part of this policy.

Fourd shall detail how it carries out threat information collection, processing and analysis.

Fourd shall explore the usage of tools for threat intelligence and AlienVault SIEM or OTX pulse to ensure appropriate prevention or mitigation action for threats and vulnerabilities.

This provides awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

a) Collect the log after CISO approval.
b) Verify external source and collect information from Cert-in, NIST, CISA, OTX also referring latest CVE and if it is relevant and Required based on the asset, CISO will forward to Team, we will take action follow change management process
c) CVEs are verified from MITRE framework to find new threat and attacks.

8.2 Information Security in Project Management

a) Fourd has integrated information security into its project management processes, ensuring that all projects undergo security assessments and reviews to identify and mitigate potential risks and vulnerabilities.

b) This integration includes processes that cover areas such as access control, data classification, encryption, vulnerability management, and incident response.

c) Regular security awareness training is required for all project stakeholders, and a team of information security experts works closely with project managers to address security concerns throughout the project lifecycle.

Further to the above, Fourd shall ensure that:

a) Information security objectives shall be included in project objectives.

b) An information Security Threat and Risk Assessment shall be conducted at an early stage of the project to identify necessary controls.

c) Information security implications shall be reviewed regularly in all projects.

d) Responsibilities for information security shall be defined and allocated to specified roles defined in projects.

e) The Information Owner shall enquire that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures.

f) Change control processes shall be enforced to identify and document modifications or changes which may compromise security controls or introduce security weaknesses in projects.

g) Owners shall ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. Prior to implementation, information systems must be assessed to verify the adequacy of, and document the details of, the security controls used, by completing a security certification.

This ongoing integration of security into the project lifecycle enables Fourd to confidently deliver secure projects that protect its sensitive information and assets.

9.0 Information assets

9.1 Inventory of information and other associated assets

Fourd has established and maintains the inventory of information and other associated assets, including owners. The inventory is regularly updated to ensure that it accurately reflects the organization's current assets and their ownership. This enables the organization to manage its assets effectively, allocate resources appropriately, and prioritize its

information security efforts based on the criticality and sensitivity of the assets. The inventory is also used to support other information security processes, such as risk assessments, incident management, and access controls.

a) All major information and IT assets shall be identified and inventoried.

b) All computer equipment should be labelled and recorded. An inventory of information assets should be maintained, including:

   a. Software assets (including application software, system software, development tools and utilities)

   b. Physical assets (including computer and communications equipment, media, specialist technical equipment)

   c. Cloud assets/ instances list

c) The inventory of all IT assets - computer systems / printers / computer media / licensed software shall be maintained and tracked by IT Team manually or through asset management tool.

d) Asset criticality needs to be recorded against all assets and assets categories.

9.2 Labelling of Information

- Fourd has developed and implemented an appropriate set of processes for information labelling in accordance with its information classification scheme. These procedures ensure that all information is labelled with the appropriate classification level based on its confidentiality, integrity, and availability requirements. The labelling process is integrated into the organization's information management processes to ensure that it is consistent and effective.
- Regular training is provided to all relevant personnel to ensure that they understand the importance of information and asset labelling and how to apply the procedures correctly.
- The effectiveness of the information labelling procedures is regularly reviewed and updated as necessary to ensure that they remain appropriate and effective.

Physical labels (unique identification number, serial number) should be used for labelling the physical assets (desktops, laptops, servers, networking devices etc.). Labelling should be visible with a unique serial number which shall identify the equipment in a fixed asset and/or inventory register / system

Refer : (A5.37 Documented operating procedures- 3.7.8 -Information classification)

9.3 Information Transfer

Fourd has established information transfer rules, procedures, and agreements for all types of transfer facilities within the organization and with external parties. These rules and procedures ensure that information is transferred securely, with appropriate controls in place to protect its confidentiality, integrity, and availability. Regular training is provided to relevant personnel to ensure that they understand the importance of information transfer security and how to apply the rules and procedures correctly. The effectiveness of the information transfer controls is regularly reviewed and updated as necessary to ensure that they remain appropriate and effective.

Information Transfer Policy and Procedures

a) All users should adhere to the procedures designed to protect exchanged information from interception, copying, modification, mis-routing, and destruction.

b) All business correspondence, including messages, shall be retained as per the data retention policy.

c) Sensitive or critical information shall not be left on printing facilities like copiers, printers, etc.

d) All users shall ensure that they take appropriate precautions to avoid revealing sensitive information when making a phone call.

e) All employees shall ensure that they do not have confidential conversations in public places or open offices and meeting places.

f) Users shall be made aware of the risk of Information Security while exchanging information through Voice, Fax, and Video Communication facility.

Agreements on information transfer

a) These standards apply to bulk exchange or transmission of data for major systems. Guidelines regarding Emails are given in a separate section.

b) Circumstances of data exchange with other organisations, individuals and agencies should be recognised and documented.

c) There should be agreements defining liability and responsibility for exchanges of data with other parties.

d) Data exchange agreements should define management responsibilities for controlling and notifying transmission, despatch and receipt of data.

e) There should be procedures for notifying transmission, despatch and receipt of data.

f) Minimum standards for packaging and transmission of data should be defined.

g) Responsibilities and liabilities in the event of data loss should be defined and understood.

h) Agreements for data exchange must include:
   - Definition of data and software ownership
   - Responsibilities for data protection
   - Responsibilities for software copyright, compliance and similar considerations.

i) Special measures may be provided for protection of very sensitive items (such as encryption keys).

Email and Web Security Policy

a) The allotment of E-Mail User-IDs to employees should be strictly on a 'need to use' basis. Management reserves the right to grant / disable / revoke the facility at its discretion.
b) E-mail facility is for use by the organisation's employees for carrying out organisational work.
c) Users should make suitable arrangements during their absence to ensure that organisation's interest is not affected because of inaccessibility of their e-mail facility.
d) Electronic mail message containing sensitive information should be forwarded only if the recipient is authorised to view the information or the originator approves the forwarding.
e) Broadcast messages should be sent only with permission or knowledge of the Technical Head.
f) Email attachment size are restricted to 30MB including email content.
g) Frivolous use of E-Mail for transmitting non-work-related messages, pictures, jokes, programs, chain letters, spamming, etc. is strictly prohibited.
h) Each employee is responsible for the contents of his / her e-mail. All e-mails must be identified with a user's name or e-mail ID to allow for individual tracking.
i) Individuals accessing the e-mail services of Fourd must not use or access an e-mail account assigned to another individual to either send or receive messages. If there is a need to read another person's e-mail (while he /she are away on vacation for instance), message forwarding and other facilities must be used instead. A written approval from the ISM must be obtained in case a user's e-mail needs to be read in his / her absence.
j) To prevent computer viruses, employees must not open attachments that are from an unknown source.
k) Fourd employees must treat e-mail messages and files as confidential information. E-mail must be handled as a confidential and direct communication between a sender and a recipient.
l) All the e-mails are Fourd's property and are liable to be read, intercepted and if necessary, deleted.
m) All messages sent by employees by e-mail are the records of Fourd. At any time and without prior notice, the management reserves the right to examine e-mail, personal

file directories, and other information stored on Fourd's computers and servers used by Fourd. E-mail messages may be monitored for any of the following reasons:

a. Ensuring internal policy compliance,
b. To support internal investigations for suspected criminal activity and,
c. To assist with the management of information systems of Fourd.

n) Fourd may also disclose e-mail messages sent or received to law enforcement officials without prior notice to the employees who may have sent or received such messages. Users should restrict their communications to business matters in recognition of this electronic monitoring. Monitoring of e-mail for the above-mentioned reasons must, however, be explicitly authorized by the ISSC. Unless specifically delegated, the task of monitoring e-mail messages by all other employees is prohibited.

o) Users must not automatically forward their e-mails to any address outside the group / Fourd's networks, unless approved by the ISSM. Auto forwarding of e-mails within Fourd for business purposes, may be allowed for a limited period with the prior approval of the ISSM.

p) E-mail systems must be used primarily for business purposes only (unless management has specifically approved the non-business use).

q) Confidential information should never be disseminated to unauthorized sources. This includes the transmission of documents containing Project Related information or financial information.

9.4 Return of assets

a) Fourd requires all personnel and other interested parties to return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement. This includes but is not limited to laptops, mobile devices, access cards, and keys.

b) The return of assets is verified by the appropriate manager or supervisor and recorded in the organization's asset inventory. This helps to protect the organization's assets and ensures that they are not misused or accessed by unauthorized individuals.

c) Regular reminders are provided to personnel to ensure that they are aware of their obligations regarding the return of assets.

d) IT Team and respective teams owning the assets shall document the return of assets in the possession of employees upon termination of their employment using standard processes.

e) These processes must ensure the return of systems, information or documents, files, data, books and manuals in physical or other media formats including other information assets developed or prepared by an employee or contractor in the course of their duties.

f) IT Team shall ensure that returned items are verified against established asset inventories and signed off in the exit workflow after inspecting for the condition.

g) Recovery of compensation for assets not returned, based on established criteria regarding depreciation and replacement value for classes of items shall be as per documented procedures

h) If personnel and other interested parties purchase the organization's equipment or use their own personal equipment, procedures should be followed to ensure that all relevant information is traced and transferred to the organization and securely deleted from the equipment

i) In case of Absconding, will follow the termination or change of employment and will try to recover the asset.

j) During the notice period and thereafter, the organization shall prevent unauthorized copying of relevant information (e.g. intellectual property) by personnel under notice of termination

a) user endpoint devices;

b) portable storage devices;

c) specialist equipment;

This protects the organization's assets as part of the process of changing or terminating employment, contract or agreement.

9.5 Classification of Information

Fourd classifies information according to its information security needs based on confidentiality, integrity, availability, and relevant interested party requirements. The classification levels are defined and communicated to all relevant personnel to ensure that they understand the requirements for handling and protecting different types of information. The classification process is regularly reviewed and updated to ensure that it remains appropriate and effective in light of changing business needs and the evolving threat landscape. This enables the organization to allocate resources effectively and prioritize its information security efforts based on the criticality and sensitivity of the information.

(a) When an item of Information is created or procured by Fourd, it is classified using its Information Classification Scheme mentioned in the classification of assets procedure.

(b) Individuals with access to information processing facilities are properly instructed to contact the ISSM for protection requirements if they are unsure of how to properly classify or handle protectively marked information.

(c) Recipients of Information must handle it with due care and must respect the classification established by the originator of the information.

(d) When handling customer or third-party proprietary information, personnel understand any differences in terminology with respect to how Information is classified, and affecting how the information is to be handled or transmitted, to ensure that the

information is protected to no less than the same level as the customer's or third party's classification.

