INFORMATION SECURITY POLICY

Rev.	Date	Description	Prepared By	Checked By	Approved By
2.1	23.05.2025	Section 11.2 has been updated	Rahul Mishra	Gagan Arora	Vinod Sharma
2.0	07.08.2024	The name of the document is updated	Rahul Mishra	Gagan Arora	Vinod Sharma
1.0	17.01.2024	First Issue	IT Team	Gagan Arora	Vinod Sharma

TABLE OF CONTENTS

1.0 PURPOSE

1.1 The information security policy statement defines the rules and procedures for protecting the confidentiality, integrity, and availability of the organization's data and IT assets.

1.2 To provide IT infrastructure that would enable the users to identify opportunities, improve performance, and understand the business environment.

1.3 To develop and preserve information as a corporate resource and to offer infrastructure to ensure coherent access for users to complete, concise, and timely information.

2.0 APPLICABILITY

2.1 This document applies to all staff of Hero Future Energies Global Limited and its hold cos, subsidiaries, including step-down subsidiaries and joint ventures (collectively referred to herein as "HFE", "Company", "we", "us" or "our"). It is also applicable to all associates in the organization, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access time to services.

2.2 The document is available on HFE Intranet portal (Smartflow) and is shared with new hires during the induction program.

3.0 RESPONSIBILITY AND AUTHORITY

3.1 CISO has the primary responsibility to implement Information Security & Technology Framework, Policy, and Procedures to ensure compliance including but not limited to the following:

3.1.1 Establish and maintain a cyber security policy, framework, procedures, and guidelines across the organization monitor its adherence, and cyber security training, ensure compliance to regulations in respective geography, and coordinate for internal and external audits.

3.1.2 Ensure its policy and procedures shall be in line with the requirements of the local laws and regulations of the respective geography where the Company operates.

3.1.3 Identify prospective risks for the computing environment and take necessary mitigating actions.

3.1.4 Oversee forensic (investigations) of security breaches including suspected insider threats.

3.1.5 Work closely with various business units, legal & regulatory, information technology, business process teams, and DGC to provide regular updates on cyber security.

3.1.6 Ensure the appropriate Committee is in place to implement and oversee any such task as may be necessary for the efficient implementation of this policy.

3.1.7 Ensure policy statements shall be prepared in compliance with the applicable laws and regulations and placed on the Company website, wherever required.

3.2 All individuals, including employees, contractors, and affiliated third parties must ensure that they read, understand, and comply with this Policy at all times.

4.0 EFFECTIVE DATE

4.1 This Policy comes into force w.e.f. last review / approval date as mentioned in the version control

table and will be reviewed once in a year or if there is a major change.

5.0 ABBREVIATIONS

IT	Information Technology
HFE	Hero Future Energies
ISMS	Information Security Management System
DGC	Digital Governance Committee
CISO	Chief Information Security Officer
MoP	Ministry of Power
PDPA	Personal Data Protection Act
DSA	Digital Security Act
CERT-In	Computer Emergency Response Team – India

6.0 DEFINITIONS

Definition	Description
Information Security Management System (ISMS)	A structured approach designed to safeguard an organization's valuable information assets. It ensures the confidentiality, integrity, and availability of these assets.

7.0 POLICY STATEMENT

7.1 At HFE, the security of information assets is of paramount importance. Confidentiality, integrity, and availability of information assets shall always be maintained through controls that commensurate to the criticality of the assets and will be protected from all types of potential threats.

7.2 HFE will ensure IT compliance with all statutory, regulatory, and contractual requirements as per applicable laws.

7.3 HFE is committed to continuously adopting new technologies that enhance business and operational performance.

7.4 HFE is committed to create, maintain, and encourage a cyber security-conscious culture across the organization.

7.5 Personal data will be collected only for record-keeping purposes and protected against alteration, destruction, and loss to ensure integrity and confidentiality.

8.0 EXCEPTIONS TO THE POLICY

8.1 This Policy is intended to be a document of information security requirements that shall be complied with at all times. However, in particular circumstances, exceptions may be allowed with prior approval of the CISO, with proper justification and risk involved along with proper documentation. CISO shall also review all such exceptions and verify with risk closure evidence along with its mitigation controls.

9.0 TRAINING

9.1 Training on this policy forms part of the induction process for all individuals who work for the Company, and regular training will be provided as necessary.

10.0 BREACHES OF THIS POLICY

10.1 HFE will take all necessary measures and actions in case of any breach of this policy. Any employee of the organization found to have violated this policy will be subject to disciplinary action, up to and including termination of employment as the case may be.

11.0 CHANGES TO THIS POLICY

11.1 The policy does not form part of any employee's contract of employment. We reserve the right to change this policy at any time without notice.

11.2 This policy does not override any applicable national data privacy laws and regulations in the countries where the company operates.

INDIA

- Information Technology Act, 2000 (India) MoP India guidelines (India)
- CERT-IN guidelines (India)

SINGAPORE

- The Personal Data Protection Act (PDPA)

UNITED KINGDOM

- UK GDPR

VIETNAM

- Vietnam’s Law on Information Technology No. 67/2006/QH11

UKRAINE

- The law of Ukraine “On Protection of Personal Data” No. 2297-VI dated 01st June 2010

12.0 RELATED DOCUMENTS

Document Name
All related ISMS policies and procedures