HFCL Limited

Cyber Security Policy

Version 1.0

Sr. No.	Type of Information	Document Data
1	Document Title	HFCL Cyber Security Policy
2	Document Code	HFCL/CSP/2025/1039
3	Document File Name	1039_ HFCL Cyber Security Policy v1.0
4	Document Owner	ISMS & PIMS Steering Committee
5	Document Author(s)	ISMS & Privacy Team
6	Document Approver	CISO & DPO

Document Change History

Version Number	Reviewed by	Review Date	Approved By
1.0	**Mr. Sanjay Kumar Head - IT Operations & Compliance; Digital & IT**	**01-14-2025**	**Mr. Sunil Pandey Chief AI & Digital Officer, Digital & IT**

1. About the policy

This policy safeguards HFCL's information assets, including IT and Operational Technology (OT)/Industrial Control Systems (ICS)—to ensure confidentiality, integrity and availability across global operations. It integrates cyber risk governance at Board level, aligns incident reporting and privacy obligations with Indian law (DPDP Act 2023; IT Act 2000/CERT-In Directions) and embeds international best practices (ISO/IEC 27001:2022; COSO ERM; NIST SP 800-82r3; IEC 62443). The policy also addresses ESG-related data integrity risks and anti-greenwashing controls for sustainability disclosures and supply-chain compliance.

2. Objectives

The objective of a cybersecurity policy is to establish clear guidelines and practices for protecting an organization's digital assets, systems, and sensitive information from cyber threats. It aims to define roles and responsibilities, ensure the confidentiality, integrity, and availability of data, and mitigate potential risks through preventive and corrective measures. The policy sets standards for security protocols, incident response, and compliance with legal and regulatory requirements. It fosters a security-conscious culture, ensuring employees and stakeholders understand their responsibilities in safeguarding information. Ultimately, the policy seeks to minimize the impact of cyber incidents and protect the organization's reputation and assets.

3. Scope

This policy applies to:

- Applies to all HFCL employees, directors, contractors, third-party vendors, and value-chain partners who access, process or manage HFCL data or systems (IT, OT, cloud), in India and overseas. Covers data in digital and physical form; onsite and remote access; manufacturing plants, R&D, warehouses and field operations.
- Information assets across the organization, including data, software, hardware, and networks, both within India and overseas in digital and physical form; onsite of offsite.

4. Legal and Regulatory Compliance

The organization commits to compliance with the following key legal and regulatory frameworks:

- **ISO/IEC 27001:2022**:
  - ✓ The organization adheres to the principles of ISO/IEC 27001:2022, focusing on the establishment, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS).

- **Indian Cyber Laws (IT Act, 2000)**:
  - ✓ Compliance with the **Information Technology Act, 2000**, including **Section 43A** (reasonable security practices for data protection), **Section 66** (cybercrime), and **Section 79** (intermediary liability).
  - ✓ **CERT-In** regulations for incident reporting.

- **Digital Personal Data Protection (DPDP) Act, 2023**:
  - ✓ The organization adheres to the provisions of the **DPDP Act, 2023** concerning the collection, processing, and storage of personal data of Indian citizens.

- Ensuring user consent, transparency, and data security when handling personal data. **GDPR (General Data Protection Regulation)**

HFCL shall comply with the principles of data protection enumerated in the EU General Data Protection Regulation and ISO 27701:2019.

✓ **Lawfulness, fairness and transparency**

Personally, Identifiable information (PII) shall be processed lawfully, fairly and in a transparent manner in relation to the PII principal. Data we collect and process shall be fair, supported by a legal basis. PII shall only be collected for specific and legitimate purposes.

✓ **Purpose limitation**

Personally, Identifiable information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

✓ **Data minimisation**

Personally, Identifiable information collected and processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. HFCL shall use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII Principals, reduce the observability of their behaviour and limit the likability of the PII collected.

