CYBERCORP
Firewall to a secure world

CYBERCORP LIMITED

3C, Camac Street, Kolkata-700016 India

ETHICS, COMPLIANCE & GOVERNANCE (ECG) POLICY

(Group-Wide Master Policy aligned with ISO/IEC 27001:2022, CMMI, ESG Principles, and SEBI Corporate Governance Norms)

1. INTRODUCTION AND PHILOSOPHICAL FOUNDATION

CyberCorp Limited ("CyberCorp" or "the Company") recognizes that in an era defined by digital transformation, cybersecurity, data sovereignty, and global regulatory scrutiny, **ethical conduct, compliance discipline, and governance maturity** are not optional attributes but essential conditions for legitimacy, trust, and long-term sustainability.

As a holding company overseeing multiple technology-driven subsidiaries operating across sensitive domains including cybersecurity, software platforms, data intelligence, public infrastructure, healthcare, education, and defence-adjacent environments, CyberCorp bears a heightened responsibility to ensure that **every action, decision, and process across the Group reflects the highest standards of integrity, legality, transparency, and accountability**.

This Ethics, Compliance & Governance (ECG) Policy is therefore not merely a compliance document but a **foundational charter** that codifies the values, responsibilities, controls, and expectations governing the CyberCorp Group.

2. PURPOSE AND OBJECTIVES OF THE POLICY

The objectives of this Policy are to:

1. Establish a **uniform ethical and governance framework** across CyberCorp and all group entities
2. Ensure full compliance with applicable **laws, regulations, and standards**
3. Protect **information assets, intellectual property, financial resources, and reputation**
4. Define **clear accountability and oversight mechanisms**
5. Embed **risk-based thinking and process maturity** across operations
6. Support **ISO/IEC 27001 certification and CMMI maturity goals**
7. Enable credible **ESG governance disclosures**
8. Align internal governance with **SEBI-style best practices**, irrespective of listing status

3. APPLICABILITY AND SCOPE

3.1 Group Applicability

This Policy applies mandatorily to:

- **CyberCorp Limited**
- All subsidiaries, affiliates, associate companies, joint ventures, and special-purpose entities, including but not limited to:
    - Sundyne Technologies Private Limited
    - Sundyne Innovations Private Limited
    - AGTS CCL Private Limited
    - Paramaah CCL Private Limited

Each subsidiary shall adopt this Policy **in toto**, without dilution.

3.2 Persons Covered

This Policy is binding on:

- Directors and Key Managerial Personnel
- Officers and employees (permanent, temporary, contractual)
- Consultants, advisors, interns, and trainees
- Vendors, service providers, partners, and third parties acting for or on behalf of the Group

4. GOVERNANCE PRINCIPLES (SEBI & ESG ALIGNED)

CyberCorp's governance architecture is founded on the following principles:

- **Ethical Leadership and Integrity**
- **Accountability and Fiduciary Responsibility**
- **Transparency and Truthful Disclosure**
- **Fairness and Stakeholder Equity**
- **Risk Awareness and Control Orientation**
- **Compliance Embedded by Design**

These principles align with **SEBI Regulation 4**, OECD governance principles, and ESG governance expectations.

5. BOARD OF DIRECTORS – ROLE AND RESPONSIBILITIES

5.1 Fiduciary Duties

The Board of Directors shall act in accordance with the duties of:

- Care
- Loyalty
- Prudence
- Good faith

Directors shall at all times act in the best interests of the Company and its stakeholders.

5.2 Oversight Responsibilities

The Board shall:

- Set the ethical tone and governance culture
- Approve policies, strategies, and risk appetite
- Oversee compliance, audit, and information security
- Ensure integrity of financial and non-financial disclosures

5.3 Committees

The Board may constitute:

- Audit & Compliance Committee
- Risk Management & Information Security Committee
- Ethics & Whistleblower Committee

Each committee shall function with defined charters and reporting obligations.

6. ROLE OF SENIOR MANAGEMENT

Senior management shall:

- Implement Board-approved policies
- Allocate adequate resources for compliance and security
- Ensure operational adherence to laws and standards
- Promote ethical conduct and accountability at all levels

Failure of senior management to prevent or address violations shall be treated as a governance lapse.

