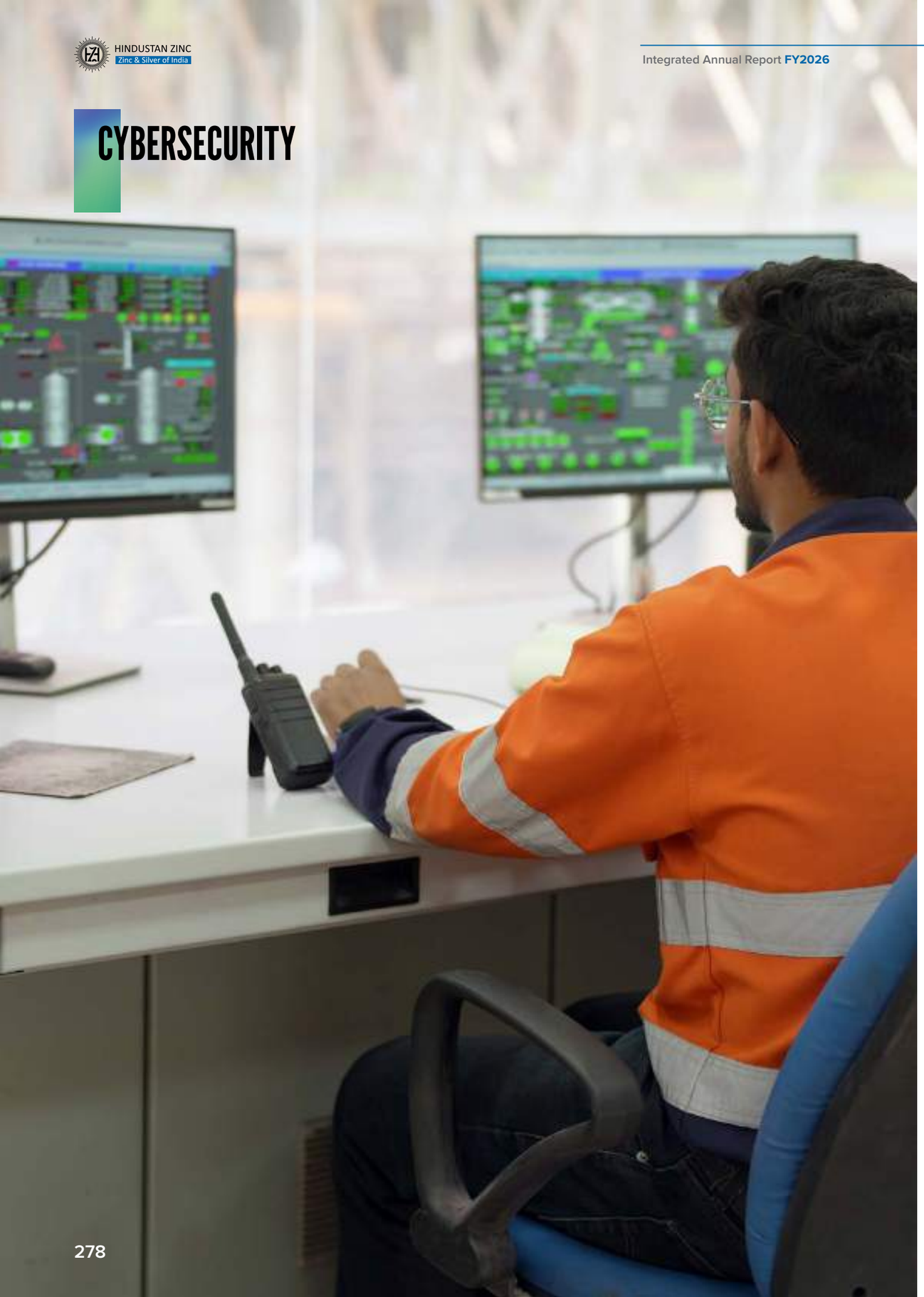
CYBERSECURITY



CYBERSECURITY GOVERNANCE

At Hindustan Zinc, we are investing significantly in strengthening our cyber resilience across our operations to maintain data integrity, confidentiality, and business continuity against cyberattacks and evolving threats. Strong governance and enterprise risk management framework with improved technology and control systems are consistently improving our cybersecurity posture.