✓ **Accuracy**

Personally, Identifiable information collected and processed shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that the PII that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

✓ **Storage limitation.**

Personally, Identifiable information shall be kept in a form which permits identification of PII principals for no longer than is necessary for the purposes for which the such information is processed.

- ✓ **Integrity and confidentiality (security)**

  HFCL have an obligation to provide security for the data we collect from users. The level of security matches the sensitivity of the data being collected. PII, we hold shall be kept safe and secure. PII shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- ✓ **Individual participation and access**

  Every PII Principal has a right to receive confirmation from us about the PII we collect from or relating to the individual. If such PII exists, the PII Principal has the right to request and receive such PII in a timely manner and at a reasonable cost. Upon granting the request, we deliver the PII to the individual in a format that is intelligible to the PII Principal. If the request for the information is denied, PII Principal have the right to challenge the denial. Furthermore, if upon receipt of the data PII Principal determines that the data is incorrect, he/she has the right to have the data corrected, amended or deleted.

- ✓ **Privacy compliance**

  We ensure that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors. We have appropriate internal controls and independent supervision mechanisms in place that assure compliance with relevant privacy law/ regulations.

- ✓ **Accountability**

  We believe that processing of PII entails a duty of care and the adoption of concrete and practical measures for its protection.

5. CYBER SECURITY POLICY

a) Governance, Risk, and Compliance (GRC)

- Board & Committee Oversight: The Board delegates cyber risk oversight to the Risk Management Committee (RMC). The Risk Management Committee of the Company is constituted in line with the provisions of Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015. The roles and Responsibilities of the RMC include formulation of a detailed risk management policy which shall include a framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the RMC. The Audit Committee oversees the vigil mechanism and investigates cyber-fraud claims.

- Risk Appetite & COSO ERM Integration: Management shall define and annually review cyber/OT risk appetite and tolerance linked to strategic objectives. Enterprise risk assessments shall follow COSO ERM principles with an integrated portfolio view and performance reporting.
- Establishment of an **Information Security Governance Framework** that ensures alignment with business objectives and regulatory requirements.
- Conduction of **regular risk assessments** to identify threats, vulnerabilities, and risks to organizational assets, and prioritize them based on impact and likelihood.
- Ensuring compliance with relevant laws, regulations, standards (e.g., **ISO 27001:2022** and **NIST CSF**) through regular audits and assessments.
- Policies & Standards: ISMS policies shall be maintained for Access Control, Data Protection, Incident Response, Vendor Risk, OT/ICS Security, Secure Development/SBOM, and ESG Data Governance.
- Creation and maintenance of a **Cybersecurity Policy** to guide all organizational activities related to information security.

b) Asset Management

- Maintenance of an inventory of all IT assets, including hardware, software, and data, with classification levels indicating the sensitivity of the asset.
- Assignment of asset ownership to ensure accountability for the management and protection of each asset.
- Conducting periodic audit of asset inventories to ensure accuracy and update them whenever there is a change in infrastructure or technology.
- Secure disposal of old assets and data according to their classification and compliance requirements.

c) Access Control

- Enforcement of least privilege access by ensuring users and systems have the minimum level of access necessary for their roles.
- For all the users who need admin rights, the following procedure is followed:
    - ✓ Employees who need administrator rights must get approval from their Business Unit Heads and consult the IT Department.
    - ✓ A consent form must be signed to confirm that the user will not install unauthorized applications or use their domain ID without IT and Digital Department approval.
    - ✓ Violations of this policy will have legal consequences, and the user will be held responsible for any issues. The Digital and IT Departments will not be held liable.

