Incident Response Procedure

POL No.: ROSS-IT-OVS-POL-001

POL GOVERNANCE, REVISION HISTORY & REVIEW PLAN

POL Name	Global Overseas IT Policy
POL No.	ROSS-IT-OVS-POL-001
Current Version	1.0
Effective Date	20-Jul-2026
Owner Department	Information Technology (IT)

APPROVALS

Version No.	Prepared By	Reviewed By	Approved By
1.0 (Initial Version)	Nitin Srivastava (Asst. Manager - IT)	Bhavesh Sangani (Group Head - IT)	Ketan Sablok (Group CFO)

NEXT REVIEW:
On or before 19-Jul-2027

Table of Contents

1. Purpose

This Global Overseas IT Policy ('**Policy**') establishes a comprehensive, risk-based framework governing the use, protection, and management of information technology assets, systems, data, and infrastructure across all overseas locations, subsidiaries, and group companies of Rossari Biotech Limited ('**Rossari**' or '**the Company**').

The Policy is aligned with Information Security Management Systems and Rossari's corporate Information Security Management System (ISMS). It is designed to:

- Protect the confidentiality, integrity, and availability of all corporate information and IT assets.
- Establish standardised IT governance, access control, and operational security practices across all global offices.
- Address specific risks inherent to chemical manufacturing environments, including operational technology (OT), industrial control systems (ICS), and proprietary formulation data.
- Enable business continuity and resilience against cyber threats, data breaches, and operational disruptions.
- Ensure compliance with applicable laws, regulations, and contractual obligations in each jurisdiction, to the extent applicable.

This Policy acts as the primary governing document and supersedes all prior overseas IT policies. All subsidiary, associated, and functional policies must be read in conjunction with and subordinate to this Policy.

2. Scope

This Policy applies to:

2.1 Entities Covered

- Rossari Biotech Limited (head office and all domestic locations acting as global IT governance anchor).
- All overseas branch offices, representative offices, subsidiaries.
- Joint ventures and associate companies where Rossari hold management control or IT governance responsibility.
- Third-party vendors, contractors, and service providers who access Rossari systems or process Rossari data from local or overseas locations.

2.2 Personnel Covered

- All full-time and part-time employees stationed at or working remotely for overseas operations.
- Contractors, consultants, temporary staff, and interns.
- Third-party personnel granted access to Rossari IT systems.

2.3 Systems and Assets Covered

- All IT hardware: desktops, laptops, servers, mobile devices, and peripherals.
- All software: licensed applications, ERP systems, cloud services, SaaS platforms.
- Network infrastructure: LAN/WAN, Wi-Fi, firewalls, VPNs, and SD-WAN links.
- Operational Technology (OT) systems: SCADA, DCS, PLCs, HMI, and plant control networks.

- Data assets: structured databases, files, emails, logs, formulation data, customer data.
- Cloud environments: IaaS, PaaS, SaaS platforms used for business purposes.

2.4 Exclusions

Personal devices not used for Rossari business are excluded unless they connect to Rossari systems, in which case the relevant sections of this Policy apply.

3. Definitions & Abbreviations

Term / Abbreviation	Definition
CIA Triad	Confidentiality, Integrity, and Availability – the three core principles of information security.
ISMS	Information Security Management System – the overarching framework under ISO/IEC 27001:2022.
OT / ICS	Operational Technology / Industrial Control Systems – systems controlling physical processes (SCADA, DCS, PLC, HMI).
SCADA	Supervisory Control and Data Acquisition – industrial control system architecture.
DCS	Distributed Control System – used in chemical plant process automation.
PLC	Programmable Logic Controller – industrial digital computer for manufacturing automation.
MFA	Multi-Factor Authentication – requiring two or more verification factors for access.
RBAC	Role-Based Access Control – assigning system access based on job role.
PAM	Privileged Access Management – controls and monitoring of privileged/admin accounts.
EDR	Endpoint Detection and Response – security solution for endpoint threat detection.
SIEM	Security Information and Event Management – log collection and security event correlation platform.
DLP	Data Loss Prevention – technology to prevent unauthorized data exfiltration.

Term / Abbreviation	Definition
CSPM	Cloud Security Posture Management – tools to identify and remediate cloud misconfigurations.
VPN	Virtual Private Network – encrypted tunnel for secure remote network access.
RTO	Recovery Time Objective – maximum acceptable downtime after an incident.
RPO	Recovery Point Objective – maximum acceptable data loss measured in time.
SLA	Service Level Agreement – contractual commitment on service performance.
SOC	Security Operations Centre – centralised team monitoring security events.
NDA	Non-Disclosure Agreement – contractual obligation to protect confidential information.
GRC	Governance, Risk and Compliance – integrated management of these three disciplines.
BCP/DR	Business Continuity Plan / Disaster Recovery – plans to maintain and restore operations.
IP	Intellectual Property – formulations, trade secrets, processes, and patents.