7. ETHICAL CONDUCT AND BUSINESS INTEGRITY

7.1 Standards of Conduct

All covered persons shall:

- Act honestly, transparently, and responsibly
- Avoid fraud, deception, concealment, or misrepresentation
- Conduct business solely in the Company's legitimate interest

7.2 Conflict of Interest

- All actual or potential conflicts must be disclosed immediately
- Directors and senior executives shall make annual disclosures
- Any conflicted person shall recuse themselves from decision-making

7.3 Anti-Bribery and Anti-Corruption

CyberCorp adopts **zero tolerance** towards corruption.

- No bribes, kickbacks, facilitation payments, or inducements
- Strict compliance with Prevention of Corruption Act, IPC, and international anti-corruption laws
- Gifts and hospitality only if modest, transparent, and pre-approved

8. LEGAL AND REGULATORY COMPLIANCE

CyberCorp and its subsidiaries shall comply with all applicable laws, including but not limited to:

- Companies Act, 2013
- SEBI regulations and corporate governance norms
- Labour and employment laws
- Taxation laws
- Information Technology Act, 2000
- Intellectual Property laws
- Sector-specific regulatory frameworks

Ignorance of law is not a defence.

9. INFORMATION SECURITY & DATA GOVERNANCE (ISO/IEC 27001 CORE)

CyberCorp shall operate a **Group-wide Information Security Management System (ISMS)**.

9.1 Asset Identification and Classification

- All information assets shall be identified and classified
- Ownership and protection responsibilities assigned

9.2 Access Control

- Role-based access
- Least-privilege principle
- Secure authentication and authorization mechanisms

9.3 Secure Development and Operations

- Secure Software Development Lifecycle (SSDLC)
- Configuration and change management
- Logging, monitoring, and audit trails

9.4 Incident Management

- Defined incident response procedures
- Mandatory breach reporting
- Root cause analysis and corrective actions

9.5 Exit Management and Data Surrender

Upon cessation of engagement:

- Immediate surrender of all assets and data
- No retention, copying, or backups permitted
- Written confirmation of deletion required

Any violation shall constitute **gross misconduct**, **breach of trust**, and **criminal offence**.

10. INTELLECTUAL PROPERTY GOVERNANCE

- All IP created during engagement belongs exclusively to the Company
- No unauthorized use, disclosure, or transfer
- Strict protection of source code, repositories, designs, algorithms, and trade secrets

11. PROCESS GOVERNANCE & QUALITY (CMMI ALIGNMENT)

CyberCorp adopts a **process-centric governance model**, including:

- Organizational Process Definition (OPD)
- Risk Management (RSKM)
- Configuration Management (CM)
- Verification and Validation (VER/VAL)
- Measurement and Analysis (MA)

Continuous improvement is mandatory and auditable.

12. ESG – ENVIRONMENTAL, SOCIAL & GOVERNANCE COMMITMENTS

12.1 Environmental Responsibility

- Resource efficiency
- Energy conservation
- E-waste management
- Environmentally responsible procurement

12.2 Social Responsibility

- Equal opportunity and non-discrimination
- Safe and inclusive workplace
- Respect for dignity and human rights
- Community engagement and skill development

12.3 Governance

- Ethical leadership
- Transparent reporting
- Stakeholder accountability

13. WHISTLEBLOWER MECHANISM

- Confidential reporting channels
- Protection against retaliation
- Independent and impartial investigation

Aligned with **SEBI Regulation 22** and ESG governance standards.

14. FINANCIAL INTEGRITY & ASSET PROTECTION

- Accurate books and records

- Prevention of fraud and misappropriation
- Internal and statutory audits

15. THIRD-PARTY AND VENDOR GOVERNANCE

- Due diligence before engagement
- Contractual compliance and audit rights
- Termination for violations

16. MONITORING, AUDIT & ENFORCEMENT

- Periodic internal audits
- Compliance reviews
- Disciplinary and legal action for violations

Consequences may include termination, recovery, civil and criminal proceedings.