- Performing **regular access reviews** to ensure that users' permissions are up-to-date and relevant to their current roles.
- Immediately **revoking access** when employees leave or change roles, or when third-party access is no longer required.
- Implemented **role-based access control (RBAC) and Zero Trust Model** to align user permissions with their job responsibilities. Every access request, whether internal or external, is verified, authorized, and continuously validated before being granted.

d) Data Security and Privacy

- Data is classified and labelled according to sensitivity, applying appropriate security controls to protect it.
- Ensured data encryption for sensitive data both at rest and in transit, using industry-standard encryption protocols (TLS v1.2 and above).
- Limited access to sensitive data based on the principle of least privilege is followed.
- Regular updating expired certificates, assuring that it is signed by a trusted authority for secure transmission of data.
- Pseudonymizing and anonymizing sensitive data where applicable to reduce exposure.

e) Network Security

- Deployment of firewalls at key entry and exit points to filter traffic and block unauthorized access.
- Implementation of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor and respond to malicious activity on the network.
- Using Virtual Private Networks (VPNs) to secure remote access and ensure the confidentiality of transmitted data.
- Segregation of networks based on sensitivity, ensuring that critical systems are isolated from less secure networks.
- Application of network segmentation and micro-segmentation to minimize lateral movement of attackers and restrict access to sensitive data.
- Monitoring network traffic and logs continuously for anomalous behaviour and DDoS attacks using network traffic analysis tools.
- Identifying and blocking the malicious IoA's (Indicators of Attack) and IoC's (Indicators of Compromise) identified from honeypot sensors to prevent the network.
- Regular evaluation and closing of **open ports** which are not required.
- Periodic conduction of network penetration testing to evaluate weakest links or loopholes present in the network.

f) Identity and Access Management (IAM)

- Implementation of a structured **IAM system** that manages user identities and access privileges across all organizational systems.

- Integration of IAM with **single sign-on (SSO)** to simplify access management **in critical company applications and portals**.
- Regularly conduction of review and **audit of user access logs** to detect and prevent unauthorized access or suspicious activities.

g) Security Monitoring and Incident Response

- Deployment of **Event Log Analyser** systems to collect, analyze, and correlate security data across all systems and networks.
- Implementation of **continuous monitoring** of all critical systems and networks for signs of intrusions or other security incidents.
- Establishment of an **Incident Response Plan (IRP)**, detailing how to respond to security incidents, including containment, eradication, and recovery.
- Implement **forensic capabilities** to investigate security incidents and identify their root causes.
- Define escalation procedures and establish **clear communication channels** during an incident.

h) Application Security

- Conduct code reviews and static code analysis to detect vulnerabilities early in the development process.
- Implementation of regular vulnerability assessments and penetration testing on all critical applications to identify and fix security weaknesses.
- Ensure that third-party libraries and software used within applications are secure and regularly updated.
- Application of input validation to prevent injection attacks (e.g., SQL, XSS).
- Use of security testing tools to perform automated security assessments on web applications.

i) Endpoint Security

- Installation and regular update of antivirus software and endpoint protection tools on all systems.
- Encrypting all endpoint devices that access sensitive data to ensure data security in case of device theft or loss.
- Reviewing and ensuring that backend update of security tools like antivirus is successful to the latest version in all the systems.
- Enforcement of device access controls, ensuring that only authorized devices can access the corporate network.
- Regularly updating all the systems with application of necessary patches.

j) Cloud Security

- Implementation of **cloud security controls** to define the boundaries of security responsibilities between the cloud provider and the organization, following a Shared Responsibility Model.
- **Encryption of data** stored in the cloud, both at rest and in transit, using strong encryption standards.
- Ensuring that **cloud configurations** (e.g., firewalls, IAM policies) are properly set up to prevent unauthorized access or misconfigurations.
- Implementing **cloud security monitoring** tools to detect and respond to any suspicious activity or data breaches within cloud environments.
- **Limiting cloud resource access** by enforcing least-privilege policies for all users and systems accessing cloud services.
- Regular conduction **cloud security** audits to ensure compliance with internal policies and regulatory requirements.

k) Physical and Environmental Security

- Restricting access to sensitive areas (e.g., data centers, server rooms) using physical security controls such as biometric authentication, badge access, or security guards.
- Implementation of video surveillance in critical areas to monitor access to physical resources.
- Ensuring environmental controls (e.g., fire suppression, HVAC systems, uninterruptible power supplies) are in place to protect physical assets from environmental hazards.
- Performing regular physical security audits to identify vulnerabilities and implement corrective actions as necessary.
- Implementation disposal protocols to securely destroy physical media, such as hard drives or printed materials, when they are no longer needed.