10.0 Access Control

The policy of Fourd is to ensure:

Groupwise access define and regularly review their access.

a) Access to Server, Firewall, Network services and information is managed based upon "Need to Know" and "Authorized to Know" attributes. Prior to access being given to Server or Information or file/ folder shares, both conditions must be satisfied.

b) All persons with access to information processing facilities are limited without repudiation.

c) Business requirements for critical systems and applications are defined for access control to information processing facilities.

d) The granting of access and modification of access rights to information processing facilities is controlled within a formal procedure that satisfies all statutory, regulatory, and contractual obligations. *(Refer to information security procedures for more details)*

e) Validation of access rights requested, or granted, to information processing facilities are performed to ensure consistency with the Information Security Policy, and that segregation of duties, where implemented, is not compromised.

f) User access rights are audited and reviewed at regular and periodic intervals with the Process Owners where appropriate, consistent with statutory, regulatory, and contractual obligations.

g) The outcome of user access rights audit and review are properly documented and maintained.

h) Passwords used to access IT systems and information are managed to ensure they are not disclosed to un-authorized persons, are sufficiently complex and changed at an acceptable frequency to prevent unauthorized use. Password policy for the proper control and protection of passwords are established and provided to individuals with access to information processing facilities.

i) Acceptable usage policy is provided to individuals with access to IT equipment, system, or information to assist in protecting said equipment, systems and information from unauthorized use, or misuse.

j) Access to network services is controlled and monitored, to ensure that the security of the services is not compromised, and that access is managed in accordance with all Fourd' Policies.

k) All connections to Fourd' internal networks, and IT assets, where the connection originates outside of Fourd' networks are controlled to prevent unauthorized access.

l) The acceptable use of, and authority and authorization for use of system utilities capable of overriding or modifying access controls is strictly controlled and documented. ISSM regularly reviews the list of individuals having this access to limit it to a minimum number.

10.1 Identity Management

Fourd has implemented a comprehensive identity management system that covers the full lifecycle of identities, from creation to retirement. This system ensures that all user accounts and access privileges are properly authorized, monitored, and maintained, with policies and procedures regularly reviewed and updated to ensure compliance with industry standards and regulations. Regular review and recertification of access privileges prevent unauthorized access and ensure alignment with the principle of least privilege. A team of identity management experts oversees the implementation of controls to protect sensitive information and assets.

a) All personnel shall acknowledge Fourd's Information Security Policy before access is granted to an account or Fourd's Asset.

b) All accounts created shall have an associated, and documented, request and approval.

c) Segregation of duties shall exist between access request, access authorization, and access administration.

d) Information Resource owners shall be responsible for the approval of all access requests.

e) All accounts shall be uniquely identifiable using the user's name assigned by Fourd's IT team and include verification that redundant user IDs are not used.

f) All accounts, including default accounts, must have a password expiration that complies with Fourd's Authentication Standard.

g) Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege". No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities

h) Whenever possible, access to Information Resources shall be granted to user groups, not granted directly to individual accounts.

i) Shared accounts shall not be used. Where shared accounts are required, there use shall be documented and approved by respective management.

j) Upon user role changes, access rights shall be modified in a timely manner to reflect the new role.

k) Creation of user accounts and access right modifications shall be documented and/or logged.

l) Any access to Fourd's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period

m) Any accounts that have not been accessed within a defined period of time shall be disabled.

n) Accounts shall be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.

o) System Administrators or other designated personnel shall be responsible for modifying and/or removing the accounts of individuals that change roles.

p) Administrative/Special access accounts shall have account management instructions, documentation, and authorization.

q) Personnel with Administrative/Special access accounts shall refrain from abuse of privilege and must only perform the tasks required to complete their job function.

10.2 Authentication Information

10.2.1 Password Policy

The policy of Fourd is to ensure:

a) All Fourd's owned electronic devices must, if possible, have password protection enabled.

b) Password strength shall be minimum of 8 characters.

c) Passwords must contain a mixture of uppercase and lowercase letter, numbers and special characters.

d) Passwords must not contain common dictionary words.

e) Password must be changed once in 30 days.

f) The user account must be locked out after 5 invalid logon attempts.

g) The Account lockout counter must reset after one day.

h) Temporary password assigned must be changed at the first log-on

i) The same password should not be repeated within a cycle of 5 password changes.

j) Passwords must not be inserted into email messages or other forms of electronic communication and should not be shared with anyone, including via email or phone conversations.

k) Passwords should not be written down or stored electronically without encryption.

l) MFA to be enabled wherever it requires.

m) All passwords should be (Data masking) masked while using.

10.3 Access rights

Fourd provisions, reviews, modifies, and removes access rights to information and other associated assets in accordance with its relevant policies and rules for access control.

Reviews of User Access Rights

- Access rights given to user shall be reviewed by the information owner at least monthly once or whenever there is a major change in the assignment of user rights. User access lists to applications, assets, software's etc shall be reviewed and reconciled with the HR list of active/ inactive employees.
- Access given to third parties for Fourd's information resources should be restricted and governed by the same principle of 'least privilege' and "need to know basis". Fourd's employees coordinating with the respective third-party consultants, engineers, vendor's representatives etc. are responsible for justifying and authorizing the access rights granted to third parties. The network access agreement must be entered into with the 'Third Party' before granting access to Fourd's network, which would cover the responsibilities as well as the terms and conditions agreed by the third party.
- Third party representatives must be restricted to use Fourd 's information resources from within Fourd's network. In other words, remote connectivity from their office to the Fourd's network shall not be allowed.
- Access rights to the consultants and other third parties must be formally granted and monitored. The relevant rights must be taken back once the required assignment is over. An access rights form / an email with requisite access details must be submitted by the third party. Technical Head / System Administrator should review activity logs generated at the Operating System level to monitor activities performed by third parties.
- The authorisation of special privileges like the access to third parties, remote logins, and accesses from networks outside Fourd's network should be reviewed once in three months.

Removal of Access Rights

- In case of terminations, IT shall ensure that access to information systems is revoked on the last working date after business hours by deactivation or deletion of the person's access identifiers and the removal of the access authorities granted to them.
- In case of job changes, IT shall modify rights of the employee in line with the access control policy.
- IT shall send communication of removal of access rights to HR Department

10.4 Secure authentication

- A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.
- Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility to the network and applications where ever possible.
- The strength of authentication should be appropriate for the classification of the information to be accessed. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as digital certificates, smart cards, tokens or biometric means, should be used.
- Authentication information should be accompanied by additional authentication factors for accessing critical information systems (also known as multi-factor authentication). Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorized accesses. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.
- Biometric authentication information should be invalidated if it is ever compromised. Biometric authentication can be unavailable depending on the conditions of use (e.g. moisture or aging). To prepare for these issues, biometric authentication should be accompanied with at least one alternative authentication technique.
- Unauthorized access shall not be permitted. Access to information systems must use a secure login process and factor in the following.
    - Information displayed during logon
    - Unsuccessful logon attempts
    - Password transmission
- Logon process shall not display passwords in clear text as they are entered.

- The use of shared user IDs for a group of users should be considered only where the use of such group ids does not significantly affect accountability and segregation of duties and is within the limits of the licensing agreements

Refer: Secure authentication procedure available - *A5.37 Documented operating procedures v1.1*

10.5 User endpoint devices

Fourd implements necessary controls to protect information stored on, processed by or accessible via user endpoint devices. Security measures are in place to ensure the confidentiality, integrity and availability of information, including regular updates and patches, anti-virus software, firewalls, and data encryption. Additionally, access to sensitive information is restricted and controlled through the use of strong passwords, multi-factor authentication and other appropriate access control mechanisms.

Mobile Device Policy

The scope of mobile devices in the organization includes mobile phones (for checking emails) and office provided laptops

The loss or theft of a laptop / portable computer containing unencrypted confidential / critical information results in the loss of both a physical and proprietary information asset. Therefore, utmost care should be taken regarding the safety of a laptop or mobile device.

- A record of all portable equipment (mobile phones and laptops) available together with configuration and identification numbers should be maintained by the Technical Head / System Administrator.
- The ownership and responsibility of all such equipment should be clearly established to ensure accountability and maintenance.
- Technical Head / System Administrator should record and acknowledge after issue of Laptops to Senior Executives for their exclusive use.
- When not in use within a work area, the laptop should always be stored, in a well-secured filing cabinet / desk. It should be never left on desk unattended even for short periods.
- While taking portable equipment or mobile devices (not usually authorised to be taken out of work area), the relevant security gate passes should be made and authorised by the appropriate authority
- Laptops and other portable equipment used to connect to the network over the Internet must be protected by personal firewall.

- Encryption, anti-virus / anti-malware protection shall be made mandatory for all mobiles which are intended to be part of the domain
- Fourd shall take into consideration key security factors like access, software installation, patches of applicable software etc. for mobile devices in its IT network.
- Periodic checks shall be done for endpoint device software (including versions) and for applying relevant updates, where needed

Special care during Travel

For laptops, smartphones and other mobile devices being carried during travel, the following precautions need to be taken:

- Laptops and smartphones should always be stored when not in use, in a well-secured place.
- Laptops and smartphones should be never left in the open on a desk unattended even for short periods of absence.
- Laptops and smartphones should always be kept in the user's possession. They should never be left unattended in cars or Guest House/ hotel rooms.
- Laptops and smartphones should not be left with hotel / guesthouse personnel, and they should not be checked in as registered baggage and should always be carried as cabin/hand baggage in an aircraft.
- Power on password should be used to prevent disclosure of information in the computer in the event of a loss.
- In case of any loss of smartphone or laptop, employee will have report the incident as per the incident reporting procedure.

Unattended User Equipment

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

- Whenever a user leaves equipment unattended, it should be secured with a screen saver with a password, and wherever available auto log out/ off settings should be used for applications/ systems.

- Fourd shall ensure users log-off from applications or network services when they are no longer needed

- Other locking mechanisms available should also be utilised to protect any resources and application when they are unattended during or beyond working hours.

This protects information against the risks introduced by using user endpoint devices.

10.6 Information access restriction

- Fourd shall ensure that it does not allow access to sensitive information by unknown user identities or anonymously

- Fourd shall implement physical or logical access controls for the isolation of sensitive applications, application data, or systems.

- End users should be allowed to see only user documentation that should not contain sensitive technical information.

- The sensitivity of each information-processing asset should be analysed. Depending on the sensitivity, the computing environment should be considered for isolation.

- Systems that have highly sensitive information should be isolated logically, especially when client agreements require such isolation. They should be isolated from the network normally using Virtual LANs and be connected only when necessary. Further, the traffic during connectivity be properly controlled and logged.

- Customer specific environments should also be considered for such isolation based on business needs. Wherever possible, areas handling highly sensitive information should be isolated physically too.

- An application-wise List of Employees with access and roles defined shall be maintained. Further, a complete list of Employees with privileged access or access to database shall also be maintained and accesses/ restrictions periodically reviewed.

This ensures only authorized access and to prevent unauthorized access to information and other associated assets.

11.0 Supplier Relationship

11.1 Information Security in Supplier Relationships

11.1.1 General Provisions

In general, information security requirements will vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

However the following will generally apply.

1. The information security requirements and controls should be formally documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract
2. Separate Non-Disclosure Agreements should be used where a more specific level of control over confidentiality is required
3. Appropriate due diligence must be exercised in the selection and approval of new suppliers before contracts are agreed
4. The information security provisions in place at existing suppliers (where due diligence was not undertaken as part of initial selection) must be clearly understood and improved where necessary
5. Remote access by suppliers must be via approved methods that comply with our information security policies
6. Access to Fourth Dimension Technologies Pvt Ltd information should be limited where possible according to clear business need
7. Basic information security principles such as least privilege, separation of duties and defence in depth should be applied
8. The supplier will be expected to exercise adequate control over the information security policies and procedures used within sub-contractors who play a part in the supply chain of delivery of goods or services to Fourth Dimension Technologies Pvt Ltd.
9. Fourth Dimension Technologies Pvt Ltd will have the right to audit the information security practices of the supplier and, where appropriate, sub-contractors
10. Incident management and contingency arrangements should be put in place based on the results of a risk assessment
11. Awareness training will be carried out by both parties to the agreement, based on the defined processes and procedures if required.

The selection of required controls should be based upon a comprehensive risk assessment taking into account information security requirements, the product or service to be supplied, its criticality to the organization and the capabilities of the supplier.

