Chromewell Engineering Private Limited

Data Privacy, Information Security & Cybersecurity Policy

POLICY NO: CW-ETH-004 | VERSION: 4.0

ISSUE DATE: JAN 2026 | NEXT REVIEW: JAN 2027 | SUPERSEDES: V3.0 (JUNE 2025)

882/1, Pune Nagar Road, Sanaswadi, Taluka Shirur, 412208 Pune, Maharashtra, India.

Table of contents

1. Document Information:

Document Details		Governance
Policy Owner: Head of IT	**Scope:** All personal data, business-confidential data, and information systems managed by or on behalf of Chromewell Engineering, including employee data, customer data, supplier data, financial records, and product intellectual property.	**Reviewed & Approved By:** CEO & CFO
Secondary Owner: Head of Compliance	**Applies To:** All employees, contractors, and third-party service providers who access, process, store, or transmit Chromewell's data or information systems. All devices, networks, cloud platforms, and applications used for Chromewell business.	**Review Cycle:** Annual – Once a year

2. Purpose

Chromewell Engineering Pvt Ltd handles significant volumes of personal data - employee records, payroll, health surveillance, customer contact data - and commercially sensitive information including product designs, tooling specifications, customer pricing, and supply chain data. The confidentiality, integrity, and availability of this data is critical to our business, our employees' privacy rights, and our obligations to EU and USA customers who share proprietary information with us.

This policy is aligned with:

- ISO 27001:2022 - Information Security Management Systems
- EU General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679
- Indian Digital Personal Data Protection Act 2023 (DPDPA)
- Indian Information Technology Act 2000 and IT (Amendment) Act 2008
- GRI 418: Customer Privacy (2016)
- CSRD ESRS G1 - Business Conduct (data and information integrity)
- NIST Cybersecurity Framework (CSF 2.0)

3. Scope

This policy applies to all information assets of Chromewell Engineering:

- Personal data: employee records (HR, payroll, health, performance), customer contact data, supplier contact data, and any data relating to identified or identifiable individuals
- Business-confidential information: product designs, tooling drawings, customer pricing, contracts, trade secrets, and supply chain commercial information
- IT systems: all servers, workstations, laptops, mobile devices, cloud platforms, ERP systems, IMDS portals, and email systems
- Third-party data: customer-provided product specifications, OEM technical data, and supplier financial information.

4. Key Objectives and Targets

Chromewell Engineering defined both qualitative objectives and quantitative targets for Information Security issues from its own operations and from its supply chain.

Information Security Issue	Key Objectives	Target (2025–2027)
Personal Data Protection	Collect, process, and store personal data only where there is a lawful basis, only for the stated purpose, and only for as long as necessary. Respect data subject rights - access, correction, deletion, and portability.	DPDPA consent register: implemented by December 2025. Employee data subject rights requests: 100% responded to within 30 days Data retention schedule: reviewed and implemented by December 2025 Zero personal data sold to third parties
Information Security Controls	Implement layered technical and organisational controls to protect the confidentiality, integrity, and availability of all Chromewell information assets, aligned to ISO 27001.	ISO 27001 self-assessment: completed annually Vulnerability assessments: conducted annually on all critical systems Access reviews: conducted quarterly for all privileged accounts

		MFA (multi-factor authentication): deployed for all remote access by December 2026
Cybersecurity Incident Prevention & Response	Prevent cybersecurity incidents through proactive controls and respond swiftly and effectively to any incident that occurs to minimise harm and restore operations.	Cybersecurity incidents resulting in data loss: zero target Cybersecurity incident response plan: documented and tested annually Incidents notified to DPDPA Board (if applicable): within 72 hours of detection Employee phishing test failure rate: < 5% by December 2026
Employee Awareness & Training	Ensure all employees who handle data understand their responsibilities, common cyber threats (phishing, social engineering), and the secure handling of personal and confidential information.	100% of employees complete information security awareness training annually Phishing simulation: conducted at least annually New employees: trained within 30 days of joining
Third-Party Data Security	Ensure that all third parties - IT service providers, cloud vendors, ERP suppliers, and logistics partners - who process Chromewell data meet adequate security standards through contractual and audit controls.	NDA signed with 100% of 3rd party IT vendors/partners Critical IT vendors: security assessed annually Cloud service providers: ISO 27001 or equivalent certification confirmed annually
Customer Data and IP Protection	Protect OEM customer product designs, tooling drawings, pricing, and technical specifications as confidential information with access restricted on a need-to-know basis and secure transmission controls.	Customer IP access: restricted to authorised personnel only - 100% Customer-provided data: encrypted in transit and at rest Customer data breach incidents: zero Customer data handled per NDA/contract terms: 100% compliance