GOVERNANCE COMMITTEE

Board's Audit and Risk Management Committee	IT and Cyber Security Steering Committee	Chief Information Security Officer (CISO)

COMPOSITION

Chaired by Independent Director, Ms. Pallavi Joshi Bakhru, who provides strong leadership and governance oversight of enterprise cyber and technology risk management.

She strengthens the Committee's effectiveness by:

- Providing strategic direction and oversight to ensure cybersecurity and digital risks are appropriately embedded into enterprise risk management and key business decisions
- Overseeing the governance and effectiveness of enterprise cyber resilience programme, including incident preparedness, business continuity, and recovery mechanisms

- Chaired by the Chief Executive Officer (CEO)
- Comprises leaders from all the business functions, including IBU Heads, Chief Financial Officer (CFO), Chief Human Resource Officer (CHRO), Chief Information Officer (CIO), and Chief Commercial Officer (CCO)

RESPONSIBILITIES AND ACCOUNTABILITY

- Reports to the Board and oversees cybersecurity governance
- Responsible for all business risks, including cyber risks

- Sets up expectations, provides direction and support for the cybersecurity measures
- Reviews and monitors the progress and maturity of the organisation's cybersecurity posture

- Sets up the cybersecurity vision and strategy
- Defines cybersecurity governance framework
- Ensures effective execution of the programmes to safeguard confidentiality, integrity and availability of all information assets
- Holds accountability to the IT and Cyber Security Steering Committee as well as the Audit and Risk Management Committee of the Board on all cybersecurity matters

OUR LEADERSHIP AND GOVERNANCE STRUCTURE FOR CYBERSECURITY STRATEGY, EXECUTION AND MONITORING

Audit and Risk Committee of the Board
(Chaired by Independent Director, Ms. Pallavi Joshi Bakhru)

IT & Cyber Security Steering Committee
(Chaired by CEO)

- **Chief Security Officer** (Physical Security)
- **Chief Information Security Officer** (Reports to CFO)
- **Digital Head**

Approach to Manage Cybersecurity Risks

We recognise the need for a strong and agile risk management framework to protect the confidentiality, integrity and availability of our technology and data assets. Our cybersecurity risk management framework features the following elements:

Risk-focused Cybersecurity Framework
Built on clearly-defined principles/standards and an objective-based approach, the framework prioritises risk mitigation and deployment of critical controls across all our assets.

Cybersecurity Standards
The framework is supported by information security management and personal data privacy standards, disaster recovery and business continuity management, and risk management, ensuring strong governance.

Integrated ISO Certification
ISO 27001 (Information Security), ISO 22301 (Disaster Recovery & Business Continuity Plan), ISO 31000 (Risk Management), and ISO 27701 (Privacy Management) cover 100% of our assets in India.

Alignment with COBIT Framework
Our risk register and risk control matrix are mapped with the control objectives of the information and related technology (COBIT) framework.

INFORMATION SECURITY FRAMEWORK

The Company manages information security through a well-structured Information Security Management Framework, integrated with our Enterprise Risk Management (ERM) framework. The framework brings together key policies, standard operating procedures (SOPs), technology standards, and rigorous security assessment and audit to mitigate cyber risks. This is further reinforced by implementing security-by-design in our business and technology landscape.