11.1.2 Cloud Services

Cloud service providers (CSPs) should be clearly recognized as such so that the risks associated with the CSP's access to and management of Fourth Dimension Technologies Pvt Ltd cloud data may be managed appropriately.

When acting as a CSP, Fourth Dimension Technologies Pvt Ltd will clearly set out the relevant information security measures it will implement as part of the agreement. Fourth Dimension Technologies Pvt Ltd will also ensure that information security objectives are set for third parties who provide components of the cloud service to customers and that they carry out adequate risk assessment in order to achieve an acceptable level of security.

11.1.3 Due Diligence

Before contracting with a supplier, it is incumbent upon Fourth Dimension Technologies Pvt Ltd to exercise due diligence in reaching as full an understanding as possible of the information security approach and controls the company has in place. It is important that the documented *Supplier Due Diligence Assessment Procedure (A15.3)* is followed so that all of the required information is collected and an informed assessment can be made.

11.2 Addressing Security within Supplier Agreements

Once a potential supplier has been positively assessed with due diligence the information security requirements of Fourth Dimension Technologies Pvt Ltd must be reflected within the written contractual agreement entered into. This agreement should take into account the classification of any information that is to be processed by the supplier (including any required mapping between Fourth Dimension Technologies Pvt Ltd classifications and those in use within the supplier), legal and regulatory requirements and any additional information security controls that are required.

For cloud service contracts, information security roles and responsibilities should be clearly defined in areas such as backups, incident management, vulnerability assessment and cryptographic controls.

Template Fourth Dimension Technologies Pvt Ltd *Supplier Information Security Agreement (A15-2)* should be used as a starting point.

Appropriate legal advice must be obtained to ensure that contractual documentation is valid within the country or countries in which it is to be applied.

11.2.1 Evaluation of Existing Suppliers

For those suppliers that were not subject to an information security due diligence assessment prior to an agreement being made, an evaluation process should be undertaken to identify any required improvements. For details Refer *A5.37 Documented operating procedures v1.1*.

11.3 Monitoring and Review of Supplier Services

In order to focus resources on the areas of greatest need, suppliers will be categorized based on an assessment of their value to the organization.

Each supplier will be placed into one of the following four categories:

1. Commodity
2. Operational
3. Tactical
4. Strategic

11.4 Managing information security in the ICT supply chain

- All requests for access to restricted / confidential / internal information coming from a third-party shall be forwarded to the information owner who shall decide whether the request should be granted and level of access to be granted.
- Reasons and type of access given to the third party (physical or logical) should be approved after all the required security checks are done.
- Connections to IT facilities owned by Fourd must conform to Fourd's Information Security Policy.
- Access to information and information processing facilities by third parties should not be provided until appropriate controls have been implemented and a contract has been signed defining the terms for connection or access.

11.5 Information security for use of cloud services

a) Fourd has established processes for acquisition, use, management, and exit from cloud services in accordance with the organization's information security requirements.

b) Fourd shall establish and communicate relevant policy on the use of cloud services to all relevant interested parties.

c) Fourd shall define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how Fourd manages services provided by suppliers or external.

d) The use of cloud services can involve shared responsibility for information security and collaborative effort between the cloud service provider and Fourd acting as the cloud service customer. It is essential that the responsibilities for both the cloud service provider and Fourd, acting as the cloud service customer, are defined and implemented appropriately.

Fourd shall identify:

a) all relevant information security requirements associated with the use of the cloud services;

b) cloud service selection criteria and scope of cloud service usage;

c) roles and responsibilities related to the use and management of cloud services;

d) which information security controls are managed by the cloud service provider and which are managed by Fourd as the cloud service customer;

e) how to obtain and utilize information security capabilities provided by the cloud service provider;

f) how to obtain assurance on information security controls implemented by cloud service providers;

g) how to manage controls, interfaces and changes in services when Fourd uses multiple cloud services, particularly from different cloud service providers;

h) procedures for handling information security incidents that occur in relation to the use of cloud services;

i) its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks;

j) how to change or stop the use of cloud services including exit strategies for cloud services.

k) Cloud service agreements are often pre-defined and not open to negotiation. For all cloud services, Fourd should review cloud service agreements with the cloud service provider(s). A cloud service agreement should address the confidentiality, integrity, availability and information handling requirements of Fourd, with appropriate cloud service level objectives and cloud service qualitative objectives.

l) Fourd shall also undertake relevant risk assessments to identify the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the Senior leadership of Fourd.

An agreement between the cloud service provider and Fourd, acting as the cloud service customer, should include the following provisions for the protection of the Fourd' data and availability of services:

a) providing solutions based on industry accepted standards for architecture and infrastructure;

b) managing access controls of the cloud service to meet the requirements of Fourd;

c) implementing malware monitoring and protection solutions;

d) processing and storing the Fourd' sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction;

e) providing dedicated support in the event of an information security incident in the cloud service environment;

f) ensuring that the Fourd' information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted);

g) supporting Fourd in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions;

h) providing appropriate support and availability of services for an appropriate time frame when Fourd wants to exit from the cloud service;

i) providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by Fourd, acting as the cloud service customer;

j) providing and returning information such as configuration files, source code and data that are owned by Fourd, acting as the cloud service customer, when requested during the service provision or at termination of service.

Fourd, acting as the cloud service customer, shall consider whether the agreement should require cloud service providers to provide advance notification prior to any substantive customer impacting changes being made to the way the service is delivered to Fourd, including:

a) changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering;

b) processing or storing information in a new geographical or legal jurisdiction;

c) use of peer cloud service providers or other sub-contractors (including changing existing or using new parties).

d) Fourd shall maintain close contact with its cloud service providers. These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and Fourd, acting as the cloud service customer, to monitor each service characteristic and report failures to the commitments contained in the agreements.

Fourd shall periodically review the security compliances and assessments done by the cloud provider (for eg., ISO, SOC 2 certifications) to confirm continued compliance.

12.0 Incident Management

The policy of Fourd is to ensure:

a) ISSC formalizes processes and procedures that are used to support the resolution of Incidents.

b) ISSC has defined procedures for Incident Management that make certain sufficient information is recorded to ensure the effective and efficient execution of all related processes and procedures.

c) The approved method, or methods, for reporting incidents are published and made available to all end-users.

d) Analysis of incidents occurs on a periodic and regular basis to determine if there exists a persistent and recurring defect in information processing facilities. If a persistent and recurring defect found to exist, then a defect/ weakness will be recorded for resolution.

e) All incidents reported or identified are prioritized for resolution based upon their impact to the normal execution of business processes.

f) The impact of incident on service performance or availability is made available to the concerned people.

g) CISO ensures the implementation of solutions is done in accordance with the Change Management policy.

Refer: Information Security Incident Management

13.0 Business Continuity Management

a) To recover lost data, licensed recovery software applications and hardware tools can be used.
b) We keep a backup hardware device on standby for any end- or network-related devices in case of emergencies.
c) Having a secure backup plan in place is crucial for businesses to ensure that operations can continue running in the event of a disaster.
d) A reliable backup solution is essential for restoring data and applications in case of damage or destruction to the data center, server, or other IT infrastructure.
e) Ensure server and application which is cloud services are backup or replication enabled.

Refer: A-5.29-Business Continuity Plan and Procedures

14.0 Compliance requirements

14.1 Legal, statutory, regulatory and contractual requirements

Fourd identifies, documents and keeps up to date, the legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements.

1. The ISM shall maintain a checklist of all applicable legislation governing Information Security and related areas.
2. All relevant statutory, regulatory and contractual requirements shall be documented, tracked and monitored for compliance.

Refer: CL-4.2 Legal, Regulatory and Contractual Requirements Policy and Procedure

14.2 Intellectual property rights

- All assets with requirements to protect IPR such as technical manuals, articles, papers, journals other paper documents software, music, digital material, movies, advertisements, stories, literature, product designs, brand name, trademarks etc. shall be identified and protected appropriately.
- Fourd shall ensure that all license agreements are respected and limits the use of the products to specified machines, and for specific purposes.
- The IPR of hardware, software and documentation belonging to Fourd shall not be disclosed to any outside party unless and otherwise cleared by legal department
- The IPR of programs and associated material supplied by outside organizations / collaborators shall be used by Fourd for only those purposes for which they are licensed.
- Controls shall be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing.
- Fourd shall ensure that information and software is only acquired from reputable vendors or sources.
- Fourd shall maintain proof or evidence of ownership or right to use adhering to the terms and conditions of use associated with intellectual property.
- Fourd shall ensure that the maximum number of users permitted is not exceeded.
- Fourd shall implement processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licenses
- Fourd's users shall use only licensed and approved software for all business purposes. Any unauthorized reproduction of computer software may expose Fourd and the staff

members to civil and criminal liability for infringement and breach of copyright and other intellectual property rights.

- Technical Head / System Administrator shall maintain an inventory of licensed software.
- Any act relating to unauthorized duplication of software or copyrighted materials may be subjected to disciplinary action which may include the termination of the staff member's employment contract.

This ensures compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.

14.3 Protection of records

Records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release through the implemented procedures by Fourd.

- Fourd shall ensure that important records are protected from loss, destruction and falsification. The following records of Fourd are safeguarded:
    - Master List of Documents
    - Master List of Records
    - All contracts and agreements
- All records shall be retained for a defined period with retention policies, as specified by the owner of the information after factoring in the applicable laws and regulations.
- Storage and handling of all these records shall be in accordance with a defined procedure.
- The documented information shall be protected from loss, destruction and falsification, unauthorized access, release, and disposal in accordance with legislative, regulatory, contractual and business requirements.

When deciding upon protection of specific organizational records, Information Owners shall consider the information security classification

14.4 Privacy and protection of PII

Fourd has identified and met the requirements for preserving privacy and protecting Personally Identifiable Information (PII) in accordance with applicable laws, regulations, and contractual requirements.

- Information Owners shall document and implement policies for privacy and the protection of personal information.
- The policy shall be communicated to all employees involved in the processing of personal information.
- Privacy Impact Assessment and Security Threat shall be done as part of the Risk Assessment process for all operations areas that are collecting, processing and storing sensitive personal information.
- The organization shall refer to its Information Security Policy and guidelines along with other supporting controls and measures for ensuring maximum protection to PII and sensitive information.

14.5 Independent review of information security

Fourd has established an approach to managing information security that includes regular independent reviews of its implementation, including people, processes, and technologies. These reviews occur at planned intervals or whenever significant changes occur.

- Information security management system at Fourd shall be subject to independent review annually.
- The review shall be conducted by auditors who are independent of the Information Security / IT Functions.
- The auditors can be either external or internal audit teams.
- Information security auditors shall submit the audit findings to the management of Fourd
- The independent reviews go hand-in-hand with the internal reviews that are done periodically by the ISSC and discussed as part of Management Reviews.

14.6 Compliance with policies, rules and standards for information security

Fourd has established a process to regularly review compliance with the organization's information security policy, other relevant policies, rules and standards.

- It is the duty of the Fourd management including the ISSM to ensure that all security procedures within their area of control are in strict compliance with this manual.
- ISSM shall also support review and checking processes to ensure better compliance.
- In cases where non-compliance has been noticed, the ISSM shall:
    - Determine the cause of non-compliance
    - Action plan to avoid recurrence of non-compliance

- Implement appropriate corrective plan
- Review the corrective actions taken

- Results of reviews and subsequent corrective actions shall be recorded.
- Fourd shall review IS policies, procedures etc. periodically with sign offs from CISO
- Review of critical logs by CISO shall also be carried out and documented.

