



ZYETA

ZYETA INTERIORS PVT. LTD.

201, #2/3, Alfred St, Richmond Town, Bengaluru,
Karnataka-560025, India.

ESG- Policy Manual - IT

	Name	Signature
Prepared by	Akshay BP Studio Director	
Approved by	Shilpa Revankar Co-Founder	

DOC NO : ZYETA/ESG/POLICY

ISSUE NO : 02

REV NO : 00

INITIAL ISSUE DATE : 5th February, 2023

FIRST ANNUAL REVIEW DATE: 5th February, 2024

AMENDMENT SHEET

Date	Issue No	Rev No	Reason	Remarks
5 th March, 2023	01	00	INITIAL ISSUE DATE	-
5 th March, 2024	02	00	FIRST ANNUAL REVIEW DATE	-

TABLE OF CONTENT

SL.NO	DESCRIPTION	PAGE NO
ZYETA/ESG/P-01	INFORMATION SECURITY POLICY	04

INFORMATION SECURITY POLICY

ZYETA/ESG/P-01

1. Introduction

Zyeta, a leading design consultation and project management company in India, understands the critical importance of information security in the modern, digital, and interconnected world. With our core competency in providing Building Information Modeling (BIM) and sustainability management systems, we handle large amounts of sensitive and confidential data. As such, protecting this data from unauthorized access, use, disclosure, disruption, modification, or destruction is a priority for us. This policy outlines our commitment to ensuring robust information security practices are implemented and maintained throughout our organization.

2. Scope of Application

2.1 Who is Covered: This policy applies to all Zyeta employees, management, directors, contractors, consultants, and any third parties conducting business on behalf of the company.

2.2 Business Area or Operations Covered: All services provided by Zyeta, including design consultation, project management, and Building Information Modeling (BIM), are subject to this policy.

2.3 Geographical Area Covered: It covers all the branches

3. Roles and Responsibilities

3.1 Management Team

- Responsible for the overall implementation and oversight of the information security policy.
- Provides resources and promotes awareness across the organization.
- Ensures compliance with legal and regulatory requirements and approves policy effectiveness during annual reviews.

3.2 Information Security Officer (ISO)

- Manages the day-to-day implementation of information security practices at Zyeta.
- Coordinates security efforts across departments and ensures proper training programs are in place.
- Reports and manages any security breaches or incidents effectively.

3.3 Employees and Contractors

- Must follow security guidelines and maintain confidentiality at all times.
- Required to report security breaches, risks, and comply with mandatory training.
- Adhere to operational and technical procedures to ensure ongoing information security.

3.4 IT Department

- Maintains and secures technical infrastructure, ensuring proper encryption and system patches.
- Implements access controls and monitors system activity for any security threats.
- Manages data integrity through regular backups and quick response to potential security issues.

3.5 Human Resources

- Conducts security-related background checks for new hires.
- Educates employees on the importance of information security and company policies.
- Ensures compliance with the information security policy throughout the employee lifecycle.

4. Application of the Policy

This policy mandates all employees and business associates to conduct due diligence on clients, vendors, and third parties, ensuring that business dealings align with AML regulations. They must promptly report any suspicious transactions or activities that may indicate money laundering or financial misconduct. Additionally, employees are required to maintain accurate and complete records of all financial transactions to support transparency and accountability. Participation in AML training programs is also mandatory to enhance awareness and compliance with AML regulations.

5. Governance of this Policy:

The governance of this Information Security Policy is overseen by Zyeta's Senior Management and the Information Security Committee. The Chief Information Security Officer (CISO) is responsible for ensuring the implementation and enforcement of this policy across the company. Senior management provides support and resources for information security initiatives, while the Information Security Committee monitors and evaluates the effectiveness of the policy.

The policy aligns with Zyeta's broader risk management and compliance frameworks and is reviewed periodically to ensure it addresses emerging security threats.

6. Information security Policy

6.1 Record Retention Plan

Zyeta has established a records retention schedule to ensure compliance with information management regulations. This schedule details the length of time each type of data must be retained and outlines procedures for the secure disposal of records once their retention period has expired. The retention policy minimizes the risk of unauthorized access to obsolete or unnecessary data.

6.2 Acceptable Use of IT Resources

6.2.1 Authorized Usage: All IT resources provided by the company, including hardware, software, networks, and systems, should be used solely for business purposes unless explicitly permitted by management.

6.2.2 Prohibited Activities: The following activities are strictly prohibited and may result in disciplinary action, including termination:

- a) Unauthorized access to data, systems, or networks.
- b) Intentional introduction of viruses, malware, or other harmful software.
- c) Distribution or storage of illegal, offensive, or inappropriate material.
- d) Unauthorized modification, deletion, or disclosure of data.
- e) Breaching copyright, intellectual property, or licensing agreements.
- f) Use of IT resources for personal financial gain or solicitation.

6.2.3 Network Usage: Employees must not congest or compromise the network's performance by engaging in excessive bandwidth-consuming activities such as streaming, online gaming, or downloading large files, unless necessary for work-related tasks. Password Security: Employees are responsible for creating and maintaining strong passwords for their accounts. Passwords should not be shared with others and should be changed regularly.