CORE DEFENSIVE PILLARS

1

Cyber Resilience

Our Cyber Crisis Management Plan (CCMP) ensures round-the-clock readiness through:

- 24X7 security incident detection and monitoring plan, and response and recovery playbooks
- Alignment with the organisation's crisis management plan, and associated decision/communication matrix for cross-functional stakeholders
- Cyber insurance and incident response retainer services to provide protection from low-probability, high-impact cyberattacks
- Annual executive cyber drills and purple teaming for continuously enhance our cyber resilience

2

Social Engineering and Awareness

Recognising the importance of an informed workforce in mitigating cyber threats, we deliver multi-layered awareness initiatives to strengthen team capabilities in identifying and reporting breaches, which include:

- Mandatory cybersecurity training embedded in new joiners' onboarding process
- A self-service online awareness training capsule made available to all users
- Annual extensive security awareness covers all employees and business partners with access to our systems or premises
- Awareness disseminated through posters, gamified videos, quizzes, end-to-end social engineering simulations, covering scenarios such as phishing, vishing, smishing, deep-fake, and digital arrest scenarios, etc.
- Cyber Security Awareness Month (CSAM) observed through engaging initiatives, including external expert-led live demonstrations of prevalent digital frauds
- Training of employees on the ethical use and/or security of AI

3

Data Privacy Readiness

- Privacy information management system (PIMS) in place, supported by privacy policies, procedures, consent management, and data subject rights management
- Organisation-wide privacy awareness for employees
- Privacy impact assessments for business processes involving large-scale personal information
- Data discovery to identify personally identifiable information (PII) collection, storage, processing, transfer, etc.

4

Operational Technology Security

- Phased upgradation of our legacy operational technology (OT) systems/plant technical systems to the latest versions
- Vulnerability scanning of OT systems to identify and remediate known vulnerabilities declared by original equipment manufacturers (OEMs)
- Intended implementation of dedicated Security Operations Centre (SOC) to enhance OT environment, ensuring long-term resilience of plant technical systems

5

Cloud Security

- Risk-based remediation of security issues across our assets, such as virtual machines, applications, services hosted on corporate IaaS (Infrastructure as a Service) cloud or SaaS (Software as a Service) applications
- All assets integrated with the Security Operations Centre (SOC) for 24X7 security monitoring
- Deployed Web application firewall and privileged access management to protect our crown jewel applications and privileged users against cyberattacks

6

Data Leakage Prevention

- Thorough data flow analysis (DFA) conducted with our business/functional teams to identify critical data and crown jewels
- Implemented DFA-informed comprehensive data leakage prevention (DLP) capability, covering various communication channels such as web, email, mobile devices, etc.
- Regular DLP rule-based review and fine-tuning maintain continuous alignment with DFA
- Dedicated 24X7 DLP monitoring desk monitors and manages all data leakage incidents

7

Third-Party Risk Management

- Systematic identification of third parties posing cybersecurity risks, with a defined governance structure for its mitigation
- Annual risk assessments for high-risk third parties (including new third-party vendors), ensuring risk measurement and mitigation
- Robust security clauses incorporated into third-party contracts

8

Governance, Risk and Compliance

- A strong risk management framework is in place to identify, assess and address a wide range of organisational risks
- Detailed risk assessments guide our information security strategy, shaping both long-term and short-term roadmaps
- Targeted cybersecurity initiatives are implemented to address identified risks, bolstering capabilities across businesses
- Regular review of cybersecurity policies and procedures ensures their relevance and effectiveness in an evolving threat landscape

REVIEW OF POLICIES, PROCEDURES AND RISK FRAMEWORK

IT and Cyber Security Steering Committee

Conducts an annual review of the risk framework, in consultation with external experts, to incorporate applicable regulatory requirements, industry best practices, and emerging threats

CIO, CISO and Information Security Function

Review the Information Security and Data Governance policies and procedures every year to ensure alignment with the evolving security landscape

THE APPROVED AND ENFORCED POLICIES ARE EFFECTIVELY COMMUNICATED AND MADE ACCESSIBLE TO ALL EMPLOYEES AND BUSINESS PARTNERS (BPs) THROUGH HIGH-IMPACT, MULTI-CHANNEL COMMUNICATION.