14.7 Documented operating procedures

Fourd has documented and made available operating procedures for information processing facilities to personnel who need them.

- Fourd shall define a set of operating manuals for key processes and functions, including core IT domains, the operation of applications and their security features.
- Operating procedures and responsibilities for information systems and information processing facilities shall be authorized, documented, and maintained.
- Operating procedures should be treated as formal documents and changes should be authorized by management.

These procedures should specify the detailed execution of each job including:

- Processing and handling of information
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities.
- Support contacts in the event of unexpected operational or technical difficulties.
- Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from the failed jobs.
- System restart and recovery procedures for use in the event of system failures.

There should be documented operating procedures for computer and network management as well as applications including:

- Start-up and close-down
- Data backup
- Testing and verification of backup media
- System restart and recovery in the event of system failure / equipment maintenance
- Computer room management, safety, and security

There must be documented operating procedures for:

- Correct handling of data files
- Scheduling requirements and timing inter-dependencies.
- Handling errors or other exceptional conditions during job execution, including restrictions on the use of system utilities
- There must be documented operating procedures for handling special output, including confidential output and disposal of confidential waste output

15.0 Planning

15.1 Actions to Address Risks and Opportunities

15.1.1 General

In accordance to the clause 6.1.1 of ISO/IEC 27001:2022, Fourd considers the issues referred to in 4.1 and the requirements referred to in 4.2 and determines the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement. The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to integrate and implement the actions into its information security management system processes; and evaluate the effectiveness of these actions.

15.1.2 Information security risk assessment

Fourd, relies on the following ISMS documents, ***'Risk assessment'*** to carry-out its Risk management function, as the same is elaborate and comprehensive and also applicable to Fourd.

In accordance to the clause 6.1.2 of ISO/IEC 27001:2022, establishes information security risk assessment process that:

a) determines and maintains information security risk criteria including the risk acceptance criteria; and criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results.

c) identifies the information security risks:

1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
2. identify the risk owners;

d) analyses the information security risks:

1. assess the potential consequences that would result if the risks identified in 6.1.2 (c) (1) were to materialize;
2. assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 (c) (1); and
3. determine the levels of risk;

e) evaluates the information security risks:

1. compare the results of risk analysis with the risk criteria established in 6.1.2 (a); and
2. prioritize the analysed risks for risk treatment.

Fourd retains documented information about the information security ***risk assessment*** process.

15.1.3 Information security risk treatment

Fourd, relies on the following ISMS documents, ***'Risk assessment*** to carry-out its Risk management function, as the same is elaborate and comprehensive and also applicable to Fourd.

Fourd Risk treatment, which is part of the risk management, considers the following risk treatment options: (i) Acceptance (ii) Transfer (iii) Mitigation

In accordance to the clause 6.1.3 of ISO/IEC 27001:2022, FourdI establishes information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

c) compare the controls determined in 6.1.3 b) above with those in Annex-A and verify that no necessary controls have been omitted;

d) produce a Statement of Applicability that contains:

— The necessary controls (see 6.1.3 b) and c));

— Justification for their inclusion;

— Whether the necessary controls are implemented or not; and

— The justification for excluding any of the Annex A controls

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

Fourd retains documented information about the information security ***risk treatment*** process.

16.0 Logging and Monitoring

16.1 Logging

Event Logs

- The ISSM should decide on the conditions for logging. Audit logs should contain:
    - User ID's
    - Dates and times for log-on and log-off
    - Terminal identity or location if possible
    - Records for successful and rejected system attempts
    - Records of successful and rejected data and other resource access attempts
- The following are the major audit event types that need to be logged in applications/ networks:
- Unsuccessful attempts to read, modify, copy or delete.
- Allowed / denied access.
- Event Timestamp
- Successful and Failed transactions
- User access privileges
- User ID, address, port blocking or blacklisting
- File access
- Activation or de-activation of protection systems
- Changes to system configuration
- Alarm raised by access control system.
- Successful / unsuccessful attempt to access security related directories.

- Successful / unsuccessful logons and logoffs
- All faults reported by users shall be logged by the IT Team.
- Similarly, faults displayed by systems/ servers pertaining to information processing or communication systems shall be logged by the IT Team and the respective vendor shall be notified
- IT Team shall record the corrective action taken for resolution of these faults in the said log.
- Review of logs shall be carried out by respective departments on periodic basis, using different techniques such as, but not limited to – manual reviews, SIEM, Log analysers etc. to identify and detect anomalies and conduct root cause analyses.
- The ISSM shall review the corrective measures taken to ensure that controls have not been compromised, and that the action taken is fully authorised.
- Logging feature shall be activated and always enabled whereas deliberate action to disable logging will consider as a security violation.

Protection of Logs

- Access to edit or delete log files shall not be allowed to anyone.
- Logs shall be stored in a centralized repository with adequate access controls in addition to the local system.
- All log files shall be backed up and made available to the monitoring authority.
- Log backups shall be done on a server different from the device that is being logged.
- All log files shall be retained for a period of six months.
- Fourd shall document a list of employees having access to Critical Event and Access logs for various applications and have the same signed off. This will undergo periodic scrutiny, as part of Access Reviews.

Logs of Administrators/ Super Users

- Logs shall be enabled to capture details of all activities done by the Technical Head / System administrator/ Super Admin users of applications.
- Super User Logs should include the following information:
    - System starting and finishing time

- System errors and corrective action taken
- Confirmation of correct handling of data files and computer output
- Name of the person making the log entry

- These logs shall be subjected to regular, independent checks against operating procedures. These checks shall be performed by IT team.

This records events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

16.2 Monitoring activities

- As part of its monitoring activities, Fourd shall use tools and analyzer (eg. SIEM) to monitor the events, activities and potential incidents in the organization network or cloud.
- Fourd shall monitor the outbound and inbound network, system and application traffic
- Fourd shall have monitoring mechanisms in place for access to systems, servers, networking equipment, monitoring system and critical applications
- Fourd shall monitor the logs from security tools [such as antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention]; and critical or admin level system and network configuration logs and discuss the same periodically in the management review meetings of ISSC
- Alert mechanisms shall be configured for event logs relating to systems.
- Fourd shall consider the use of blacklists or whitelists for allowed IP and monitor the same for any non-adherence or attempts to access blacklisted IP or sites.

Threats that are monitored by Fourd may include:

- malicious software/ IP addresses
- unplanned termination of process/apps
- DDoS, buffer overflows
- unusual system behaviour
- unauthorised access or scanning of applications and networks
- successful and unsuccesful attempts to access protected data (eg., DNS server, file systems)

Baseline of normal behaviour and monitoring against this baseline (review in peak and normal periods, time, location and frequency of access for each user/ group) shall be done and documented by Fourd.

16.3 Clock synchronization

1. The real-time clocks on workstations should reflect the accurate current time at their physical location The correct setting of critical computer clocks is important and shall be carried out to ensure the accuracy of audit logs. This enables the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.
2. One Server is identified as Time Master Server & other Servers of the network are synchronized with the Master.
3. Computer and end user device clocks shall all be synchronized for accurate reporting.
4. Administrators must synchronize information system clocks to:
    - the local router gateway/ network; or,
    - the organization approved clock host.
5. System administrators shall confirm system clock synchronization:
    - Following power outages or blackouts.
    - As part of incident analysis and audit log review; and,
    - At least semi-annually in conjunction with UTC and IST

- Time discrepancies, if identified shall be reported to IT Helpdesk.
- Time synchronization shall be enforced at the system level through clock synchronisation protocols such as Network Time Protocol (NTP).
- The organization shall ensure that all its endpoint systems, CCTV alarms, access devices, cloud systems, application times displayed, DC and DR, as well as other Information Processing systems in Chennai, Mumbai and other branch offices carry the same/ uniform time on its systems which can be configured to a centralized time master server like NTP.

17.0 Operational software

17.1 Use of privileged utility programs

This control acts as a preventive measure to maintain risk by establishing guidelines for the use of utility programs that have the potential to override critical business systems and applications.

a) The term “utility program” refers to any software designed to analyze or maintain a computer system or network.

b) Examples of utility programs include:

1) Disk defragmenters.
2) Backup software
3) Networking tools
4) Diagnostic tools
5) Patching assistants
6) Antivirus programs

17.2 Installation of software on operational systems

- The operational system shall be updated only after authorization by the Technical Head / System Administrator.
- The updating shall be as per the instructions of the software or application vendor.
- The updating in the production environment shall be done only after successful testing in a test / development environment.
- Previous versions of software shall be retained as a contingency. An audit log shall be maintained of all updates to operational program libraries.
- Vendor supplied software used in operational systems should be maintained at a level supported by the supplier.
- Software patches should be applied when they can help to remove or reduce security weaknesses.
- Patch management procedures shall include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner. Rigorous rigorous testing of security patches before deployment into the production environment
- List of Authorised Third Party Software allowed to be installed on end user systems shall be defined and approved by CISO
- Administrative control shall be in place in all laptops to restrict installation of other unapproved software by users or employees
- Any exceptions to the list of approved/whitelisted software that may be required on employee's systems will have to be approved by CISO and documented.

Restrictions on Software Installation

- Fourd users shall use only licensed and approved software for all business purposes. Any unauthorized reproduction of computer software may expose Fourd and the staff members to civil and criminal liability for infringement and breach of copyright and other intellectual property rights. Any act relating to unauthorized duplication of software may be subjected to disciplinary action which may include the termination of the staff member's employment contract.
- The use of unauthorized software (including games) may also expose systems to the threat of serious virus attack.
- Staff members shall undertake that he/she shall abide by the organization's policy on software protection, namely:
    - Use of the computer software only in accordance with the applicable license agreement;
    - Only use software approved for use within Fourd;
    - no downloading or uploading of unauthorized software or files over the internet;
    - Abide by the organization's policies on the use of anti-virus software, and shall not load games or malicious software onto Fourd's end user systems;
    - Raise any doubts concerning the use or duplication of any given software with the Technical Head; and
    - Notify the Technical Head promptly of any misuse of software related documentation which comes to the staff member's notice.

This ensures the integrity of operational systems and prevent exploitation of technical vulnerabilities.

18.0 Network access controls

18.1 Network Security

Networks and network devices are secured, managed, and controlled by Fourd to protect information in systems and applications. This includes implementing firewalls, intrusion detection and prevention systems, and access control mechanisms. Network traffic is monitored and anomalous behavior is investigated promptly. Regular vulnerability assessments and penetration testing are conducted to identify and address potential weaknesses. Network devices are configured securely and access to them is restricted to authorized personnel only. Network logs are produced, stored, protected, and analyzed to identify security incidents and track network activity.

- Any single weakness in one portion of the network can create vulnerabilities that can be exploited to attack or access some other resource elsewhere on the network. Hence,

Network Security is very important and aims to secure every Server, PC, cloud and all other devices on the network.

- Following network controls should be considered:
    - Permissions need to be obtained before installing any networking equipment like gateways and routers.
    - No leased line or ISDN connection to any external network including the Internet should be installed without appropriate approvals.
    - Where such connections are made, or exist, adequate security measures should be taken in consultation with the ISSM/ CISO
    - Access to public networks from Fourd's systems and networks should only be by approved routes.
    - Responsibilities for the management of remote equipment (including in user areas) should be established.
    - Computer and network management should be co-ordinated so that security measures are consistently applied across the IT infrastructure.
    - Network security policies must be followed for connecting to Fourd networks by remote systems.
    - The use of a personal firewall on the laptop is recommended. The support personnel should arrange for installation and configuring of the firewall, taking guidance from administrators where necessary.
    - ISSO should ensure that the VPN permissions for remote users are suitably restricted using the features in the operating system of the server. Only those services that are strictly required should be enabled.
    - Only a hardened and vetted hardware / software should be deployed by the Portfolio Managers. During the hardening process, Portfolio Managers should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments/software
    - All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

External Network Connectivity

- The organisation's computers or networks should be connected to third party computers or networks only after approval from ISSO.