4. IT Governance & Organisational Responsibilities

Consistent with ISO/IEC 27001:2022), the following structure governs IT and information security across all overseas operations:

4.1 Governance Structure

Role	Responsibility
Managing Director / Board	Ultimate accountability for ISMS. Approve policy. Ensure adequate resources.
Group CFO	Oversight of financial risk relating to IT and cybersecurity investments.
Group IT Head	Define and enforce global IT standards. Own this, Policy. Chair ISMS reviews.
ISMS Manager	Day-to-day ISMS operations: risk assessments, audits, training, incident coordination.
Overseas IT Manager / Lead	Implement Policy at local level. Liaise with Group IT. Manage local assets.
Department Heads	Ensure team compliance. Participate in risk identification. Authorise access requests.
All Employees & Contractors	Comply with this Policy in all IT activities. Report incidents and violations.

4.2 ISMS Steering Committee

An ISMS Steering Committee shall be constituted comprising the Group IT Head, Infrastructure Manager, Head Legal, and Senior representatives from Operations and Finance. The Committee shall meet at minimum quarterly to review ISMS performance, risk posture, and policy compliance.

4.3 Policy Compliance Obligation

Compliance with this Policy is mandatory for all persons within scope. Non-compliance will be addressed in accordance with Section 25 (Policy Violations) of this document.

5. Risk Management Framework

Rossari shall maintain a risk-based approach to information security in accordance with ISO/IEC 27001:2022

5.1 Risk Assessment

- A formal Information Security Risk Assessment shall be conducted at minimum annually and upon any significant change (new system, new site, major process change, regulatory update).
- Risk assessments shall cover IT systems, OT/ICS environments, cloud platforms, vendor access, and physical assets.

- Risk assessments shall be documented in the Rossari Risk Register, maintained by the ISMS Manager.

5.2 Risk Treatment

For each identified risk, one of the following treatments shall be applied:

- Mitigate: Apply controls to reduce likelihood or impact.
- Transfer: Use insurance, contracts, or SLAs to transfer risk.
- Accept: Formally accept residual risk with Group IT Head/MD approval and documented justification.
- Avoid: Discontinue the activity or process that introduces the risk.

5.3 Statement of Applicability (SoA)

Rossari shall maintain a statement of applicability referencing all **Annexure A** controls of ISO/IEC 27001:2022, indicating which are implemented, with justification for inclusions and exclusions. The SoA shall be reviewed annually.

6. Access Control Policy

Access to Rossari information systems, networks, and data shall be controlled on a least-privilege basis and governed by the principles of need-to-know and role-based authorisation.

6.1 User Access Management

- All user accounts shall be created, modified, and revoked through a formal access request and approval workflow involving the user's line manager and the IT department.
- Access rights shall be assigned based on approved Role-Based Access Control (RBAC) matrices maintained per system.
- Access reviews shall be conducted every six months. Accounts inactive for more than 60 days shall be automatically disabled.
- Upon termination, transfer, or role change, access shall be revoked or modified within 24 hours of HR notification.

6.2 Privileged Access Management (PAM)

- All privileged accounts (administrators, root, service accounts) shall be governed by a PAM solution.
- Privileged sessions shall be recorded and subject to audit.
- Shared privileged credentials are prohibited. Each administrator shall have a uniquely attributed account.
- Privileged access to OT/ICS systems shall require dual authorisation (four-eyes principle).

6.3 Password Policy

- Minimum password length: 08 characters.
- Complexity: must include uppercase, lowercase, digit, and special character.
- Password expiry: 90 days for standard accounts, 60 days for privileged accounts.
- Account lockout: after 5 failed attempts, until IT reset.

6.4 Remote Access

- All remote access to Rossari systems from overseas locations must be via the approved corporate VPN.

- Split tunnelling is prohibited unless explicitly approved by the Group IT Head for specific business cases.
- Users must not access Company data via public Wi-Fi without VPN.

7. Asset Management

7.1 Asset Inventory

A comprehensive IT asset inventory shall be maintained for all overseas locations, including: hardware (laptops, desktops, servers, mobile devices, network equipment, OT devices), software licences, data assets, and cloud subscriptions. The inventory shall be reviewed at minimum annually and updated within 5 (five) working days of any change.