9

Zero Trust Security Architecture

- Modernised network access and cloud-security controls by implementing Network Access Control (NAC) and Security Service Edge (SSE) to reduce implicit trust, minimise attack surface, and strengthen continuous security validation
- NAC verifies every user and device attempting to connect to our corporate resources, ensuring only authenticated, compliant, and trusted endpoints are granted access
- SSE enables secure, identity-based access to applications and data from any location, integrating capabilities such as secure web gateway, cloud access security broker, and zero-trust network access

10

AI Governance Programme

Our organisation has implemented a balanced and secure artificial intelligence (AI) governance framework that enables responsible adoption of artificial intelligence across business processes while maintaining strong data protection standards, user awareness and compliance requirements.

- Authorised AI tools are deployed and employees are encouraged to use them for enhancing productivity, automation and operational efficiency
- Robust data loss prevention (DLP) controls and cloud proxy monitoring detect and block unauthorised uploads of confidential or regulated data on AI platforms
- AI governance model emphasises responsible use, ethical practices and compliance, ensuring innovation is advanced while protecting organisational, customer and partner information

NAVIGATING THE REGULATORY LANDSCAPE

COMPLIANCE WITH THE INFORMATION TECHNOLOGY ACT

Hindustan Zinc is fully compliant with the requirements of the Information Technology Act, 2000, and the associated Sensitive Personal Data or Information (SPDI) Rules, 2011. The Company has implemented robust mechanisms to ensure strong governance, data protection, and adherence to statutory obligations across all digital operations of the organisation.

- Sensitive personal data is collected only with explicit written consent
- Disclosure of such data is undertaken with prior authorisation
- External transfer of such data is permitted only to entities maintaining equivalent standards of data protection
- A comprehensive privacy policy governs data handling practices across the organisation

Hindustan Zinc has established and published a comprehensive privacy policy which enforces reasonable security practices across its systems, prevents the publication or transmission of prohibited electronic content, and maintains electronic records in a secure, accessible, and legally compliant manner.

COMPLIANCE WITH THE DIGITAL PERSONAL DATA PROTECTION ACT

Hindustan Zinc has launched a comprehensive privacy compliance programme to align with the Digital Personal Data Protection Act, 2023 (DPDPA). As part of this programme:

- We have mapped personal-data processing across applications and business processes through detailed ROPA (Record of Processing Activities) and DFD (Data Flow Diagrams) exercises
- A structured gap assessment against DPDPA obligations and global privacy standards has also been conducted
- Privacy policies, procedures and templates have been updated accordingly to reflect regulatory requirements
- Implementation is underway for key technical controls such as privacy notices, cookie banners, data masking, encryption and consent management
- A network of trained privacy champions and business heads has been formalised to build accountability and steward responsible personal-data processing within their respective functions

The privacy compliance programme reinforces our commitment to strong data-protection practices and builds greater trust among employees, partners and stakeholders.

COMPLIANCE WITH THE INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN)

Hindustan Zinc adheres to the cybersecurity requirements mandated by CERT-In, India's national incident-response authority, which oversees guidelines and expectations for cybersecurity-readiness and reporting. To ensure a secure and resilient IT environment across operations, the Company:

- Ensures timely reporting of notifiable cyber incidents
- Maintains required log-retention and monitoring controls as prescribed under CERT-In Directions
- Aligns security practices and procedures with CERT-In-driven standards and regulatory expectations

Hindustan Zinc is certified under the ISO 27001:2022 ISMS framework, ISO 27701:2019 PIMS framework, ISO 22301:2019 BCMS framework, and ISO 31000:2018 risk management framework.

INCIDENT MANAGEMENT AND RESPONSE

Microsoft Sentinel	Incident Response Through Security Operations Centre

Hindustan Zinc has significantly strengthened its cybersecurity posture by implementing Microsoft Sentinel as its central platform for security incident management and response platform.