17. TRAINING, AWARENESS & ACKNOWLEDGEMENT

All covered persons shall:

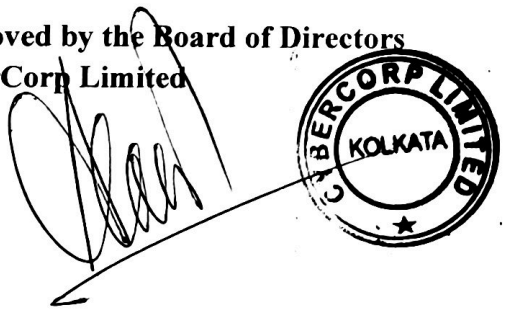
- Undergo periodic training
- Acknowledge compliance
- Support audits and investigations

18. POLICY REVIEW AND AMENDMENT

- Policy Owner: Board of Directors, CyberCorp Limited
- Annual review or earlier if required
- Binding on all subsidiaries

This ECG Policy constitutes the **governance backbone of the CyberCorp Group**. It reflects CyberCorp's commitment to ethical excellence, regulatory compliance, information security, process maturity, ESG responsibility, and sustainable growth.

Approved by the Board of Directors
CyberCorp Limited



CYBERCORP
Firewall to a secure world

ANNEXURE – A

ISO/IEC 27001:2022 CONTROL-TO-POLICY MAPPING

(Mapping of ISO/IEC 27001 Controls to CyberCorp ECG Policy)

Purpose of Annexure

This Annexure demonstrates how the **Ethics, Compliance & Governance (ECG) Policy of CyberCorp Limited** satisfies and operationalizes the requirements of **ISO/IEC 27001:2022**, including **Clauses 4–10** and **Annex A controls**.

This mapping confirms that the ECG Policy functions as a **top-level governance and control document** within CyberCorp's Information Security Management System (ISMS).

SECTION I – ISO/IEC 27001:2022 MANAGEMENT SYSTEM CLAUSES

Clause 4 – Context of the Organization

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
4.1	Understanding the organization and its context	Sections 1, 2, 3	Policy defines CyberCorp's operating context, regulatory environment, subsidiaries, and risk exposure
4.2	Understanding needs of interested parties	Sections 4, 12, 13	Stakeholders including employees, customers, regulators, investors, and partners identified
4.3	Determining scope of ISMS	Sections 3, 9	Group-wide applicability covering all subsidiaries and operations
4.4	ISMS establishment	Sections 8, 16, 18	Policy mandates enterprise-wide ISMS and continuous governance

Clause 5 – Leadership

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
5.1	Leadership and commitment	Sections 5, 6	Board and senior management accountability clearly defined
5.2	Information security policy	Entire ECG Policy	ECG Policy acts as overarching security & governance policy
5.3	Roles and responsibilities	Sections 5, 6, 16	Defined governance structure, committees, and ownership

Clause 6 – Planning

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
6.1	Risk assessment and treatment	Sections 8, 11, 16	Risk-based approach embedded through ISMS & CMMI alignment
6.2	Information security objectives	Sections 2, 9, 18	Policy objectives aligned to security, compliance, and resilience

Clause 7 – Support

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
7.1	Resources	Sections 6, 9, 17	Management responsibility to allocate resources
7.2	Competence	Section 17	Mandatory training and awareness
7.3	Awareness	Sections 7, 17	Ethics, security, and compliance awareness mandated
7.4	Communication	Sections 11, 13	Whistleblower and reporting channels
7.5	Documented information	Sections 11, 16	Document control and audit readiness

Clause 8 – Operation

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
8.1	Operational planning & control	Sections 8, 11, 15	Secure operations, process control, vendor governance

Clause 9 – Performance Evaluation

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
9.1	Monitoring, measurement, analysis	Sections 11, 14	Internal audits and compliance reviews
9.2	Internal audit	Section 14	Periodic ISMS and compliance audits
9.3	Management review	Sections 5, 18	Board-level review and oversight

Clause 10 – Improvement

ISO Clause	Requirement	ECG Policy Reference	Alignment Explanation
10.1	Nonconformity & corrective action	Sections 14, 16	Disciplinary and corrective measures
10.2	Continual improvement	Sections 11, 18	Continuous improvement mandated

SECTION II – ISO/IEC 27001:2022 ANNEX A CONTROL MAPPING

A.5 – Organizational Controls

Control	Description	ECG Policy Reference
A.5.1	Policies for information security	Entire ECG Policy
A.5.2	Information security roles	Sections 5, 6
A.5.3	Segregation of duties	Sections 5, 11
A.5.7	Threat intelligence	Sections 8, 9
A.5.8	Information security in project management	Sections 9, 11
A.5.23	Information security for cloud services	Sections 8, 15