- Employees and vendors working for the organisation should not make arrangements for, or actually complete the installation of voice or data lines with any carrier, unless they have first obtained written approval from the ISSM.
- Remote access to the organisation's computers should be granted only to those users who have a demonstrable business need for such access. The ISSM should approve such remote access. IT Team should keep a record of such remote accesses granted, the method of access and the security measures enabled. Changes in remote access should also be periodically notified.

Third Party Access

- All third-party access to Fourd network should be approved by the ISSM.
- These third parties include information providers such as hardware & software vendors, business partners such as suppliers or agents, as well as contractors and consultants/ freelancers working on special projects.
- Access privileges for third party users should be enabled only for the time required to accomplish previously defined and approved tasks.
- It should be ensured that any third party, who needs to access the organisation's IT infrastructure, should secure its own connected systems in a manner consistent with the organisation's requirements and make the same available for audit and verification.

This protects information in networks and its supporting information processing facilities from compromise via the network.

18.2 Security of network services

- Security features, service levels, and management requirements of all network services shall be identified and included in a network services agreement.
- The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored. Where feasible, the right to audit should be agreed between Fourd and the provider.
- Fourd should also consider third-party attestations provided by service providers to demonstrate they maintain appropriate security measures

Rules on the use of networks and network services shall be formulated and implemented to cover:

- the networks and network services which are allowed to be accessed;
- authentication requirements for accessing various network services;
- authorization procedures for determining who is allowed to access which networks and networked services

- network management and technological controls and procedures to protect access
- the means used to access networks
- time, location and other attributes

Key security considerations by Fourd for networks and network services shall include:

- Technology applied such as authentication, encryption and network connection controls
- Technical parameters for secure connection
- Caching, in line with security, availability and confidentiality requirements
- Network service usage access restrictions

18.3 Segregation of networks

- The sensitivity of each information-processing asset should be analysed. Depending on the sensitivity, the computing environment should be considered for isolation.
- Systems that have highly sensitive information should be isolated logically, especially when client agreements require such isolation. They should be segregated using Virtual LANs (VLANs).
- Separate VLANs shall be established for each of the following groups:
    - Wi-fi devices
    - Guest users
    - Internal LAN
- Customer specific environments should also be considered for such isolation based on business needs.
- Wherever possible, areas handling highly sensitive information should be isolated physically too.
- VPCs are to also be enabled on the Cloud Environment and VPCs which are region specific shall be created to deploy instances. Security groups and subnets shall be created for the VPCs deployed

This splits the network in security boundaries and to control traffic between them based on business needs.

18.4 Web filtering

Access to external websites is managed by Fourd to reduce exposure to malicious content via Firewall and Defender for endpoint.

- The Web URL Filter application shall restrict, monitor, and log Internet usage of users on the Network.

- The Web URL Filter shall assign web sites to one of several predefined categories.
- Exceptions shall be granted upon request, based upon work requirements as per formal approvals. Accounts that are granted exceptions may be subject to elevated monitoring and additional security controls to protect organization's resources.
- Dynamic DNS: Sites that provide and/or utilize dynamic DNS services to associate itself with multiple IP's shall be restricted through firewall or filtering tool.
- Sites that provide access to or clients for peer-to-peer sharing of torrents, download programs, media files, or other software applications shall be restricted.
- User awareness training on phishing attacks is conducted periodically.

This protects systems from being compromised by malware and to prevent access to unauthorized web resources.

19.0 Encryption

19.1 Use of cryptography

This control ensures the proper and effective use of cryptography to protect the confidentiality, authenticity, and integrity of information.

a) It considers business requirements, information security needs, and legal, statutory, regulatory, and contractual aspects related to cryptography.

20.0 Change Management

The policy of Fourd is to ensure:

a) All requests to modify an IT service or the underlying technical infrastructure are done through a formal procedure and approved by CEO/CISO, wherever necessary.

b) All requests to modify a Non IT infrastructure service are done through a formal procedure and approved by CEO/CISO, wherever necessary

c) CEO/CISO shall ensure that all security related risks are properly identified and mitigated by including the Information Security Steering Committee in their Change Management process and procedures if it is found to be necessary. This is primarily applicable for all planned changes.

d) CISO/ISSM communicates to all affected parties of the risk and impact of all change requests.

e) ISSM defines and IT documents procedures to address emergency change requests, including authority for authorizing such requests.

f) Wherever possible, changes are developed and tested in an environment separate from production environment.

g) All changes to IT services are approved by the process owners prior to implementation into the production environment whenever possible.

h) Backups of configuration, application, and data are performed, to the thoroughness warranted by the identified risk of the change request, to restore the IT service to its previous functional condition, if it is found to be necessary.

For every change request, ISSM identifies any supplemental training requirements for IT personnel and end-users of the IT service. ISSM ensures IT personnel are adequately trained to support the affected IT service, or the underlying technical infrastructure. ISSM forward end-user training recommendations to CISO, if it is found to be necessary

21.0 Asset Management

The policy of Fourd is to ensure that:

1. CEO has approval authority for the procurement/renting of all assets and services, and approval must be granted prior to procurement.
2. Sourcing agreements for IT assets and services are approved by Administration Manager. A copy of every such agreement is maintained by Administration Team.
3. Any miscellaneous assets should be purchased only after getting CEO approval.
4. ISSM ensures that assets meet all applicable security requirements throughout their service life.
5. New products or services are introduced in conformity with the Change Management policy.
6. Inventory of all assets is maintained along with their ownership assigned to each of the newly introduced asset maintained by office Admin.
7. All assets are labelled as per the asset labelling procedure.
8. A formal disposal procedure is used for assets that have exceeded their usefulness and are deemed no longer necessary for corporate use (Refer Information security procedures for more details)
9. The disposal process shall address the removal of corporate information from the asset.
10. ISSO is the approval for Management Software Licencing.

22.0 Privilege Management Policy

a) The privileges associated with each system product like Server, application systems and the peripherals like printers, scanners etc, and the categories of staff to which they need to be allocated shall be identified.

b) Privileges shall be allocated to individuals on a need-to-basis and on event-by-event basis.

c) An authorization process and a record of all privileges allocated shall be maintained with respect to each user. Privileges shall not be granted until the authorization process is complete.

d) Special system privileges such as the default ability to access the files of any other users must be restricted to those directly responsible for systems administration and/or systems security. An exception to this standard can be made only if a department head and CISO has approved the exception in writing.

e) Systems administrators must perform configuration changes, operating system changes, and related activities that require "administrative" privileges.

- Department Head should share administrative privilege detail with ISSM and CISO.
- On termination or change in IT contract, the CISO shall insist the new Department Head to change all the previous privilege details and changed privilege details shall be shared with CISO and ISSM.

f) Special system privileges need to be re-authorized or eliminated for end users at least annually for Fourd employees, and at least every 6 months for all others.

g) Default user permissions must not allow access to all users.

h) When a user fails to provide a valid User ID or password, the system must not disclose which was invalid.

i) Application access (Eg. Tally) would be given / restricted to the registered owners only. Custodians of various software systems have all the authority to grant/revoke access to the system/application access privileges to the end users.

j) Request to IT help desk, in case the user is locked out/forgot the password should be made through the Team leader/Manager or in exceptional case at least by confirmed colleague either by mail, by calling the designated helpdesk phone numbers or by logging a request on the helpdesk self service application. IT help desk shall log the transaction and issue a new password to the user.

23.0 Capacity and Availability Management

The policy of Fourd is to ensure:

a) All services required for the normal execution of business processes or supporting the achievement of strategic business objectives are governed by the Capacity and Availability Management policy.

b) Information Security Organization defines the capacity and availability requirements of each service, identified by the Process Owners as required for normal business

operation or supporting the achievement of strategic business objectives, reflecting both current and future business requirements and with consensus of the process owners.

c) IT team document, maintain and review the capacity and availability requirements of each service identified. This shall be done with the help of monitoring tools.

d) ISSO allocates sufficient resources to meet, or exceed, the capacity and availability commitments of each service identified if require ISSO will get approval from CEO.

e) IT team reports to Process Owners and ISSM on measured capacity and availability proactively.

f) CISO & ISSM remediates deficiencies in measured capacity and availability.

g) Tool will initiate, if it goes beyond 90 % will alert all critical devices.

h) End user will inform if the capacity of their system not good to system administrator he will check and update if required based on approval from ISSO.

24.0 Email & Internet Usage

The policy of Fourd is to ensure the appropriate protection of Fourd's information transmitted over the Internet and through emails.

(a) Company employees are encouraged to use the Internet responsibly and productively.

(b) All Internet data that is composed, transmitted and/or received by Fourd's computer systems is considered to belong to Fourd and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

(c) The equipment, services and technology used to access the Internet are the property of Fourd and the company reserves the right to monitor Internet traffic and access data that is composed, sent or received through its online connections.

(d) All sites and downloads may be monitored and/or blocked by Fourd if they are deemed to be harmful and/or not considered to be valuable/productive to the business.

(e) Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images by Enabling DLP in monitoring mode.

(f) It is also strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If anyone receives an e-mail of this nature, they must promptly notify their reporting manager / ISSM.

(g) Sending confidential information by e-mail is sensitive and shall be protected by applying suitable controls.

(h) Emails transfer through encrypted path like TLS.

(i) It is mandatory to add disclaimers to each outgoing mail. It shall be as follows:

"This e-mail, together with any attachments, is confidential. It may be read, copied and used only by the intended recipient. Access to this e-mail or any of its attachments by anyone else and disclosure or copying of its contents is unauthorized. If you have received this email by mistake, please notify the sender immediately by e-mail or telephone. Please then delete it from your computer without making any copies or disclosing it to any other person. Emails are not secure and may suffer errors, viruses, delay, interception and amendment. Fourth dimension technologies pvt ltd does not accept liability for any damage caused by the transmission of this email".