7.2 Asset Classification

Classification Level	Description	Examples
Confidential	Highly sensitive; restricted to specific named individuals.	Formulation data, trade secrets, M&A documents, PAM credentials
Internal – Restricted	Sensitive; available to authorised staff only.	Financial data, HR records, strategic plans, customer contracts
Internal – General	General internal use; not for public disclosure.	Internal memos, project plans, operational procedures
Public	Approved for external publication.	Marketing materials, published annual reports, press releases

7.3 Asset Ownership

Each asset shall have a designated owner responsible for classification, access authorisation, and disposal. Ownership follows the departmental head responsible for the system or data set.

7.4 Acceptable Use

- IT assets are provided for business purposes. Limited personal use is tolerated provided it does not impact performance, security, or compliance.
- Installation of unauthorised software is strictly prohibited.
- Connecting personal storage devices (USB drives, external HDDs) to Rossari systems requires prior IT approval.

7.5 Asset Disposal

All hardware disposal must follow the Rossari Secure Disposal Procedure: Data shall be wiped or physically destroyed for drives containing Confidential data. A disposal certificate shall be retained.

8. Endpoint Security

- All endpoints (laptops, desktops, servers) must run Company approved endpoint detection and response (EDR) software, kept updated automatically.
- Operating system and application patches must be applied: Critical – within 72 hours, High – within 7 days, Medium – within 30 days, Low – within 90 days.
- Local administrator rights shall not be granted to end users.
- USB ports shall be restricted by default via endpoint policy. Approved removable storage requires IT-issued encrypted devices only.
- Screen lock shall activate after 10 minutes of inactivity. Remote desktop sessions shall time out after 30 minutes of inactivity.

9. Network Security

9.1 Perimeter Security

- All overseas offices shall deploy enterprise-grade firewalls with deep packet inspection, application-layer filtering, and IDS/IPS.
- Firewall rule sets shall be reviewed quarterly. All rules shall have documented business justification, owner, and expiry date.
- External-facing services shall be protected by a Web Application Firewall (WAF) where applicable.

9.2 Network Segmentation

Networks shall be segmented as follows:

- Corporate LAN: general staff systems.
- Server / DMZ zone: servers and services accessible from the internet.
- OT/ICS network: physically or logically isolated from corporate IT. No direct routing between OT and internet.
- Guest / Visitor Wi-Fi: completely isolated with no access to internal resources.
- Management network: infrastructure management (switches, firewalls, UPS) – restricted to IT only.

9.3 Wireless Security

- Corporate Wi-Fi shall use WPA3-Enterprise with certificate-based authentication. WPA2-PSK is not permitted on the corporate SSID.
- Guest Wi-Fi SSIDs shall be isolated on a separate VLAN with internet-only access.
- Rogue access point detection shall be enabled on all wireless controllers.

9.4 WAN / MPLS / SD-WAN

- All site-to-site connectivity between overseas locations and India HQ shall be over IPsec VPN or MPLS with encryption.
- SD-WAN deployments shall enforce traffic policy ensuring that confidential data traffic does not traverse public internet links unencrypted.

10. Data Storage & File Server Policy

All official Company data must be stored on the designated Company server or approved cloud storage platform. Local storage is restricted.

10.1 Mandatory Central Storage

- All Company-related files, documents, reports, software backups, and project data must be stored on the Company server or shared drive only.
- Employees are strictly prohibited from permanently storing official data on: local desktop/laptop drives (C:, D:, E: drives), personal USB drives or external storage devices, personal cloud accounts (personal OneDrive, Google Drive, Dropbox), or personal email accounts.

10.2 Risks of Local Storage

Data stored locally is exposed to: permanent loss due to hardware failure or theft; ransomware and virus attacks; uncontrolled access; and inability to be backed up by IT. IT Department will not be responsible for recovery of data stored on local drives.

10.3 Approved Storage Platforms

- Company file server (mapped network drives).
- Google Drive / Microsoft SharePoint / OneDrive for Business (corporate licensed accounts only).
- ERP document management modules.
- Any other platform explicitly approved in writing by the Group IT Head.

10.4 Data Residency & Sovereignty

For overseas locations, data residency requirements of the host country shall be assessed during site setup. Where local regulations require data to be stored in-country, a compliant local storage or cloud region shall be designated with Group IT Head approval. Cross-border data transfers shall comply with applicable data protection regulations (the Digital Personal Data Protection Act, 2023, GDPR, local equivalents).

11. Data Protection & Privacy

11.1 Data Classification & Handling

All data shall be classified per the framework in Section 72 and handled accordingly. Confidential and Restricted data shall not be transmitted via unencrypted email or stored on unencrypted media.

11.2 Encryption

- Data at rest: AES-256 encryption for all sensitive data storage, including database encryption for ERP and file servers.
- Data in transit: TLS 1.2 or higher for all network communications. TLS 1.0 and 1.1 are prohibited.
- Email containing Confidential data must use S/MIME encryption or be sent via secure file transfer.