How Security Operations Centre Enhances Our Cybersecurity Posture

Real-Time Monitoring and Response

Provides Cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) capabilities, enabling real-time monitoring, advanced threat detection and automated incident response across our digital ecosystem

AI-Drive Response Efficiency

Integrated analytics, AI-driven correlation and automated playbooks offer enhanced visibility into security events, faster triage and improved response efficiency

Comprehensive Threat Coverage

Allows seamless integration with Microsoft 365, Azure, GCP, WAF and other security solutions, ensuring comprehensive coverage and rapid mitigation of potential threats

OUTCOMES

Improved ability to proactively identify risks

Lesser security incidents

Resilient operational environment

END-TO-END INCIDENT MANAGEMENT APPROACH AT HINDUSTAN ZINC

All information security and data incidents are detected through our Security Operations Centre (SOC), data loss prevention (DLP) desk operations and reports from both the information security function and end users

▶

A well-established system tracks and monitors all security incidents to logical closure

▼

Root cause analysis and mitigation plans developed in line with our incident management and data breach policy, prevent future recurrences

▼

A well-defined and comprehensive escalation process is also in place

◀

Disaster recovery drills (DR drills), conducted twice a year as part of our business continuity plan (BCP), enhance preparedness

Hindustan Zinc has invested in a comprehensive Purple Teaming exercise to strengthen its Security Operations Centre (SOC). This initiative ensures that our incident detection and response capabilities remain top-tier and aligned with global best practices, reassuring our stakeholders.

VULNERABILITY MANAGEMENT

To protect our information technology (IT), operational technology (OT) and digital environment, we maintain a robust vulnerability management policy designed to effectively identify and mitigate risks and vulnerabilities. The in-depth structure of the Company's vulnerability management programme extends across all tiers of defence, ensuring adequate coverage to policy & framework, physical perimeter, network, application, cloud environment, and data security.

Vulnerability Assessment and Analysis

During the year, we conducted multiple assessments to identify vulnerabilities, monitor threats & shortcomings, analyse associated risks/impacts, track mitigation actions, and maintain compliance. These assessments included review of governance & frameworks , red teaming exercise for physical security assessment, data governance and compliance assessment. We partner with globally recognised third-party agencies for internal and external vulnerability assessment and penetration testing (VAPT) programme and ISO surveillance audits. The assessment of IT general controls (ITGC) is conducted by a statutory auditor under applicable financial compliance frameworks.

Hindustan Zinc's information security function and the Group's management assurance services (MAS) function jointly conduct VAPT, including simulated hacker attacks, at least twice a year. It enables us to define, identify, classify, and prioritise vulnerabilities in computer systems, applications and network infrastructures. Our consistent track record places us as one of the highest rated entities in the MAS audit group.

Recognising the critical importance of proactively identifying system vulnerabilities, Hindustan Zinc has introduced a Bug Bounty Programme. This initiative helps us uncover and address potential security gaps across our digital ecosystem, reinforcing our commitment to maintaining a strong cybersecurity posture and safeguarding stakeholder interests.

INCIDENT REPORTING AND ESCALATION

We empower our employees to report suspicious activities or threats against the organisational assets, intellectual property, other business documentation, our personnel, or finances, to Myitsupport@vedanta.co.in and hzl.isms@vedanta.co.in. Phishing emails are reported via the "Report Phishing" option provided in the mail menu. Following initial triage and analysis, verified threats are formally escalated for resolution.

CYBERSECURITY-LINKED PERFORMANCE EVALUATION

At Hindustan Zinc, our performance evaluation framework aligns the performance of IT/OT personnel with the Company's information security goals. The internal and external vulnerability assessments, management reviews and reported incidents help evaluate the efficacy of processes and technologies. Offenders under the social engineering simulation exercises are issued advisory letters from the CHRO's office, cautioning them about the risks and potential punitive actions that any repeated instance of offence may incur.

Our Report Card

Particulars	FY2026	FY2025
Total number of information security breaches	0	0
Total number of clients, customers and employees affected by the breaches	0	0