Unacceptable use of the Internet by employees includes, but is not limited to the following:

a) Access to sites that contain obscene, hateful, pornographic, unlawful, violent, or otherwise illegal material can filter/Block using firewall or AV.

b) Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Fourd' email service.

c) Using computers to perpetrate any form of fraud, and/or software, film, or music piracy.

d) Stealing, using, or disclosing someone else's password without authorization.

e) Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization.

f) Sharing confidential material, trade secrets, or proprietary information outside of the organization.

g) Hacking into unauthorized websites.

h) Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.

i) Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.

j) Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

k) Passing off personal views as representing those of the organization.

l) Electronic Messaging Device (EMD) includes Personal computers, electronic mail systems, voice mail systems, electronic bulletin boards, Internet services, mobile data/digital terminals, and facsimile transmissions.

m) EMD's are designed and intended for conducting business of Fourd and are restricted to that purpose.

n) Transmission of electronic messages and information on communications media shall be treated with the same degree of propriety and professionalism as official written correspondence.

o) Confidential, proprietary or sensitive information may be disseminated only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained.

p) No employee shall access any file or database unless they have a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

q) Unless authorized by the ISSO, employees shall not install any file, software, or other materials without System Administrator approval.

r) Employees shall not download any executable file, software or other materials from the Internet or other external sources other without ISSO approval. If any employee is uncertain whether or not a file is executable, they should contact the ISSO team for guidance.

s) The size of file which can be attached to the email is restricted to 10MB.

t) Employees shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

u) Employees shall observe copyright restrictions of any documents sent through or stored on electronic mail

25.0 Mobile Device Policy

The policy of Fourd is to ensure that all the Laptops/mobile devices and the information on those systems shall be protected from theft, mishandling and environmental threats.

a) The physical and logical controls that are available within Fourd environment are not automatically available when working outside of that environment. There is an increased risk of information being subject to loss or unauthorized access. Mobile Device users shall take special measures (as per the guidelines given to them during the awareness sessions) to protect sensitive information in these circumstances.

b) Removal off-site of Fourd' information assets, on laptops or other mobile devices, must be properly authorized by the responsible information owner and ISSM.

c) Staff accessing information systems remotely to support business activities must be authorized to do so by the responsible information owner and ISSM.

d) Sensitive data stored on laptops and other mobile storage devices should be kept to a minimum to reduce risk and impact should a breach of security occur.

e) Loss of any mobile device containing sensitive data, or any other security breach, should be reported immediately to IT /ISSM.

f) Laptops and home personal computers should not be used for business activities without appropriate security measures, including up to date security “patches” and virus protection.

g) Sensitive information held on any mobile device must be securely erased before the device is reassigned to another user or to another purpose.

h) All the critical information contained in the laptop shall be backed up periodically with the help of IT as per the backup policy.

26.0 Backup and Retention

The policy of Fourd is to ensure:

a) Data backup rotation strategy and data archival retention periods are documented and validated with the process owners of each business unit and respect business or contractual data retention requirements.

b) Backup operations shall be performed regularly in accordance with business, legal, regulatory, and contractual requirements and as per the agreed backup plan.

c) Backup restoration exercises are defined and are performed regularly to validate the integrity of the backed-up data from the backup media without risk to the data or business operations.

d) Review of backup logs is performed daily to verify the successful completion of backup and/or restore operations.

27.0 Data Centre Management

The policy of Fourd (Co-located) is to ensure.

a) Data Centre physical location and design of the computing facility limits its vulnerability to environmental threats.

b) Data Centre has suitable environment and physical controls which are monitored and regulated.

c) A controlled entry system is installed for doors entering and exiting the Data Centre.

d) Access to the Data Centre is limited to personnel that have a need and right of access. Rights of access are granted by the CISO.

e) A Separate register shall be kept as an audit trail to track for third party visits to the Data Centre.

f) Periodic Detailed Cleaning of Data Centre equipment is performed to reduce risk of equipment failure.

g) Separate UPS is used for power supply to the data centre resources.

h) Data Centre is air conditioned, and the temperature is monitored regularly.

The policy of Fourd (Co-located & On-Prim) is to ensure

a) A controlled entry system is installed for doors entering and exiting the Data Centre.

b) Access to the Data Centre is limited to personnel that have a need and right of access. Rights of access are granted by the ISSO/CISO.

c) A Separate register shall be kept as an audit trail to track for third party visits to the Data Centre.

28.0 Patch Management Policy

The policy of Fourd is to ensure:

a) All the servers /devices are updated with latest security patches.

b) Mechanisms to detect systems with missing patches.

c) All the necessary updates are assessed and acquired from the respective vendors.

d) Patches are deployed successfully without affecting the systems.

e) Necessary rollback or backup restore plan is employed if needed.

29.0 Antivirus Policy

The policy of Fourd is to ensure:

a) The most current available version of the anti-virus software package will be taken as the default standard.

b) Automatic update features will be installed on all newly installed systems.

c) All systems attached to the Fourd network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

d) Any activities with the intention to create and/or distribute malicious programs onto the network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

e) If an employee receives any malicious content, or suspects that a computer is infected with virus, it must be reported to the IT/ISSM immediately.

f) No employee attempts to destroy or remove a virus, or any evidence of that virus, without direction from the IT department/ ISSM.

g) Any virus-infected computer will be removed from the network until it is verified as virus-free.

30.0 Technical vulnerability management

30.1 Capacity management

- Projections of future capacity needs should be made **at least once a year**, or whenever a significant systems change is planned or occurs. These should include new system requirements as well as projected trends in computer and network use of current systems. These shall be documented in a Capacity Management Plan document
- Monitoring and trend analyses of the utilisation of key system resources (physical) **must be performed at least quarterly as part of the Capacity Management plan review**. This should include:
    - Processors and End User Systems Memory Utilization
    - Main Servers Storage
    - File storage and Network Capacity
    - Communications Systems
    - Licenses for software
    - Human Resources
    - Software Handling Capabilities
        - Checking analysis of processing utilisation for business applications and MIS tools must be performed **at least once a quarter**.

References: *Capacity Management Plan*

This ensures the required capacity of information processing facilities, human resources, offices and other facilities.

30.2 Configuration Management

a) Keep the number of users with administrator privileges to a minimum.
b) Disable any unused or unnecessary identities.

c) Closely monitor access to maintenance programs, utility applications and internal settings.
d) Ensure that clocks are synchronised like NTP in order to log configuration correctly and assist in any future investigations.
e) Immediately change any default passwords or default security settings that are supplied with any device, service or application.
f) Implement a default logoff period for any devices, systems or applications that have been left dormant for a specified period of time.
g) Ensure that all licensing requirements have been met.

30.3 Management of technical vulnerabilities

- A Vulnerability Assessment Scan (VAPT) for Critical devices and server shall be run on all the networked by the CISO / System Administrator at least once in year. Such vulnerability scans shall be scheduled to be done during non-peak hours and shall be done in consultation with the Technical Head and end user departments.
- Vulnerability Assessments and Penetration Test will be done internally by Fourd.
- The Vulnerability Assessment and Penetration Test Reports shall be reviewed and summarised by the ISSC. The summary shall identify all critical vulnerabilities and the recommendations for fixing the same. The ISSC shall review the recommendations and approve the proposed actions.
- A timeline and closure plan shall be set for implementing the said recommendations. If a patch is proposed to be installed to fix vulnerability, the risks associated with installing the patch shall be assessed.
- The patches shall be tested and evaluated before they are installed to ensure they are effective.
- A proper record of all vulnerability scans run and actions taken shall be maintained.

Refer:4.9 Management of technical vulnerabilities in procedure (A5.37 Documented operating procedures v1.1)

30.4 Protection against malware

- With extensive connectivity across networks within the organisation and the internet, the proliferation and propagation of viruses is a real cause of concern and needs to be addressed with stern measures.
- ISSO should evaluate and approve the antivirus software which should be used by the organisation.
- Virus checking systems approved by the ISSO should be in place on all personal computers, laptops and servers.

- The entire antivirus solution should be set up in such a way that the latest versions of the antivirus software are automatically updated on every server and end user system from a designated antivirus server.
- The default settings of the antivirus software should be configured to offer adequate security to detect all viruses /worms at the immediate point of entry.
- Detective scans should also be undertaken / scheduled at predetermined intervals automatically.
- Frequent reviews of the software and data content of systems supporting critical business processes should be conducted and the presence of any spurious files or unauthorised amendments formally investigated.
- Where executable code is exchanged, or downloaded by data networks, protection from virus infection should be provided. (This includes electronic mail attachments.)
- PC and workstation users should be informed of their responsibilities, liabilities, and good practice for virus prevention, including checking devices of uncertain or unauthorised origin for viruses before use.
- Users are not authorised to turn off or disable virus-checking systems. No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.
- System administrators should ensure that the anti-virus software is updated daily.
- User possession or development of viruses or other malicious software is prohibited.
- All laptops, and servers within scope must have a standard antivirus solution installed, which must remain operational real time and adherent to configuration directives specified in related global antivirus procedure documentation as appropriate for the operating system.
- Full Anti-virus scans must be scheduled once per week on all user-controlled workstations, servers and cloud.
- All network attached storage devices within scope must have all applicable content scanned by a compliant antivirus solution before or during file creation or modification.
- All email traffic processed by Fourd must be scanned with email anti-virus solutions that adhere to specifications present in related antivirus procedure documentation.

- Fourd's users shall use only licensed and approved software for all business purposes and any unlicensed downloads shall be detected by the anti-virus solution.

This ensures information and other associated assets are protected against malware.

31.0 Privacy controls

31.1 Information Deletion

a) Ensure that deletion extends to temporary files, cached information, copies of data and legacy versions.
b) Consider using specialised deletion utility applications to minimise risk.
c) Only contract out to certified, verifiable deletion specialists, if the need arises to use a third-part service.
d) Implement physical deletion measures that are appropriate to the device in question (e.g. degaussing magnetic storage media, restoring factory settings on a smartphone or physical destruction).
e) Ensure that cloud service providers are aligned with the organisation's own deletion requirements.

31.2 Data masking

- The organization shall consider hiding of PII data by using techniques such as data masking, pseudonymization or anonymization.
- When using pseudonymization or anonymization techniques, it shall be verified that data has been adequately pseudonymized or anonymized.
- Pseudonymization shall be configured by a secret key so that only the authorized people have access to and pseudonymize PII, thus denying access to external attackers.
- Fourd shall also follow various other techniques such as encryption, masking, deletion of characters, substitution, and hashing.
- Legal requirements, if any on data masking or redacting shall also be considered
- PII in resource identifiers and their attributes [e.g. file names, uniform resource locators (URLs)] should be either avoided or appropriately anonymized

31.3 Data Leakage Prevention

a) Classify data in line with recognised industry standards (PII, commercial data, product information), in order to assign varying risk levels across the board.
b) Closely monitor known data channels that are heavily utilised and prone to leakage (e.g. emails, internal and external file transfers, USB devices).

c) Take proactive measures to prevent data from being leaked (e.g. robust file permissions and adequate authorisation techniques).

d) Restrict a user's ability to copy and paste data (where applicable) to and from specific platforms and systems.

e) Mass storage devices like USB allowed based on approval (Media handling procedure can be followed)

f) Require authorisation from the data owner prior to any mass exports being carried out.

g) Consider managing or preventing users from taking screenshots or photographing monitors that display protected data types.

h) Encrypt backups that contain sensitive information.

i) Formulate gateway security measures and leakage prevention measures that safeguard against external factors such as (but not limited to) industrial espionage, sabotage, commercial interference, and/or IP theft.

j) Use strong encryption for data transfer (Email, file transfer).

32.0 Protection of information systems during audit testing

- Audit requirements, scope and schedules should be carefully planned to avoid disruptions and to ensure effective coverage, as part of audit agreements.
- The methodology and tools adopted by audit staff should not compromise security.
- Auditors should have 'read only' access to data and where it is not read-only, it is to be isolated from the main data set
- Audit tests that may be run and affect system availability are to be ensured only outside of business working or peak hours.
- All procedures and work done by the auditors should be documented by them.
- Audit reports should be submitted to the management of Fourd.
- Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.
- Monitoring and logging of such audits is to be done by Fourd (audit trails, activities track etc.)

33.0 Backup and Redundancy

33.1 Information backup

Backup copies of information, software, and systems are being regularly maintained and tested in accordance with the agreed relevant policy on backup at Fourd.