5. Governance and Allocation of Responsibilities

Clear accountability is assigned at every level of Chromewell Engineering's ESG Governance Structure. The table uses a RACI framework (Accountable, Responsible, Consulted, Informed).

Role / Designation	RACI Level	Department	Key Responsibilities Under This Policy
CEO/CFO	Accountable (A)	Executive	Final accountability for information security. Receives annual cybersecurity and data privacy report. Approves data security investment. Notified immediately of significant data breach.
Head of IT	Primary Owner (R)	IT & Data	Manages technical information security controls: network security, access management, vulnerability management, MFA deployment, backup systems, incident response, and IT vendor security.
Head of Compliance	Primary Owner (R)	Compliance	Manages GDPR and DPDPA compliance: data processing register, lawful basis documentation, data subject rights requests, DPAs with processors, regulatory notifications, and data breach legal response.
Compliance Executive	Secondary Owner (R)	Compliance	Manages GRI 418 / CSRD ESRS G1 privacy disclosures.
Head of HR	Consulted (C)	Human Resources	Co-manages employee personal data under DPDPA and GDPR (as applicable). Ensures employee privacy rights are respected in HR processes. Manages employee security training and phishing simulations.
Finance / CFO	Consulted (C)	Finance	Manages security of financial systems and data. Ensures ERP access controls reflect current employment status. Reviews third-party financial data sharing agreements.
All Employees	Responsible (R)	All Functions	Handle personal and confidential data responsibly. Use strong passwords and lock screens. Report suspected cybersecurity incidents immediately to IT. Never share credentials.

RACI: A = Accountable (signs off, one person only) · R = Responsible (does the work) · C = Consulted (input required) · I = Informed (kept in loop).

6. Policy Commitments

6.1 Personal Data - Lawful Basis and Purpose Limitation

- Personal data is processed only where a documented lawful basis exists (consent, contractual necessity, legal obligation, legitimate interest) per DPDPA 2023 and GDPR
- Data is collected only for the specified purpose; it is not repurposed without a new lawful basis
- A data processing register documents all categories of personal data, their purpose, legal basis, retention period, and processors

- Data subject rights requests - access, correction, deletion - are responded to within 30 days

6.2 Technical Security Controls

- All Chromewell information systems are protected by network firewalls, endpoint protection, encrypted storage for sensitive data, MFA for remote access, and regular software patching
- Access to systems and data is granted on a least-privilege, need-to-know basis; access rights are reviewed quarterly
- Critical data - employee personal data, customer IP, financial records - is backed up daily with offsite encrypted backup
- Vulnerability assessments are conducted annually on all critical systems; identified vulnerabilities are remediated within defined SLA periods by severity

6.3 Cybersecurity Incident Response

- A documented cybersecurity incident response plan is tested annually through a tabletop exercise
- Any suspected data breach is reported immediately to the IT head and Head of Legal
- Where a breach involving personal data meets the DPDPA or GDPR notification threshold, the relevant regulatory authority is notified within 72 hours
- Affected data subjects are notified without undue delay where the breach is likely to result in high risk to their rights and freedoms

6.4 Customer IP and Confidential Information

- OEM customer product designs, tooling drawings, and technical data are stored in access-controlled systems with audit trails
- All customer-provided confidential information is handled in accordance with the NDA or confidentiality clauses of the supply agreement
- Customer IP is not shared with any third party without express written consent from the customer

7. KPI Monitoring and Reporting

The following KPIs are tracked by the ESG Working Group, reported quarterly to the ESG Steering Committee, and published annually in the Chromewell Sustainability Report