11.3 Data Loss Prevention (DLP)

- A DLP solution shall monitor and control outbound data flows across email, web uploads, and removable media.
- DLP policies shall flag and block transfer of defined sensitive content categories (formulation data, financial records, personal data).
- DLP alerts shall be reviewed by the IT Manager within 24 hours.

11.4 Privacy & Regulatory Compliance

- Personal data of employees and customers shall be processed in accordance with applicable privacy laws (GDPR for EU operations, PDPA for Southeast Asia, local equivalents elsewhere, to the extent as applicable).
- A privacy impact assessment shall be conducted for any new system processing personal data.
- Data subject access requests shall be responded to within the regulatory deadline of the applicable jurisdiction.

11.5 Intellectual Property Protection

Formulation data, chemical processes, R&D data, and trade secrets constitute Rossari's most sensitive intellectual property (IP). These shall be classified as Confidential, accessible only on need-to-know basis, encrypted at rest and in transit, and never stored outside approved systems. Any suspected IP breach shall be immediately reported to the Group IT Head and Legal department.

12. Email & Internet Usage Policy

12.1 Email Usage

- Company email accounts are provided for business purposes. Users must not use personal email for Company business.
- Attachments containing confidential data must be password-protected or encrypted before transmission.
- Users must not click links or open attachments from unknown or suspicious sources. Suspicious emails must be reported to IT immediately.
- Auto-forwarding of company email to external addresses is prohibited unless approved by Business Head / Group IT Head.
- Bulk emailing for marketing or commercial purposes must use an approved email marketing platform, not corporate email servers.

12.2 Internet Usage

- Internet access is provided for business use. Personal use is acceptable provided it is not excessive, does not violate this Policy, and does not consume excessive bandwidth.
- Access to the following categories of websites is prohibited: adult / pornographic content, illegal file sharing / torrents, hacking tools and exploit databases, gambling, hate speech and radicalisation content, and any site blacklisted by IT.
- Web browsing through company systems shall be filtered by a Secure Web Gateway (SWG) with URL categorisation and SSL inspection.
- Downloading software or files from untrusted internet sources onto Company devices is prohibited.

12.3 Social Media

- Employees must not share confidential business information, financial data, or unreleased product information on social media platforms or any public forum without approval of corporate communications department and legal department.
- Rossari's official social media accounts shall be managed only by authorised personnel from the marketing or corporate communications department.

13.1 Cloud Governance

- All cloud services used for business purposes must be approved by the IT department prior to adoption. Unauthorised use of cloud platforms (Shadow IT) is prohibited.
- A Cloud Services Register shall be maintained listing all approved cloud services, their classification, data types processed, and contractual terms.

13.2 Cloud Security Controls

- Cloud Security Posture Management (CSPM) tools shall be deployed to monitor cloud configurations against security benchmarks (CIS, NIST).
- Cloud Identity and Access Management (IAM): all cloud accounts shall use MFA, with privileged roles requiring PAM integration.
- Public cloud storage buckets/containers must not be set to public access unless explicitly required and approved.
- Cloud audit logs shall be enabled and forwarded to the central SIEM for monitoring.

13.3 Shared Responsibility

Rossari acknowledges the shared responsibility model of cloud providers. Responsibility for data classification, access control, encryption keys, and application security remains with Rossari regardless of the cloud model (IaaS, PaaS, or SaaS).

13.4 SaaS Usage

- All SaaS applications processing Confidential or Restricted data must be reviewed for security controls, data residency, and compliance certifications (SOC 2, ISO 27001) before approval.
- SaaS vendor contracts must include data processing agreements (DPA), right-to-audit clauses, and breach notification commitments.

14. OT / ICS Security (Chemical Manufacturing Environments)

Rossari's manufacturing operations include chemical plants where operational technology (OT) systems – including SCADA, DCS, PLCs, and HMI – control critical physical processes. A compromise of these systems could cause safety incidents, environmental damage, production loss, or loss of life. This section establishes specific security requirements for OT/ICS environments.

14.1 OT Network Isolation

- OT/ICS networks shall be physically or logically isolated from corporate IT networks. A firewall or data diode shall control any permitted data flows.
- No direct connection between OT networks and the internet is permitted.
- Remote access to OT systems is prohibited by default. Exceptions require Group IT Head + Plant Manager approval, must use an approved jump server/bastion host, must be monitored in real-time, and must be terminated immediately after use.

14.2 OT Asset Management

- A separate OT asset inventory shall be maintained for all ICS/SCADA components, including vendor, firmware version, and EOL/EOS status.
- Firmware and software updates for OT devices shall be tested in a non-production environment before deployment.