l) Business Continuity and Disaster Recovery

- **Development and Maintenance of a Business Continuity Plan (BCP):** The organization has maintained a comprehensive Business Continuity Plan (BCP) to ensure the continuation of essential operations during or after a disruption, such as natural disasters, cyber incidents, or pandemics. The BCP is regularly tested, updated, and aligned with organizational objectives.
- **Establishment of a Disaster Recovery Plan (DRP):** A detailed Disaster Recovery Plan (DRP) is established, outlining procedures for recovering critical systems and services in the event of major incidents such as cyberattacks, data breaches, system failures, or natural disasters. The DRP has clear definition of responsible teams, recovery objectives, and the existing resilience measures in place.
- **Regular Evaluation and Updates of BCP and DRP:** Both the BCP and DRP are evaluated through regular audits and updated periodically to incorporate lessons learned, new technologies, and emerging threats. These updates should apply the latest methodologies in business continuity and disaster recovery, ensuring the plans are effective and efficient.
- **Regular Backup and Secure Storage of Critical Data:** The security team ensures that **critical systems and data** are regularly backed up, and backup copies are securely stored in

multiple locations. These backups must be easily accessible for recovery and tested regularly to verify the effectiveness of the backup process.

- **Meeting Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO):** The security team ensures that business-critical functions can be restored within defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). These objectives should be established for each critical system and process, based on business requirements.
- **Development and Documentation of a Recovery Team Call Tree:** A comprehensive call tree for the recovery team is developed and documented. This includes all relevant contact information, roles, and responsibilities, ensuring that key personnel can be quickly mobilized in case of an incident or disaster.
- **Development of a Comprehensive Business Continuity Strategy:**
  A detailed Business Continuity Strategy has been developed, which includes:
  - ✓ **Emergency Management Procedures**: Procedures for immediate response during an emergency.
  - ✓ **Damage Assessment Procedures**: Defined protocols to assess the extent of the damage post-incident.
  - ✓ **Restoration of Data and Communications**: Strategies to restore data communication and processing in a timely manner.
  - ✓ **Critical Services Recovery**: Clearly defined actions to restore and prioritize critical business functions.

- **Classification of RTOs and RPOs Based on Disruption Type:** RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) is clearly defined and classified for different types of disruptions:
  - ✓ **Normal Disruption**: Minor disruptions where recovery efforts can be managed within routine operations.
  - ✓ **Crisis Disruption**: Major disruptions that require coordinated recovery efforts but are not catastrophic.
  - ✓ **Disaster Disruption**: Extreme disruptions that involve catastrophic system failures or external events, requiring an all-hands response and full recovery procedures.

- **Identification and Classification of Single Points of Failure:** The organization has proactively identified Single Points of Failure (SPOF) within critical operations and infrastructure. These are classified based on the potential disruption impact, both during normal working hours and outside of business hours, ensuring that backup processes are in place to mitigate such risks.

6. Security Awareness

- **Security Awareness Training:** All employees and users undergo regular security awareness training at the time of induction and had to give a security test to ensure they are equipped with the necessary cybersecurity knowledge. A comprehensive training is mandatory for all employees at our official Learning and Development Portal, annually.

- **Weekly Poster Circulation:** Weekly circulation of posters educating users about latest cybersecurity threats and preventive measures.

7. Vendor Security and Third-Party Management

- The security team ensures that third-party vendors meet appropriate cybersecurity standards through regular security assessments and audits.
- Vendor contracts will include security clauses, ensuring third parties protect sensitive data and report incidents as required.
- **Data Processing Agreements:**
    - For vendors handling personal data, the organization processes NDA and Data Processing Agreements (DPAs) that outline the obligations and security measures for protecting the data.