- Backups of the following types of files shall be taken regularly and retained securely:
- Data files
- Firewall and router configuration and rules files
- Operating system configuration files of critical servers and applications
- Backed up files shall be checked periodically for retrieval / restoration;
- The backup media shall be stored in a secure environment.
- Periodicity of the backup shall in general be based upon the criticality of the data.
- Check for data and software integrity by using techniques such as checksums on files or comparison of current files against backup files, where numbers are involved.
- Backups of critical files shall be stored at a remote location or cloud to escape any damage from a disaster at the main site.
- The data backup procedure followed should provide for highest security levels so that all data that leaves the production system is authorized, tracked and logged.
- Backup Restoration Test shall be conducted and documented for the application data, cloud and other critical applications and network configurations; and the same shall be documented.
- A Backup Register with details of backup taken along with approvals and status of backups (success, failure etc.) shall be maintained for applications, cloud servers, support applications, email backups, network file backups etc.

33.2 Redundancy of information processing facilities

- Information processing facilities shall be monitored, and sufficient redundancy shall be ensured by fixing the appropriate threshold level and tracking against it.
- Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
- The Information Owners shall identify business requirements for the availability of information systems.
- Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered.

- Where applicable, redundant information systems shall be tested to ensure the failover from one component to another component works as intended.
- Planning and management of the day-to-day activities are required to ensure the availability and capacity of the resources that provide information services.
- For critical systems, additional requirements shall be defined and documented.
- Controls for operations include documented processes, employee duties, and formal methods to implement changes to facilities shall be enforced.

Fall back requirements (redundancies) and procedures should consider the following aspects:

  - Fall-back requirements must be specified by Information Owners.
  - Information Custodians must be made responsible for the establishment of fall-back arrangements for each IT service.
  - Fall-back requirements for individual business applications must be integrated into an overall business continuity planning process.
  - Information Custodians must co-ordinate fall-back requirements for shared services so that each service is provided for.
  - Fall-back facilities and procedures must be tested at least once a year to an appropriate level.

- In case of power failure, arrangements should exist for automatic switchover to alternate power line.
- In case of system failure, Technical Head / System Administrator should ensure the affected component is made operational or in case rectification is not possible within reasonable time alternate equipment should be identified.
- Fourd shall define resumption procedures defining actions to be taken to return to normal full business operations at the original site when any disaster occurs, as part of its BCP-DR plan.

This ensures the continuous operation of information processing facilities.

34.0 Physical controls

34.1. Secure areas

34.1.1 Physical security perimeters

Fourd has defined security perimeters to protect areas that contain information and other associated assets. The security perimeters have been implemented and are currently being used by the organization. The perimeters have been defined based on the sensitivity and classification of the information and assets they protect, and access controls have been implemented accordingly. The perimeters are regularly reviewed and updated as necessary to ensure that they continue to effectively protect the organization's information and assets.

- The security perimeter should define a site, building, computer room, locked office, or some other form of physical boundary.
- Smaller work places shall be housed as a part of a larger building wherever possible. It should be adequately secured with doors and locking mechanisms.
- Support functions and equipment, e.g., photocopiers and fax machines, should be sited to minimize the risks of unauthorized access to secure areas or of compromise of sensitive information.
- Secure areas must be physically locked when vacated and should be checked periodically.
- External personnel supplying or maintaining support services should be granted access to secure areas only when required and authorized.
- Access control device shall be installed at the entry into the development centre. Only employees with access control cards or registered biometrics can enter the facility by using the access cards or biometric authentication, while third parties shall be allowed entry into on the basis of prior request / approval by employees of Fourd. All external personnel shall be accompanied by staff of Fourd during their stay on site.

This prevents unauthorized physical access, damage and interference to the organization’s information and other associated assets.

34.1.2 Physical entry

The degree of control that exists on entry and movement of personnel into and within the offices also should play a large role in ensuring the overall security of organisation’s information assets.

The following are the guidelines relating to physical security control:

- Fourd ’s facility shall be guarded by security personnel and monitored on a 24 x 7 x 365-day basis

- Additionally, the entry to work areas, server room and entry into secure work areas shall be monitored through CCTV cameras. Logs of CCTV cameras shall be retained for at least 30 days. CCTV logging devices shall be sited in secure areas.
- Based on risk assessment certain areas of the Fourd 's office, like the Server Room, designated secure work areas, should be restricted through secure locked rooms with access control devices like biometric or card-readers.
- Inspection of incoming and outgoing packages (e.g., bags, briefcases, boxes, laptop computers, etc.) should be conducted to ensure the unauthorized materials are not brought in or taken out of the work area or the Server Room.
- All correspondence and incoming materials shall be received and recorded in the Material Inward register by a dedicated admin staff.
- Access to sensitive information and information processing facilities (like server rooms, isolated project areas) should be controlled and restricted to authorized persons only.
- Access rights for secure areas and information should be regularly reviewed and updated.
- Employees have access to the office building campus only via company approved identification badges
- Employees have access to Fourd premises only via Fourd approved identification badges and a RIFD authentication.
- All employees are issued Identification badges which have to be carried with them at all times during their presence in office. Badges should be displayed prominently to the security guard at the time of entry.
- Access to office premises is restricted to employees who don't wear their badges to office. In the event an employee forgets to carry his/her badge to office, they have to contact their supervisor who will take an approval from an authorized supervisory person to grant exception access
- All meetings with visitors should preferably be conducted in appropriate meeting / conference rooms. As far as possible, meetings/ interviews are held in the registered office
- All Visitors as a rule should not be allowed to enter secure areas unless they are escorted by an authorized person after obtaining necessary approvals.
- Personnel and visitors are asked to declare their belongings like laptop computer, mobile phones, etc. before entering restricted premises. As applicable, the security or admin will verify to prevent removal of Fourd property from the building.

- All visitors should be instructed about the security requirements in the area and emergency procedures to be followed, based on requirement.
- Access rights should be revoked immediately for staff or contractors who leave the organisation or who no longer need access to secure areas.
- All access and list of authorized users is reviewed periodically and access is revoked upon termination or change of duties.
- Access into the secure work areas shall be logged using the access control devices. Such logs shall be reviewed periodically to check for any suspicious activity.
- When employees are terminated, it shall be ensured that they are deactivated from the access control devices.

34.1.3 Delivery and Loading Areas

- All incoming materials shall be registered when entering the site.
- All outgoing materials shall be accompanied by a gate pass (either returnable or non-returnable gate pass). List of returnable gate passes shall be reviewed at periodic intervals to ensure that the materials sent out do return to the company at specified timings.
- The reception shall be further protected by access-controlled doors for entry into the work areas.

This ensures only authorized physical access to the organization's information and other associated assets occurs.

34.1.4 Securing Offices rooms and facilities

Fourd has designed and implemented physical security measures for its offices, rooms, and facilities to ensure the protection of its assets. Appropriate controls such as access controls, surveillance systems, and alarms have been put in place to safeguard against unauthorized access and breaches. Regular maintenance and testing of these security measures are conducted to ensure their effectiveness and compliance with the organization's security policies and standards.

- Perimeters should be defined for all essential computing and Information Systems areas. Server rooms should be separate within the main building.
- Centralised computer systems should be located in dedicated accommodation with zoned controls.
- A list of employees who are authorised to enter the Server or Network Room should be maintained by the ISSO.

- Access to sensitive areas should be strictly controlled and limited to those who need it. Server and network rooms should be out of bounds to all except essential operations staff. All sensitive areas should be locked and access to them controlled and monitored.
- A Network/ Server Room Access Register should be maintained for tracking entry of all other personnel into the server room. Details of visitors should be recorded and accompanied in sensitive areas.
- Equipment should be visibly labelled with a unique serial number which shall identify the equipment in a fixed asset and/or inventory system.
- Backup files should be kept securely on and off-site, as applicable. Transit methods should guarantee equivalent levels of protection.
- Risks of computer premises or facilities being overlooked from insecure locations, internal or external, should be reviewed at least every six months by the ISSO.
- Inspection of incoming and outgoing packages when ever vendor / Guest
- Information processing facilities managed by Fourd should be physically separated from those managed by third parties.
- Doors and windows should be locked when unattended.
- The ISSO should carry out physical assets inventory check annually.
- Users should ensure that they are logged off from E-mail and network before a Service Engineer is allowed to work unattended on the PC.
- Detailed fire procedures, covering the server room area, should be established, communicated, and regularly tested.
- Sensitive data shall be physically stored in locked cabinets which can be opened only by the ISSO / CEO.

This prevents unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

34.1.5 Physical security monitoring

Premises are continuously monitored for unauthorized physical access by Fourd.

- The organization shall have adequate surveillance systems, which may include security guards, intruder alarms and video monitoring systems such as closed-circuit television etc
- The organization shall have adequate safety alarms and monitoring devices or systems configured in its premises

- The organization shall take into account local laws and PII legislations if applicable for monitoring and ensure that privacy of the individuals on the premises are factored in adequately while implementing the monitoring mechanisms.

34.1.6 Protecting against physical and environmental threats

Fourd has designed and implemented protection measures against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure. These measures include identifying potential threats and vulnerabilities, assessing risks, and implementing controls to mitigate them. Regular reviews and updates of these measures are conducted to ensure their effectiveness in protecting the organization's infrastructure.

- Smoke detectors shall be installed in the facility.
- Fire extinguishers of required type shall be kept near the equipment and employees shall be trained in their proper use.
- Mock fire tests and evacuation exercises should be conducted once a year.
- Server and network rooms should be air-conditioned and kept at reasonable temperatures as per the procedures.
- Environmental factors / settings should be monitored in the server and network room by the IT Team.
- Computer systems should be kept away from glass and elevated surfaces to mitigate the risk of earthquakes.
- IT Team shall ensure that spike busters are installed wherever necessary.
- UPS shall be properly grounded.
- Wherever necessary line filters shall be installed to control voltage spikes.

This prevents or reduces the consequences of events originating from physical and environmental threats.

34.1.7 Working in secure areas

- Secure areas include server and network rooms, information processing facilities dealing in confidential information (e.g., accounts, personnel etc), specially cordoned project areas and areas where confidential information assets are being stored.
- Employees working in secure areas should only be aware of the existence of the security controls in place on a need-to-know basis.
- A responsible Fourd employee should accompany service engineer or any visitor inside the server and network room. Unsupervised working in secured areas should be avoided.

- Third Party support services personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required. This access should be authorized and monitored.
- No service engineer, contractor should be allowed to work on a holiday or at a time when a responsible Fourd employee is not around.
- During normal office hours, when a service engineer is attending to an end user computer, his/her work needs to be monitored by either the user or a field engineer.
- Secure areas should be physically locked and periodically checked.

This protects information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

34.2 Equipment security

34.2.1 Clear desk and clear screen

- Sensitive or critical business information should be locked away, when not required, to protect it from any damage.
- Incoming and outgoing mail points and unattended fax, telex machines should be protected.
- Internal, confidential, or critical business information, e.g., on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or desk or other forms of security furniture) when not required, especially when the office is vacated or outside work hours.
- Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism when unattended and should be protected by key locks, passwords, or other controls when not in use.
- Whiteboards and other types of display are cleared or cleaned of confidential or critical information when no longer required.
- Unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented.
- Media containing confidential, internal or is deemed in other ways sensitive information should be removed from printers and photocopiers immediately.
- All desks and other workspaces should be sufficiently tidy at the end of each working day to permit the cleaning staff to perform their duties.
- Screen pop-ups and notifications, such as messaging and new email alerts, should be disabled during presentations, screen sharing or in public areas.

This reduces the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

34.2.2 Equipment siting and protection

Fourd has implemented the control for sited equipment security. The equipment is sited securely and protected to ensure the confidentiality, integrity, and availability of information. Measures have been taken to prevent unauthorized access, tampering, or damage to equipment, and to protect against environmental threats such as fire or flooding.