A.6 – People Controls

Control	Description	ECG Policy Reference
A.6.1	Screening	Section 7
A.6.2	Terms & conditions of employment	Sections 7, 9
A.6.3	Information security awareness	Section 17
A.6.4	Disciplinary process	Section 14
A.6.5	Responsibilities after termination	Section 9.5

A.7 – Physical Controls

Control	Description	ECG Policy Reference
A.7.1	Physical security perimeters	Section 8
A.7.2	Physical entry controls	Section 8
A.7.4	Equipment protection	Sections 8, 9

A.8 – Technological Controls

Control	Description	ECG Policy Reference
A.8.1	User access management	Section 9.2
A.8.2	Privileged access	Section 9.2
A.8.3	Information access restriction	Section 9

A.8.7	Malware protection	Section 8
A.8.9	Configuration management	Section 11
A.8.10	Information deletion	Section 9.5
A.8.11	Data masking	Section 9
A.8.12	Data leakage prevention	Sections 9, 10
A.8.15	Logging and monitoring	Section 9.3
A.8.23	Web filtering	Section 8
A.8.24	Cryptography	Section 9

SECTION III – STATEMENT OF APPLICABILITY (SoA) NOTE

- All Annex A controls are **applicable** to CyberCorp Limited and its subsidiaries unless explicitly excluded through risk assessment.
- The ECG Policy serves as the **top-level control document**.
- Detailed SOPs, procedures, and technical standards shall be maintained as subordinate documents.

SECTION IV – AUDIT & CERTIFICATION NOTE

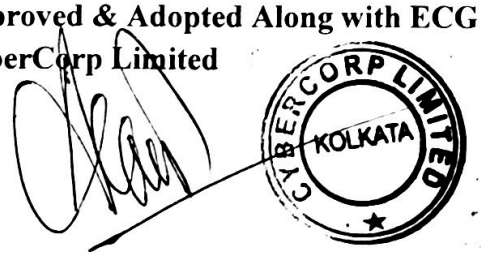
This Annexure demonstrates:

- Leadership commitment (Clause 5)
- Risk-based governance (Clause 6)
- Operational security control (Annex A)
- Continuous improvement (Clause 10)

It is suitable for:

- Stage 1 & Stage 2 ISO audits
- Surveillance audits
- Internal ISMS reviews

Approved & Adopted Along with ECG Policy
CyberCorp Limited



CYBERCORP
Firewall to a secure world

ANNEXURE – B

CMMI PROCESS ALIGNMENT MATRIX

(Mapping of CMMI Process Areas to CyberCorp ECG Policy)

1. PURPOSE OF ANNEXURE

This Annexure demonstrates how the **Ethics, Compliance & Governance (ECG) Policy of CyberCorp Limited** aligns with and supports the **Capability Maturity Model Integration (CMMI)** framework, specifically **CMMI for Development (DEV)** and **CMMI for Services (SVC)**, at **Maturity Level 3 and above**.

The ECG Policy functions as a **top-level governance and institutionalization document**, ensuring that CMMI practices are **defined, implemented, managed, and continuously improved** across CyberCorp Limited and all its subsidiaries.

2. CMMI MATURITY LEVEL CONTEXT

CMMI Level	Relevance to ECG Policy
Level 2 – Managed	Governance, monitoring, and compliance controls
Level 3 – Defined	Standardized, organization-wide processes
Level 4 – Quantitatively Managed	Measurement & analysis discipline
Level 5 – Optimizing	Continuous improvement & innovation

The ECG Policy primarily enables **Level 3 institutionalization**, while supporting Levels 4 & 5 through governance and measurement mandates.

