



FINEOTEX CHEMICAL LIMITED

INFORMATION SECURITY & MANAGEMENT POLICY

Adopted on

20th May, 2023

Policy on Information Security & Management Policy - 1

1. INTRODUCTION:

We at Fineotex Chemical Limited (FCL) recognizes that information is one of our most valuable assets belonging to our Operations & Business and which help us in maintaining integrity of information. The achievement of our business goals depend on our ability to safeguard the information we create or possess by ensuring its confidentiality, integrity and availability at all times.

This policy is an overall declaration by Fineotex Chemical Limited (FCL) of the security objectives and expectations, which will allow utilization of information and information systems for effective and efficient achievement of business goals. FCL is committed to establish and consistently improve cyber security processes and minimize exposure to risks. In continuation with our efforts, we have always strived to ensure best practices are being following within our organization and this policy is formalizing our expectations and practices.

The purpose of the Policy is to establish guidelines, responsibilities, and procedures to protect the confidentiality, integrity, and availability of information assets within the organization. This policy aims to ensure the secure handling of information, prevent unauthorized access or disclosure, and maintain compliance with relevant laws and regulations.

2. SCOPE AND APPLICABILITY:

This Information Security Policy applies to Company's all office locations and plants, including employees. Within the scope of applicability of this policy all assets such as, but not limited to, information systems, hardware (such as laptops), software, data, drawings and media in electronic form at the Company and third-party facilities are covered.

3. POLICY OBJECTIVE:

The primary objectives of the policies are as follows:

- a. **Protecting Confidentiality:** Safeguarding sensitive information from unauthorized access, disclosure, or modification.
- b. **Ensuring Integrity:** Maintaining the accuracy, completeness, and reliability of information assets.



- c. **Promoting Availability:** Ensuring timely and reliable access to information resources when needed.
- d. **Managing Risks:** Identifying, assessing, and managing information security risks effectively.
- e. **Compliance:** Ensuring compliance with applicable laws, regulations, and industry standards.
- f. **Security Awareness:** Promoting a culture of security awareness and accountability among employees.
- g. **Incident Response:** Establishing procedures for detecting, reporting, and responding to security incidents promptly.
- h. **Continual Improvement:** Regularly reviewing and enhancing the effectiveness of the information security management system.

4. DEFINITIONS:

- i) **Information:** Any communication or representation of knowledge such as facts, data, or opinions in any form, including textual, numerical, graphic, cartographic, narrative or audio visual
- ii) **Information Security:** Protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability
- iii) **Information Security Event:** An identified occurrence of a system, service or network state indicating a possible breach of information.
- iv) **Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information system processes, stores or transmits will constitute a violation or imminent threat of violation of security policies and security procedures
- v) **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of the likelihood of occurrence and the adverse impacts which would arise if the circumstance or event occurs
- vi) **Confidentiality:** Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information



- vii) **Integrity:** Safeguarding the accuracy and completeness of assets against unauthorized information modification or destruction which will ensure information authenticity
- viii) **Availability:** Ensuring timely and reliable access to and use of information
- ix) **Risk Management:** Coordinated activities to direct and control an organization with regard to risk
- x) **Risk Analysis:** Systematic use of information to identify sources and to estimate the risk

5. INFORMATION SECURITY PRINCIPLES:

The Information Security Policy will ensure:

- Consistently meeting expectations of all stakeholders (investors, suppliers, customers, and employees)
- Ensuring compliance with all applicable standards, regulatory and legal requirements
- Apply effective risk management framework to identify, manage and mitigate risks associated with FCL through undertaking a vulnerability assessment
- Protect all FCL information and assets from possible threats which could potentially disrupt the business and functioning of FCL
- A backup management system for creating copies of information which is essential to recover and restore original data in the event of data loss
- Consistently improve and upgrade technology, systems, and processes to protect FCL against known and unknown cyber security threats
- Implement incident management procedures for detecting, reporting, and responding to incident
- Effectively apply business continuity and disaster recovery management controls

6. COMPLIANCE TO THE POLICY:

Information security and cyber security are part of the employee performance evaluation as it assesses the employees and whether they are putting the organization at risk, intentionally or unintentionally. The information technology team regularly conducts violation checks on employees' laptops – including email violation, installation, and the use of prohibited software etc.



It is the responsibility of each employee to clearly understand and adhere to the Information Security Policy and in case of any violations to this policy, the Management reserves all rights to take disciplinary action, up to and including termination of employment.

7. REVIEW:

The Policy will be reviewed on periodic basis or in case of any significant changes to check for effectiveness, changes in technology and changes in risk levels that may have an impact on confidentiality, integrity and availability, legal and contractual requirements, and business efficiency.