34.2.3 Servers and Network Devices room

The server and network room is a high security zone and should be protected. Access should be controlled through locked rooms secured by access devices and accessible to only specific named staff. Detailed guidelines for the operations in the server room should be followed.

- All servers/ racks should be located and installed in enclosed space that should be effectively secured by access control device. Where existing equipment is not installed in an enclosed space it should be monitored and moved to secure locations at the next upgrade of the infrastructure.
- Wherever the server has been provided with hardware keys these should not be left hanging on the server unless they are “Power On” keys. These keys should also be in same custody arrangements as for the server room.
- The server room design or the door panel should allow a view of servers from outside.
- The following should be arranged for the server room to ensure proper functioning:
  - Air-conditioning, maintenance of ambient temperatures, humidity and dust
  - UPS, proper earthing for power supply
  - Fire alarms
  - Rodent control, cladding for cables
- Stationary and other consumables must not be kept in the server room.
- The server and network room must be constructed with fire resistant materials, and it should be structurally stable to withstand the fire or environmental damage.
- Server room should not have any wooden or other type of inflammable material.
- Smoking is prohibited in the Server Room.

- Consumption of food and beverage is not permitted in the Server Room.
- Inflammable material such as paper should be stored away from the computer room and computer printouts within the computer room should be restricted to a minimum.
- Fire extinguishers and fire exits should be marked clearly.
- Periodic inspection of the fire protection system should be arranged.
- Proper training should be given to all staff members on the use of safety measures as discussed above.

34.2.4 Networking Equipment

- Physical security of switches, routers and hubs is very important. These should be enclosed and locked in racks. The keys of the racks should have same custody arrangements as for the server rooms.
- The racks containing switches, routers and hubs should be located inside the server and network room which is provided with electronically operated access control unit where the entries can be logged through proximity card.
- All necessary infrastructures like A/C, alternate power supply and UPS etc. as mentioned for servers should be ensured for networking equipment also.
- All connections should be properly numbered. A documented scheme to facilitate easy identification, trouble shooting, and maintenance should be adopted.
- Access to telecommunication equipment installed in open spaces should be controlled effectively.
- Equipment siting and protection parameters should ensure the safety from the following:
  - Fire
  - Smoke
  - Drink & Food
  - Lightning
  - Flood
  - Theft
  - Electromagnetic Radiation
  - Dust

- Environmental conditions should be monitored for conditions which could adversely affect the operation of information processing facilities
- The impact of disaster happening in nearby premises, e.g., fire in neighbouring building, should be considered and provided for.
- Emergency Evacuation plans and exits should be defined for the office space and building; and prominently displayed in strategic visible locations for employees to see.

This reduces the risks from physical and environmental threats, and from unauthorized access and damage.

34.2.5 Security of assets off-Premises

Fourd has established a system to protect off-site assets. The protection measures are implemented based on the nature of the asset and associated risks. The assets are secured using appropriate physical security measures, such as locked cabinets or safes. Access to off-site assets is restricted to authorized personnel only, and the assets are regularly monitored and inspected to ensure their security.

- The security requirements for equipment offsite should be clearly communicated to the person or agency in whose custody and care the equipment is kept.
- Equipment and media taken off the premises should not be left unattended in public places.
- Periodic verification by Fourd staff to ensure compliance with the security controls should be carried out at the offsite premise, if applicable.
- Manufacturers' instructions for protecting the equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields.
- Suitable controls should be applied by the employees for home working environments as appropriate as lockable cabinets, clear desk policy and access controls for computers.
- Adequate insurance cover should be in place to protect the equipment offsite.
- In case a loan system operates; a set of regulations for the loan of PC equipment should be established. These regulations should define the authorisation for the issue, custodianship and return of equipment.
- For PCs on loan, the authorisation paperwork should indicate the authority of the employee for custody of the equipment and must stress the liability of the employee-custodian for any abuse of the equipment or data or software stored on it.

This prevents loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

34.3 Storage media

34.3.1 Management of Removable Media

This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, Compact Flash, Memory Stick or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support any data storage function.
- PDAs, cell phone handsets or smart-phones with internal flash or hard drive-based memory that support any data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (Wi-Fi, WiMAX, IrDA, Bluetooth, among others) or wired network access.

34.3.2 Appropriate Usage Rules

- IT department reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. IT department shall engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, and clients at risk.
- By default, USB storage media access shall be blocked via the antivirus. Temporary Access shall be provided only during the onsite travel and will revert post the travel. Access shall be whitelisted for Management, HR, Finance, IT department.

- Prior to initial use on the corporate network or related infrastructure, all USB-related hardware and related software must be registered with IT department.
- End-users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet Fourd 's established enterprise IT security policy or standards.
- Fourd shall maintain a list of approved USB-based memory devices and related software applications and utilities. Devices that are not on this list may not be connected to corporate infrastructure.
- Employees using removable media and USB-related devices and related software for data storage, backup, transfer or any other action within Fourd 's technology infrastructure shall, without exception, use secure data management procedures. A simple password is insufficient. See Fourd's password policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All USB-based devices that are used for business interests must be pre-approved by the IT department and must employ reasonable physical security measures. End-users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices shall have installed whatever anti-virus and anti-malware software deemed necessary by Fourd 's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media shall be used, must be updated in accordance with existing company policy.
- All removable media shall be subject to quarantine upon return to the office before they can be fully utilized on enterprise infrastructure.
- Passwords and other confidential data as defined by Fourd's IT department are not to be stored on portable storage devices.
- End-users must apply new passwords every business/personal trip where company data is being utilized on USB-based memory devices.

- Any USB-based memory device that is being used to store Fourd's data must adhere to the authentication requirements of Fourd's IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by Fourd's IT department before any enterprise data-carrying memory can be connected to it.
- Employees, contractors, and temporary staff shall follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. A list of detailed data wiping procedures for flash memory shall be made available shortly.
- Fourd's IT department shall support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media. This applies even to devices already known to the IT department.
- Employees, contractors, and temporary staff shall make no modifications of any kind to company-owned and installed USB hardware or software without the express approval of Fourd 's IT department. This includes, but is not limited to, reconfiguration of USB ports.
- IT department may restrict the use of Universal Plug and Play on any client PCs that it deems to be particularly sensitive. IT also reserves the right to disable this feature on PCs used by employees in specific roles.
- IT department reserves the right to summarily ban the use of these devices at any time. IT department need not provide a reason for doing so, as protection of confidential data is the highest and only priority.
- IT department reserves the right to physically disable USB ports to limit physical and virtual access.
- IT department reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end-users to transfer data to and from specific resources on the enterprise network.
- IT department can and shall establish audit trails in all situations it feels merited. Such trails shall be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end-user agrees to and accepts that his or her access and/or connection to Fourd 's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been

compromised by external parties. In all cases, data protection remains Fourd 's highest priority.

- The end-user agrees to immediately report to his/her manager and Fourd's IS department any incident or suspected incidents of unauthorized data access, data loss and/or disclosure of company resources, databases, networks, etc.
- Fourdshall not reimburse employees if they choose to purchase their own USB-based memory devices.

34.3.3 Printing Equipment Usage Guidelines

- Employees should use the Fourd printer facilities with fore thought and discretion.
- Any bulk print outs (more than 50 pages) should only be taken after obtain prior approval from the manager. All such bulk print outs shall be collated and deposited at the library. Once they become part of library, all the rules applicable to the existing books shall be implied to these collections.
- All the printing activities shall be logged and reviewed to ensure appropriate usage.

34.4 Disposal of Media

Security controls should be defined and documented for the secure disposal of information including:

- Input documents (e.g. fax messages / telexes)
- Carbon paper
- Output reports
- Removable disks
- Program listings
- Test data
- System documentation
- Expired archives

- Means should be provided for the effective destruction or recycling of media which has contained sensitive information.
- Bagging and collection services for waste disposal should be secure.

- Third party waste disposal services should be regularly inspected or otherwise checked.
- Adequate records must be maintained for confidential waste disposal.
- There should be local disposal facilities readily available.
- Before sensitive media can be reused, the stored data shall be completely and thoroughly erased by either completely over writing or by formatting the media. This is especially important when media are to be passed on to third parties.

34.4.1 Physical Media Transfer

- There should be procedures for the labelling and handling of all sensitive or valuable input/output media.
- Receipt of client media containing data and other information should be recorded and opened only by persons authorised by CISO. Any evidence of tamper during transit should be immediately escalated to the CISO.
- There should be procedures for the maintenance of formal records of the authorised recipients of data and for the clear marking of all copies of data for the attention of the authorised recipient.
- There should be procedures for the confirmation of receipt of transmitted media, where appropriate.
- There should be procedures for keeping distribution to a minimum (on a need-to-know basis) and for the review and update of distribution lists and lists of authorised recipients. Frequency of review and update should be based on the sensitivity of the information, and, if undetermined, should be at least once a year.

This ensures only authorized disclosure, modification, removal or destruction of information on storage media.

34.4.2 Supporting utilities

Information processing facilities at Fourd have been protected from power failures and other disruptions caused by failures in supporting utilities. Appropriate measures have been implemented to ensure that critical facilities are supported by backup power supply systems and that contingency plans are in place to minimize the impact of any disruption. Regular tests

are carried out to ensure that the backup systems are functioning as expected, and any issues identified are addressed promptly to maintain the resiliency of the facilities.

- Servers, PCs and other equipment should be connected to UPS depending on need. The specifications of the UPS should be reviewed at least once a year for adequacy of capacity and to check for any gross over specification.
- UPS shall be backed up with diesel power generators to provide power in case of long duration power outages.
- An annual maintenance contract with an external agency should be in place in case in-house capabilities do not exist.
- Disposal of all UPS batteries should be as per guidelines of environment protection agencies. Suitable space should be earmarked for storage of batteries.
- Fourd shall build redundancies and arrange for internet service from two different ISPs to continue services in spite of a failure of any one ISP

This prevents loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

34.5 Cabling security

- Power and telecommunication lines in the information facilities should be underground. In case it is not feasible, alternate protection should be provided.
- The power wiring shall be reviewed every half year by a trained electrician to detect any instances of tampering. Such reviews shall include both physical meter testing and visual inspection of the lines. A formal report shall be obtained from the electrician and maintained for review of the IT Team.
- Network cabling should be protected from damage and unauthorised access.
- Power cables should be segregated from communication cables to prevent interference. Suitable protection should be provided to segregate these cables.

This prevents loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

34.5.1 Equipment maintenance

Fourd maintains and upkeeps the equipment's, appropriately to ensure availability, integrity and confidentiality of information.

- The devices, machinery and equipment related to environment protection shall be covered by maintenance contracts and periodically tested for functioning
- Manufacturers' instructions regarding the protection of the equipment should be observed.
- Only authorized maintenance personnel should carry out repairs and service equipment.
- Records should be kept for all suspected or actual faults and all corrective and preventive maintenance.
- Any loss of, or damage to, the equipment must be promptly reported to IT Department as soon as possible.
- Security controls should be applied to equipment sent offsite.

This prevents loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

34.5.2 Secure disposal or reuse of equipment

- Whenever a storage media containing sensitive information is damaged, the possibility of repair should be considered.
- All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Preferably damaged hard drives/ removable media and USBs no longer used should be destroyed or shredded.
- If required a risk assessment should be done to determine if the item should be destroyed, repaired or discarded.

This prevents loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

----------End of the Document----------