3. GOVERNANCE & ORGANIZATIONAL PROCESS MANAGEMENT

OPF – Organizational Process Focus

CMMI Practice	ECG Policy Reference	Alignment Explanation
Establish process improvement objectives	Sections 2, 11, 18	Policy mandates continuous improvement
Assess strengths and weaknesses	Sections 14, 16	Internal audits and reviews
Deploy process improvements	Sections 11, 16	Board-approved process governance

OPD – Organizational Process Definition

CMMI Practice	ECG Policy Reference	Alignment Explanation
Establish standard processes	Sections 9, 11	Defined, documented, auditable processes

Tailoring guidelines	Sections 3, 11	Group-wide policy with subsidiary SOPs
Process asset library	Sections 11, 16	Controlled documentation

4. PROJECT & SERVICE MANAGEMENT

PP – Project Planning

CMMI Practice	ECG Policy Reference	Alignment Explanation
Establish project plans	Sections 9, 11	Structured planning and governance
Estimate scope, cost, schedule	Sections 9, 12	Financial discipline & risk awareness

PMC – Project Monitoring & Control

CMMI Practice	ECG Policy Reference	Alignment Explanation
Monitor progress	Sections 14, 16	Periodic reviews & audits
Corrective action	Sections 14, 18	Defined escalation and remediation

SAM – Supplier Agreement Management

CMMI Practice	ECG Policy Reference	Alignment Explanation
Select suppliers	Sections 15	Due diligence & vendor governance
Manage supplier agreements	Sections 15	Compliance and audit rights

5. ENGINEERING PROCESS AREAS (DEV)

REQM – Requirements Management

CMMI Practice	ECG Policy Reference	Alignment Explanation
Manage requirements	Sections 9, 11	Controlled documentation & traceability
Manage changes	Sections 9.3, 11	Configuration management

TS – Technical Solution

CMMI Practice	ECG Policy Reference	Alignment Explanation
Design solutions	Sections 9, 10	Secure SDLC & IP governance
Implement solutions	Sections 8, 9	Controlled development practices

PI – Product Integration

CMMI Practice	ECG Policy Reference	Alignment Explanation
Integrate components	Sections 9, 11	Change and configuration control

VER – Verification

CMMI Practice	ECG Policy Reference	Alignment Explanation
Verify work products	Sections 11, 14	Audit, review, and validation

VAL – Validation

CMMI Practice	ECG Policy Reference	Alignment Explanation
Validate products	Sections 11, 14	Customer and stakeholder validation

6. SUPPORT PROCESS AREAS

CM – Configuration Management

CMMI Practice	ECG Policy Reference	Alignment Explanation
Identify configuration items	Sections 9, 11	Asset and configuration control
Control changes	Sections 9.3, 11	Change management
Status accounting	Sections 14, 16	Audit and traceability

MA – Measurement & Analysis

CMMI Practice	ECG Policy Reference	Alignment Explanation
Define measures	Sections 12, 16	Metrics and performance monitoring
Analyze data	Sections 14, 16	Reviews and management reporting

PPQA – Process & Product Quality Assurance

CMMI Practice	ECG Policy Reference	Alignment Explanation
Evaluate adherence	Sections 14, 16	Compliance audits
Report non-compliance	Sections 11, 14	Escalation mechanisms

7. RISK MANAGEMENT (RSKM)

CMMI Practice	ECG Policy Reference	Alignment Explanation
Identify risks	Sections 8, 11	Risk-based ISMS and governance
Analyze and mitigate risks	Sections 8, 11, 18	Defined mitigation & corrective action

8. DECISION ANALYSIS & RESOLUTION (DAR)

CMMI Practice	ECG Policy Reference	Alignment Explanation
Structured decision-making	Sections 5, 6	Board oversight and approval mechanisms
Evaluate alternatives	Sections 5, 11	Risk and compliance driven decisions

9. CONTINUOUS IMPROVEMENT & OPTIMIZATION

CMMI Practice	ECG Policy Reference	Alignment Explanation
Institutionalize improvements	Sections 11, 18	Policy-driven improvement cycle
Learn from performance	Sections 14, 16	Audits and reviews

10. INSTITUTIONALIZATION & GOVERNANCE EVIDENCE

The ECG Policy supports CMMI institutionalization through:

- **Defined policies and governance structures**
- **Role clarity and accountability**
- **Audit and compliance enforcement**
- **Training and awareness mandates**
- **Management oversight and review**

11. APPRAISAL & AUDIT NOTE

This Annexure may be used as:

- **High-level evidence** during CMMI appraisals
- Input to **Process Asset Library (PAL)**
- Mapping document for **SCAMPI / Benchmark appraisals**

Detailed SOPs, metrics, and project artefacts shall provide **practice-level evidence.**

Approved & Adopted Along with ECG Policy
CyberCorp Limited

CYBERCORP LIMITED KOLKATA