

# Compliance Handbook

*Art Technology & Software Company*

## 1. Purpose & Scope

This Compliance Handbook establishes the principles, policies, and procedures to ensure that **Art Technology & Software** operates ethically, legally, and responsibly across all business activities.

This handbook applies to:

- Employees (full-time, part-time, interns)
- Contractors & consultants
- Vendors and third-party partners
- Management and leadership

---

## 2. Core Compliance Principles

We are committed to:

- **Legal compliance** in all jurisdictions of operation
- **Ethical conduct** and professional integrity
- **Data privacy and security**
- **Responsible AI & technology usage**
- **Respect for intellectual property**
- **Transparent business practices**

---

## 3. Legal & Regulatory Compliance

Employees must comply with all applicable laws, including but not limited to:

- Information Technology laws
- Data protection and privacy regulations
- Intellectual Property (IP) laws
- Employment and labor laws
- Cybersecurity regulations
- Contract and commercial laws

Failure to comply may result in disciplinary action, including termination.

---

## **4. Code of Conduct**

All employees are expected to:

- Act honestly and responsibly
  - Avoid conflicts of interest
  - Maintain professionalism with clients, partners, and colleagues
  - Refrain from harassment, discrimination, or abusive behavior
  - Protect company reputation in public and digital spaces
- 

## **5. Data Protection & Privacy Compliance**

### **5.1 Personal Data Handling**

- Collect only necessary data for legitimate business purposes
- Use data only for authorized purposes
- Store data securely using approved systems
- Do not share sensitive data without authorization

### **5.2 Applicable Standards**

- GDPR (where applicable)
  - Local Data Protection Acts
  - Client-specific data protection agreements
- 

## **6. Information Security Policy**

Employees must:

- Use strong passwords and multi-factor authentication
  - Access systems strictly on a need-to-know basis
  - Report security incidents immediately
  - Avoid using unauthorized software or hardware
  - Follow secure coding and DevSecOps practices
- 

## **7. Responsible Use of AI & Emerging Technologies**

Art Technology & Software commits to **ethical and responsible AI use**:

- AI systems must not violate privacy, bias, or discrimination laws
- Training data must be legally sourced and authorized
- Generated content must respect copyright and IP rights

- AI outputs must be reviewed before external use
  - No deployment of AI systems that cause harm or deception
- 

## 8. Intellectual Property (IP) Compliance

### 8.1 Company IP

- All work created during employment is company property
- Source code, models, datasets, designs, and documents are protected assets

### 8.2 Third-Party IP

- Respect open-source licenses
  - Do not use pirated software or unauthorized assets
  - Attribute and comply with licensing terms
- 

## 9. Software Development Compliance

All development activities must follow:

- Secure coding standards
  - Version control and code review processes
  - License compliance for dependencies
  - Documentation and audit trails
  - Quality assurance and testing protocols
- 

## 10. Client & Contract Compliance

Employees must:

- Adhere strictly to client contracts and SLAs
  - Protect client confidential information
  - Avoid unauthorized commitments or representations
  - Follow export control and cross-border data transfer rules
- 

## 11. Anti-Bribery & Anti-Corruption Policy

- No offering, accepting, or soliciting bribes or kickbacks
- Gifts or hospitality must be modest and approved
- Comply with anti-corruption laws (e.g., Prevention of Corruption Act)

---

## **12. Workplace Compliance**

### **12.1 Equal Opportunity**

- No discrimination based on gender, caste, religion, age, disability, or background

### **12.2 POSH & Harassment Prevention**

- Zero tolerance for sexual harassment
- Mandatory reporting and investigation procedures
- Compliance with POSH Act (India) and equivalent laws

---

## **13. Use of Company Resources**

Employees must:

- Use company devices and tools for business purposes only
- Avoid misuse of email, internet, or cloud resources
- Not install unauthorized software or extensions

---

## **14. Third-Party & Vendor Compliance**

- Vendors must meet security and compliance standards
- NDAs and data processing agreements are mandatory
- Regular vendor risk assessments may be conducted

---

## **15. Reporting Violations & Whistleblower Policy**

Employees are encouraged to report:

- Legal violations
- Data breaches
- Ethical misconduct
- Security incidents

Reports can be made confidentially without fear of retaliation.

---

## **16. Audits & Monitoring**

- Internal audits may be conducted periodically
  - Logs, system access, and activities may be monitored
  - Cooperation with audits is mandatory
- 

## **17. Disciplinary Actions**

Non-compliance may result in:

- Verbal or written warnings
  - Suspension
  - Termination
  - Legal action where applicable
- 

## **18. Training & Awareness**

- Mandatory compliance training for all employees
  - Periodic refresher sessions
  - Updates on regulatory or policy changes
- 

## **19. Policy Review & Updates**

This handbook will be reviewed periodically and updated to reflect:

- Changes in laws
  - New technologies
  - Business or regulatory requirements
- 

## **20. Acknowledgement**

All employees must acknowledge that they:

- Have read and understood this Compliance Handbook
- Agree to comply with all policies and procedures