14.3 OT Access Control

- Access to OT systems shall follow strict RBAC with dual-authorisation for any configuration changes.
- Default vendor credentials on all OT devices shall be changed immediately upon deployment.
- Vendor/OEM remote support shall be permitted only through a controlled access mechanism with real-time monitoring and session recording.

14.4 OT Incident Response

OT incident response shall be governed by a dedicated OT Incident Response Procedure, approved by the Group IT Head and Plant Safety Officer. Any OT security incident with potential physical safety impact shall trigger immediate escalation to plant management, Group IT Head, and MD.

14.5 OT Vulnerability Management

- OT-specific vulnerability advisories (ICS-CERT, CISA, vendor advisories) shall be monitored continuously.
- Patching in OT environments shall follow change management processes and plant maintenance windows to avoid production disruption.

  NOTE: Given the 24/7 nature of chemical plant operations, some patches may need to wait for planned maintenance shutdowns. A compensating control (e.g., network isolation, monitoring) shall be documented for unpatched vulnerabilities.

15. Backup & Data Restoration Policy

Consistent with Rossari's existing Data Backup & Restoration Policy, the following requirements apply to all overseas locations:

15.1 Backup Rules

- All critical data shall be backed up on Cloud
- Backups shall be immutable (write-once) to protect against ransomware encryption of backup data.
- Backup frequency: Critical systems –continuous incremental; Standard systems – continuous incremental

15.2 Backup Coverage

- All central file servers, ERP databases, and OT historian data included in the backup schedule on need base basis.
- Local laptop/desktop data shall not be subject to IT-managed backup. Users are responsible for ensuring all data is stored on approved central platforms (see Section 10).

15.3 Restore Testing

- Backup restoration tests shall be conducted on need base.
- Any failed restore test must be escalated to the Group IT Head within 24 (twenty-four) hours and a remediation plan actioned within 5 (five) working days.

15.4 Retention

Data Category	Retention Period
Operational / business files	7 years
Financial records	As per applicable statutory requirements (minimum 8 years)
Email archives	5 years
OT historian / process data	10 years (or as required by plant regulations)
Security logs and SIEM data	1 year online, 2 years archived
HR and personnel data	As per local employment law

16. Vulnerability Management

16.1 Scanning

- Automated vulnerability scans shall be conducted at minimum monthly across all IT systems, network infrastructure, and public-facing applications.
- OT/ICS systems shall be scanned using passive scanning tools that do not risk disrupting control systems.
- Vulnerability scan results shall be reviewed by IT within 5 (five) business days of scan completion.

16.2 Patching SLAs

Severity	Patching SLA
Critical (CVSS 9.0–10.0)	Within 72 hours; emergency change procedure.
High (CVSS 7.0–8.9)	Within 7 days.
Medium (CVSS 4.0–6.9)	Within 30 days.
Low (CVSS 0.1–3.9)	Within 90 days or next maintenance window.

16.3 Penetration Testing

- Annual penetration testing of external-facing systems and network perimeter shall be conducted by a qualified third-party provider.
- OT/ICS penetration testing shall be conducted using passive methods only, or on a test/replica environment.
- Penetration test findings shall be risk-rated and remediation tracked through the Risk Register.

16.4 Zero-Day & Threat Intelligence

- The IT Manager shall subscribe to relevant threat intelligence feeds (CERT-In, ICS-CERT, CISA, vendor advisories) and assess applicability within 24 (twenty four) hours of an alert.
- Where a zero-day vulnerability affects a critical system, an emergency risk assessment shall be conducted immediately and appropriate compensating controls implemented pending a patch.

17.1 Log Collection

- All critical systems shall generate and forward security event logs to a centralised SIEM platform. This includes: firewalls and IDS/IPS, servers and endpoints, cloud platforms, OT/ICS systems (where technically feasible), identity management (AD, Azure AD), VPN gateways, and email security gateways.

17.2 Monitoring

- The SIEM shall be configured with detection use cases aligned to the MITRE ATT&CK framework.
- Security alerts shall be triaged by the IT/SOC team. Critical alerts shall generate immediate notification to the on-call IT security resource.
- 24x7 monitoring shall be implemented for critical systems. After-hours monitoring may be handled by an outsourced Managed Security Service Provider (MSSP) where local resources are insufficient.

17.3 Log Retention & Integrity

- Security logs shall be retained for 12 months in the SIEM (hot/warm storage) and archived for an additional 24 months.
- Log integrity shall be protected via write-once storage or cryptographic hashing. Tampering with logs is a serious policy violation.

17.4 Baseline & Anomaly Detection

Behavioural baselines shall be established for users and systems. Significant deviations (e.g., unusual login times, large data transfers, access to unusual resources) shall generate alerts for investigation.