8. Social Media and Internet Usage / Acceptable Use

In our organization, internet and social media usage is strictly governed by established cybersecurity and acceptable use policies:

- Internet and social media usage is restricted to work-related activities and is enforced in line with organizational information security policies.
- Access to unauthorized, malicious, pornographic, or offensive websites is blocked through Forcepoint centralized content filtering and firewall rules.
- Employees are strictly prohibited from sharing or discussing any organizational data, internal communications, client information, or intellectual property on social media platforms.
- Limited personal use of the internet is permitted during break hours, provided it does not affect productivity or violate security controls.
- Use of external VPNs, proxy servers, or anonymizing tools to bypass network monitoring or access control mechanisms is not permitted under any circumstance.
- All internet and social media activities conducted over organizational assets are monitored and logged by the IT Security team. Logs are reviewed periodically to detect policy violations, in accordance with ISO/IEC 27001:2022 control A.5.2 and A.7.7

9. Disciplinary Action

Our organization follows a strict disciplinary framework to address cybersecurity policy violations:

- Any violation of the cybersecurity policy is subject to investigation by the Information Security department.

- Disciplinary actions are determined based on the severity of the offense, ranging from formal warnings to termination of employment.
- In cases involving data breaches, system misuse, or illegal activity, appropriate legal action will be initiated under applicable sections of the IT Act 2000, including Sections 43, 66, 66C, and 66E, and the IT (Amendment) Act 2008.
- Repeat offenders or those compromising sensitive data may be blacklisted from future employment within associated vendor ecosystems.
- The disciplinary process is documented and aligned with the organization's HR and legal frameworks to ensure fair and consistent enforcement.

10. USER RESPONSIBILITY

- Employees are accountable for any content posted using their credentials or corporate devices.
- Users must report any suspected cyber threats originating from social media or internet platforms to the IT Department or cybercell@hfcl.com immediately.

11. Grievance / Whistleblower Procedure for Cyber Threats & Data Breaches

a) **Immediate Reporting**: Any employee who suspects or becomes aware of a cyber threat, data breach, or misuse of credentials must immediately report the incident to the IT Security Team at **cybercell@hfcl.com** or through the internal ticketing system.

b) **Protection Against Retaliation**: HFCL ensures that no retaliatory action will be taken against any individual reporting in good faith, whether the report is substantiated or not.

c) **Investigation & Follow-up:** The IT Security and Compliance Teams will assess and investigate all reports within 48 hours, documenting evidence and coordinating with Legal and HR if required.

d) **Corrective Actions**: Upon confirmation of a threat or breach, appropriate technical and disciplinary actions will be taken in accordance with HFCL's various policies.

e) **Confidentiality**: All reports and whistle blower identities will be treated with the strictest confidentiality as per the Whistle Blower Policy – Vigil Mechanism of the Company to protect the integrity of the process.

12. Policy Updates

Our Cybersecurity Policy is a dynamic document maintained under a controlled change management process:

- The policy is reviewed on an annual basis, or earlier if mandated by regulatory changes, new threat intelligence, or audit observations.

- Updates are initiated by the Information Security Management Committee (ISMC) and approved by top management in line with ISO/IEC 27001:2022 Clause 5.3.
- All employees are notified of policy revisions via official communication channels. Acknowledgment of the updated policy is mandatory within a defined time frame.
- Each version of the policy is archived with complete change history and maintained for compliance audits and regulatory submissions.