KPI / Indicator	Target	Measurement Method	Cadence	Owner
Data Breaches Involving Personal Data	Zero significant breaches	IT incident log	Quarterly	IT Head
Information Security Training Completion	100% annually	HR training records	Annual	Head of HR
Phishing Simulation Failure Rate	< 5% by Dec 2026	IT security platform	Annual	IT Head
Privileged Account Access Reviews	Quarterly	IT access management records	Quarterly	IT Head
Data Subject Rights Requests - Response Time	100% within 30 days	Legal records	Quarterly	Head of Compliance

Data Processing Register Completeness	100%	Legal register	Annual	Head of Compliance
DPAs with All Personal Data Processors	100%	Legal register	Annual	Head of Compliance
Critical Vendor Security Assessments	100% annually	IT vendor records	Annual	IT Head
Vulnerability Assessment Completion	Annual	IT security records	Annual	IT Head

8. Policy Review Mechanism

Reviewed annually every April by IT Manager and Head of Legal with CEO approval. Interim review triggered by a significant cybersecurity incident or data breach, material change to DPDPA or GDPR guidance, or a new cloud platform or data processing arrangement.

Version	Date	Author	Approved By	Summary of Changes
1.0	July 01, 2021	IT Manager/Head of IT	Mr. Amardeep Mardhekar (CEO) Ms. Risha Naik (CFO)	Initial issue
2.0	May 03, 2022	IT Manager/Head of IT	Mr. Amardeep Mardhekar (CEO) Ms. Risha Naik (CFO)	Minor edits on the Quantitative targets
3.0	June 05, 2025	IT Manager/Head of IT	Mr. Amardeep Mardhekar (CEO) Ms. Risha Naik (CFO)	Updated to v3.0: KPI has been revised
4.0	Jan 14,2026	IT Manager/Head of IT	Mr. Amardeep Mardhekar (CEO) Ms. Risha Naik (CFO)	Added related policies with clear accountability and ownership

9. Compliance, Non-Conformance, and Disciplinary Action

- Deliberate data breach, unauthorised access to systems, or sharing of confidential data without authorisation constitutes gross misconduct and grounds for immediate termination
- DPDPA or GDPR violations are reported to the relevant Data Protection Authority; Chromewell cooperates fully with regulatory investigations
- Concerns are reported through Policy CW-ETH-003 - Whistleblower Protection & Speak-Up Policy
- “Report a concern” form available on ChromeNet as an anonymous grievance redressal mechanism and, we have a dedicated hotline number published on the website to report any concern anonymously.

10. Related Documents and References

Internal policies:

- CW-ETH-001 - Business Ethics & Code of Conduct Policy
- CW-ETH-003 - Whistleblower Protection & Speak-Up Policy

- CW-HR-006 - Anti-Discrimination, Harassment & Abuse Policy
- CW-PROC-SCM-001 - Sustainable Procurement Policy (data sharing with suppliers)

External standards:

- ISO 27001:2022 - Information Security Management Systems
- EU General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679
- Indian Digital Personal Data Protection Act 2023 (DPDPA)
- Indian Information Technology Act 2000 (as amended 2008)
- NIST Cybersecurity Framework (CSF 2.0)
- GRI 418: Customer Privacy (2016)
- CSRD ESRS G1 - Business Conduct

11. Formal Approval and Sign-Off

This policy has been prepared, reviewed, and formally approved:

Prepared By	Reviewed By	Approved By
Name: Mr. Rupesh Pawar **Designation:** IT Manager **Date:** Jan 2026 **Signature:**	**Name:** Mr. Prakash Kunte **Designation:** Head of IT **Date:** Jan 2026 **Signature:**	**Name:** Ms. Risha Naik **Designation:** CFO **Date:** Jan 2026 **Signature:**

FOR FURTHER INFORMATION:

This policy is issued under the authority of the CEO & CFO of Chromewell Engineering Pvt Ltd. It supersedes v3.0 (June 2025). For further information or advice, please contact a Chromewell Finance or Compliance Officer or Chromewell's Board or Directors.