18. Incident Management

18.1 Incident Classification

Severity	Description	Response Time
P1 – Critical	Active breach, ransomware, OT system compromise, or data exfiltration in progress.	Immediate (< 1 hour)
P2 – High	Confirmed breach contained, significant data loss, system outage affecting operations.	< 4 hours
P3 – Medium	Suspected breach, phishing compromise, policy violation with security impact.	< 24 hours
P4 – Low	Minor policy violation, spam incident, no data/system impact.	< 5 business days

18.2 Incident Response Procedure

- Identify & Report: Any employee who discovers or suspects an incident must report it immediately to IT via the designated incident reporting channel.
- Triage: IT assesses severity, classifies the incident, and activates the appropriate response team.
- Contain: Isolate affected systems. Revoke compromised credentials. Block malicious traffic.
- Investigate: Forensic analysis of logs, endpoint artefacts, and network traffic.
- Eradicate: Remove malware, close attack vectors, apply patches or configuration changes.
- Recover: Restore systems from clean backups. Verify integrity before returning to production.
- Post-Incident Review: Root cause analysis, lessons learned, and update to risk register and procedures within 30 days.

18.3 Regulatory Notification

Where an incident involves personal data or triggers regulatory notification obligations (e.g., GDPR 72-hour notification requirement), the IT Manager shall coordinate with Legal and ensure timely notification to relevant authorities and affected individuals.

18.4 Evidence Preservation

- All incident-related data (logs, disk images, memory dumps, network captures) shall be preserved in a forensically sound manner and chain of custody documented.
- Incident evidence shall be retained for a minimum of 3 (three) years or for the duration of any related legal proceedings or as required as per any applicable laws.

19. Third-Party & Supplier Security

19.1 Vendor Risk Assessment

- All third parties with access to Rossari systems, data, or premises shall be subject to a security risk assessment prior to engagement.
- Vendors processing confidential or restricted data shall be assessed against ISO 27001 or SOC 2 standards. Certification is preferred; where not held, compensating controls shall be agreed.

19.2 Contractual Requirements

- All vendor contracts involving data access or IT services shall include: NDA/confidentiality clauses, data protection obligations, security requirements, right-to-audit, breach notification, and data return/deletion obligations on contract termination.

19.3 Third-Party Access Management

- Third-party access to Rossari systems shall use uniquely attributed accounts – shared credentials with vendors are prohibited.
- Vendor access shall be time-limited, tied to the specific engagement, and revoked immediately upon completion.
- Third-party remote access sessions shall be monitored and recorded via PAM or ITSM tooling.

20. Physical & Environmental Security

20.1 Secure Facilities

- All overseas IT server rooms, data closets, and OT control rooms shall be designated as secure areas with physical access control (electronic access card, biometric, or key management system).
- Access logs to secure areas shall be maintained and reviewed monthly.

20.2 Physical Access Control

- Server rooms: access restricted to named IT personnel and senior management. Vendor access requires IT escort and logged entry.
- OT control rooms: access restricted to named plant personnel. IT access for maintenance requires Plant Manager authorisation.
- CCTV coverage shall be maintained at all entry points and server room areas. Footage retained for minimum 90 (ninety) days.

20.3 Environmental Controls

- Server rooms shall maintain appropriate temperature (18–27°C) and humidity (40–60% RH) through dedicated HVAC.
- UPS and generator backup shall provide at minimum 4 hours of power for critical systems. Power transfer tests shall be conducted annually.
- Smoke/fire detection and suppression (clean agent preferred for IT rooms) shall be installed and tested annually.

20.4 Clean Desk & Screen Lock

- Employees must not leave sensitive documents or materials unattended at workstations.
- Screens must be locked when leaving a workstation (mandatory screen lock after 10 minutes – see Section 9).
- Whiteboards and display screens must be cleared of sensitive information after meetings.

21. Compliance, Audit & Regulatory Requirements

21.1 Legal & Regulatory Compliance

Overseas operations shall maintain awareness of and comply with applicable local cybersecurity, data protection, and employment laws. Key jurisdictions and examples include:

Region / Jurisdiction	Relevant Regulation
European Union	GDPR (General Data Protection Regulation), NIS2 Directive
United States	CCPA (California), SOX (if applicable), NIST CSF
Southeast Asia	PDPA (Thailand, Singapore, Malaysia), CSA (Singapore)
United Kingdom	UK GDPR, Data Protection Act 2018
Middle East	PDPL (UAE, Saudi Arabia)
India (HQ reference)	IT Act 2000, DPDP Act 2023, CERT-In Guidelines

21.2 Internal Audit

- Audits shall assess compliance with this Policy and all subordinate policies.
- Audit findings shall be risk-rated and remediation tracked through an Audit Action Register.