References:

S. No.	**Cybersecurity Domain**	**Relevant Information Technology Act, 2000 / Amendment**	**National Cyber Security Policy, 2023 (NCSP)**
1	**Governance, Risk, and Compliance (GRC)**	- Section 43A: Reasonable security practices- Section 70B: Incident reporting to CERT-In	- Institutional structures for governance- 24/7 NCIIPC operations- Risk-based security enforcement
2	**Asset Management**	- Section 66B: Handling stolen computer resources	- Emphasis on asset inventory, critical infrastructure classification, and secure IT procurement practices
3	**Access Control**	- Section 66: Hacking- Section 66C: Identity theft- Section 66E: Privacy violations	- Role-based access control support- Reducing insider threat surface
4	**Data Security and Privacy**	- Section 43: Unauthorized data access- Section 66E: Violation of privacy	- Promotes encryption and protection of CII (Critical Information Infrastructure)
5	**Network Security**	- Section 66: Hacking- Section 70: Securing Critical Information Infrastructure	- Calls for segmentation, IDS/IPS, and 24/7 monitoring of national networks
6	**Identity and Access Management (IAM)**	- Section 66C: Identity theft	- Promotes user authentication systems, secure credentials, and traceability
7	**Security Monitoring & Incident Response**	- Section 70B: CERT-In reporting- Section 72A: Breach disclosure obligation	- National threat intelligence sharing- IR readiness under NCIIPC
8	**Application Security**	- Section 66: Hacking- Section 43: Data corruption or damage	- Secure-by-design application guidelines, especially for software impacting CII
9	**Endpoint Security**	- Section 66: Malware and unauthorized access	- End-user device hardening, patch management, and endpoint visibility

10	**Cloud Security**	- Section 43A: Reasonable security practices in data handling by third-party/cloud providers	- Promotes secure procurement and configuration for cloud environments
11	**Physical and Environmental Security**	- Implicit under Section 43 (damage to systems/data)	- Protection of physical infrastructure housing critical assets
12	**Business Continuity & Disaster Recovery (BC/DR)**	- Section 70: Ensuring resilience of Critical Infrastructure	- Mandates DR/BC capabilities for CII; aligns with resilience and recovery principles
13	**Security Awareness**	- Section 66 & 43A: Emphasize on human factor in cybercrime mitigation	- Calls for national awareness programs and institutional capacity building
14	**Vendor Security & Third-Party Management**	- Section 43A: Responsibility of organizations using third-party vendors	- Recommends secure outsourcing practices, and vendor assurance in national cyber supply chains

13. Legal & Regulatory Compliance

This Cybersecurity Policy ensures the organization's commitment to protecting data and information systems in line with **ISO 27001:2022**, **Indian Cyber Laws, Information Technology Act, 2000, EU General Data Protection Regulation (GDPR)** and **National Cyber Security Policy 2023**. Regular updates and audits will ensure compliance and security in an evolving digital landscape.

- DPDP Act 2023: HFCL, as Data Fiduciary, shall provide clear, multilingual notices before consent; enable rights to access, correction and erasure; implement reasonable security safeguards; and notify personal-data breaches to the Data Protection Board of India and affected individuals without undue delay in accordance with applicable rules. Significant Data Fiduciary obligations (e.g., DPO based in India, DPIA) shall be met when designated.
- CERT-In Directions (2022): Cyber incidents (including data breaches, ransomware, DDoS, unauthorized access) must be reported to CERT-In within 6 hours of becoming aware. HFCL shall retain system logs in India for at least 180 days; synchronize system clocks with trusted NTP; designate Points of Contact; and assist CERT-In investigations.
- The Companies Act, 2013: The Vigil Mechanism/Whistleblower Policy (Section 177) provides safeguards against victimization and direct access to the Audit Committee Chair. Fraud involving ICT systems shall be addressed under Section 447 (Punishment for Fraud) alongside HR/disciplinary processes.
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015: HFCL shall disclose cyber risk oversight in Corporate Governance reports/MDA; the RMC charter shall specifically cover cybersecurity and receive periodic metrics on incidents, resilience (RTO/RPO), privacy breaches, and ESG data controls.

Related Policies

This policy should be read alongside the following policies of HFCL:

S. No.	**Policy**
1	HFCL Privacy Policy
2	HFCL ISMS PIMS Roles, Responsibility and Authority
3	HFCL Data Retention and Disposal Policy
4.	Vendor Risk Management Policy
5.	Risk Management Policy
6.	Whistle Blower Policy – Vigil Mechanism