21.3 Compliance Tracking

- A Compliance Register shall be maintained tracking regulatory obligations, deadlines, and evidence of compliance.
- The ISMS Manager shall report compliance status to the Steering Committee quarterly.

22. Policy Violations & Disciplinary Action

Any breach or violation of this Policy shall be treated seriously and investigated promptly. Rossari is committed to fair and proportionate enforcement.

22.1 Reporting Violations

- Any employee who becomes aware of a policy violation or suspected violation must report it immediately to the IT department or ISMS Manager.
- Reports may be made through the ITSM ticketing system, direct email to the Group IT Head, or via the anonymous reporting channel.

22.2 Investigation

- All reported violations shall be investigated by IT and HR jointly.
- The subject of the investigation will be notified and given opportunity to respond unless doing so would compromise the investigation.
- Investigations shall be documented and findings preserved for potential legal proceedings.

22.3 Consequences

Violation Type	Consequences
Accidental/minor violation (first occurrence)	Formal warning, mandatory remedial training, documented in HR file.
Repeat or negligent violation	Written warning, increased monitoring, potential suspension of IT access.
Deliberate or serious violation (e.g., data theft, intentional breach)	Termination of employment, potential civil and/or criminal legal action.
Vendor/contractor violation	Immediate access revocation, contract termination, escalation to legal.

Nothing in this section prevents Rossari from pursuing civil, criminal or other legal remedies available for violations that constitute illegal acts.

23.1 Review Cycle

This Policy shall be reviewed at minimum once in 2 (two) years by the Group IT Head and ISMS Manager. Reviews shall also be triggered by: significant changes to IT systems or architecture, new regulatory requirements, major security incidents, changes in Rossari's overseas footprint.

23.2 Review Process

- The ISMS Manager shall initiate the review and prepare a redlined draft with proposed changes.
- Proposed changes shall be reviewed by the ISMS Steering Committee.
- Approved revisions shall be documented in the Revision History table.
- Revised Policy shall be distributed to all staff and acknowledged.

24. Artificial Intelligence (AI) & Generative AI Usage

The use of public and third-party Artificial Intelligence (AI) and Generative AI tools introduces material risks of unauthorised disclosure of confidential, proprietary, and regulated information. This section establishes mandatory controls governing the use of such tools by all personnel covered under this Policy.

24.1 Prohibited Use of Public AI Tools

Employees, contractors, and third parties shall not upload, paste, or otherwise input any of the following into public or unauthorised AI/Generative AI tools (including but not limited to ChatGPT, Google Gemini, Microsoft Copilot, DeepSeek, and similar publicly hosted services) without prior written authorisation from the IT Department:

- Company confidential, proprietary, or trade secret information.
- Chemical formulations, recipes, process parameters, R&D data, and laboratory or pilot-plant results.
- Customer data, supplier data, pricing, or other commercially sensitive business information.
- Financial records, budgets, forecasts, and unpublished financial results.
- Contracts, legal agreements, and any documents marked Confidential or Internal Use Only.
- Personal data of employees, customers, or other individuals, including any information that could enable identification of a data subject.

This restriction applies regardless of the device, network, or account used, including personal accounts accessed from corporate devices and corporate accounts accessed from personal devices.

24.2 Approved AI Platforms & Usage Guidelines

- The IT Department, in consultation with the ISMS Steering Committee, shall maintain and publish a list of approved AI and Generative AI platforms authorised for business use, including any enterprise or contractually governed AI offerings.
- Only AI platforms covered by an enterprise agreement with appropriate data protection, confidentiality, and non-training (opt-out of model training on submitted data) terms shall be approved for use with business data.
- Any new request to use an AI tool for business purposes shall be submitted to the IT Department for risk assessment and approval prior to use.
- Outputs generated by AI tools shall be independently verified for accuracy before being relied upon for business, regulatory, or technical decisions.
- Use of AI coding assistants on Rossari source code, scripts, or system configurations is permitted only via approved platforms, with no proprietary code submitted to public/free-tier AI services.
- Suspected unauthorised use of AI tools involving confidential or regulated data shall be reported immediately in accordance with Section 19 (Incident Management).

25. BYOD (Bring Your Own Device) Protection

Where personal devices are permitted to access Rossari email, applications, or data ("BYOD"), the controls in this section shall apply in addition to all other applicable provisions of this Policy.

25.1 Employee Consent & Enrolment

- Prior to enabling corporate email or application access on a personal device, the employee shall sign a BYOD Consent Form acknowledging enrolment in Mobile Device Management (MDM) and the conditions set out in this section.
- The Consent Form shall clearly disclose the scope of MDM enrolment, the remote wipe capability, and the nature and extent of compliance monitoring to be performed on the device.
- Access shall not be granted, and may be revoked, where consent is withheld or withdrawn.

25.2 Mobile Device Management (MDM)

- All personal devices used to access corporate email, applications, or data shall be enrolled in the corporate MDM solution prior to access being granted.
- MDM shall enforce minimum security baselines on enrolled devices, including device passcode/biometric lock, encryption, and a containerised work profile separating corporate data and applications from personal content.

25.3 Remote Wipe of Corporate Data

- IT shall have the right to perform a selective remote wipe of corporate data, applications, and email from an enrolled personal device upon employee separation, device loss or theft, suspected compromise, or non-compliance with this Policy.
- Selective wipe shall be scoped to the corporate container only and shall not knowingly remove personal photos, contacts, or applications outside that container.
- A full device wipe may be performed only with employee consent or where required by law, except where the device cannot be selectively wiped and corporate data is at material risk.

25.4 Compliance Monitoring

- IT shall monitor enrolled devices only for security and policy compliance attributes (e.g., OS patch level, encryption status, jailbreak/root detection, presence of required security controls) and shall not monitor personal communications, browsing history, or personal applications.
- Non-compliant devices shall be automatically restricted from accessing corporate resources until remediated.

25.5 Employee Responsibilities

- Employees shall report a lost or stolen device enrolled in BYOD to IT immediately, and no later than 12 (twelve) hours of discovery.
- Employees shall not attempt to circumvent, disable, or remove MDM controls on an enrolled device while corporate data resides on it.
- Personal devices shall not be used to store local, unencrypted copies of corporate data; access shall be limited to approved containerised applications.

Appendix A – Related Policies & Documents

Document	Reference	Owner
Rossari Information Security Policy	ROSSARI-IT-IS-POL-006	IT Department
Data Backup & Restoration Policy	Rossari-IT-BKP-POL-002	IT Department
Company Data Storage & VPN Access Policy	Rossari-IT-VPN-POL-003	IT Department
IT Assets Management Policy	Rossari-IT-AST-POL-004	IT Department
Email Policy	Rossari-IT-EML-POL-005	IT Department
Internet Usage Policy	Rossari-IT-INT-POL-007	IT Department
OT/ICS Incident Response Procedure	Rossari-IT-OT-IRP-001	IT / Plant Safety
Secure Disposal Procedure	Rossari-IT-DSP-PRO-001	IT Department
ISMS Statement of Applicability	Rossari-ISMS-SOA-001	ISMS Manager
IT Risk Register	Rossari-ISMS-RR-001	ISMS Manager

Appendix B – ISO/IEC 27001:2022 Clause Mapping

Policy Section	ISO 27001:2022 Clause / Annex A Controls
Section 4 – Governance	Clause 5 (Leadership), A.5.2
Section 5 – Objectives	Clause 6.2
Section 6 – Risk Management	Clauses 6.1.2, 6.1.3, 8.2, 8.3
Section 7 – Access Control	A.5.15, A.5.16, A.5.17, A.5.18

Policy Section	ISO 27001:2022 Clause / Annex A Controls
Section 8 – Asset Management	A.5.9, A.5.10, A.5.11, A.5.12, A.5.13, A.5.14
Section 9 – Endpoint Security	A.8.1, A.8.7
Section 10 – Network Security	A.8.20, A.8.21, A.8.22, A.8.23
Section 12 – Data Protection	A.5.12, A.5.13, A.5.34, A.8.24
Section 14 – Cloud Security	A.5.23
Section 15 – OT/ICS Security	A.8.21, A.8.22 (extended to OT)
Section 16 – Backup	A.8.13
Section 17 – DR / BCP	A.5.29, A.5.30
Section 18 – Vulnerability Mgmt	A.8.8
Section 19 – Logging & Monitoring	A.8.15, A.8.16
Section 20 – Incident Management	A.5.24, A.5.25, A.5.26, A.5.27, A.5.28
Section 21 – Supplier Security	A.5.19, A.5.20, A.5.21, A.5.22
Section 22 – Physical Security	A.7.1–A.7.13
Section 23 – Security Awareness	A.6.3
Section 24 – Compliance & Audit	Clause 9.2, A.5.33, A.5.35, A.5.36
Section 26 – Continuous Improvement	Clause 10

Appendix C – Incident Reporting Contact Details

Contact	Method	Availability
IT Helpdesk	It-helpdesk@rossari.com / ITSM Portal	Business Hours

Employee Acknowledgement

I acknowledge that I have read, understood, and agree to comply with the Global Overseas IT Policy (Rossari-IT-OVS-POL-001) of Rossari. I understand that non-compliance may result in disciplinary action as described in Section 25.

Field	Details
Full Name	
Employee / Contractor ID	
Department	
Location / Site	
Date	
Signature	