6.3 Stakeholder Consent Procedures

Zyeta obtains explicit consent from stakeholders for the collection, processing, sharing, and retention of their confidential information. We ensure stakeholders are informed about the type of data collected, the purposes for which it is used, and how long it will be retained. This transparency builds trust and ensures compliance with data protection laws.

6.4 Data Security and Privacy

6.4.1 Data Classification: Data should be classified based on its sensitivity level, such as public, internal use only, confidential, or highly sensitive. Employees must adhere to the data classification policy and handle information accordingly.

6.4.2 Data Backup: Regular backups of critical data should be performed to prevent data loss. Employees must follow backup procedures as outlined by the IT department.

6.4.3 Data Access: Access to sensitive data should be granted only on a need-to-know basis. Data access rights should be reviewed periodically, and access should be promptly revoked when no longer required.

6.4.4 Data Transmission: When transmitting sensitive information electronically, employees must use secure channels, such as encrypted emails or secure file transfer protocols, to maintain data confidentiality.

6.4.5 Personal Data Protection: Personal data collected and stored by the company must comply with applicable privacy laws. Employees must handle personal data in accordance with the company's privacy policy and ensure appropriate security measures are in place.

6.5 Information Security Training

Zyeta is committed to ensuring that all employees are trained on information security practices to protect sensitive and confidential data. We conduct regular training sessions that include presentations, practical case studies, and assessments on how to manage and secure information. This helps employees understand the importance of protecting data, identifying potential threats, and adhering to company security policies.

6.6 Software Usage:

Authorized Software: Only authorized and licensed software should be installed on company devices. Employees must refrain from using unauthorized software or illegally obtaining software licenses.

Software Updates: Employees should promptly install software updates and patches provided by the IT department to protect against security vulnerabilities.

File Sharing: File-sharing services should be used judiciously, and sensitive or confidential information should not be shared through unapproved or insecure platforms.

6.7 Third-Party Security Assessment

Zyeta ensures that third parties, such as suppliers, contractors, and vendors, meet strict information security standards through due diligence processes. We assess third-party risk by collecting data, conducting background checks, and benchmarking their security practices. This proactive approach helps mitigate the risk of information security breaches resulting from third-party relationships and ensures compliance with relevant data protection regulations.

6.8 Incident Reporting and Compliance:

Security Incidents: Any suspected or actual security incidents, such as data breaches or unauthorized access attempts, must be reported immediately to the IT department for investigation and remediation.

Compliance: All employees must comply with applicable laws, regulations, and industry standards related to information technology, data protection, and cybersecurity.

Policy Violations: Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity and repetition of the offense.

6.9 Data Security Management

Zyeta ensures the secure collection, processing, and storage of sensitive information gathered from clients, partners, and suppliers. We implement strong encryption methods, secure access controls, and other technical safeguards to protect data during transit and while stored in our systems. All information is handled with the highest level of security to prevent unauthorized access, tampering, or loss.

These measures are continuously monitored and updated to align with the latest security standards and regulatory requirements, ensuring that all sensitive data remains safe and confidential throughout its lifecycle.

6.10 Information Security Control Audits

Zyeta conducts regular internal and external audits of our information security control procedures to evaluate their effectiveness. These audits assess the current controls, ensure compliance, and identify potential vulnerabilities. Findings from audits lead to continuous improvement in our information security systems and help ensure that our company remains resilient against security breaches.

6.11 Access Control and Authentication

Zyeta enforces strict access control protocols to ensure that only authorized personnel can access sensitive data. Access rights are granted based on an individual's role within the organization, limiting exposure to only the information necessary for their job. We implement multi-factor authentication (MFA) where possible to add an additional layer of security to our systems. Regular reviews of access permissions and authentication protocols are conducted to ensure that they remain secure and compliant with industry standards, minimizing the risk of unauthorized access to critical systems and data.

6.12 Data Integrity and Backup

Maintaining data integrity is a top priority at Zyeta. We use periodic backups and data verification processes to ensure that all information remains accurate, reliable, and protected against unauthorized alterations or corruption. Our backup procedures are designed to maintain a secure, up-to-date copy of critical data, enabling recovery in the event of a system failure or data breach.

Regular integrity checks ensure that the backup data is complete, accurate, and retrievable, reducing the risk of data loss and ensuring business continuity in the face of unforeseen disruptions.

6.13 Communication Security

Zyeta prioritizes secure communication of sensitive information, both internally and externally. All communications involving confidential or sensitive data, such as email exchanges or file sharing, are encrypted using industry-standard encryption protocols. We enforce secure communication channels to prevent unauthorized interception or tampering of data.

Employees are trained to recognize secure communication practices, ensuring that any exchange of sensitive information adheres to the company's security guidelines and complies with relevant privacy regulations, safeguarding the confidentiality and integrity of data shared across all communication platforms.

6.14 Whistleblower Security Reporting Process

Zyeta has implemented a secure and confidential whistleblower procedure for reporting information security concerns. We guarantee confidentiality and non-retaliation for those who report issues related to data breaches, cyber threats, or other security vulnerabilities. A dedicated reporting channel, including email, phone hotlines, and contact persons, ensures that employees and external stakeholders can report concerns promptly and securely.

6.15 Employee Health, Safety, and Well-being

Zyeta recognizes the link between employee well-being and information security. We ensure a safe and comfortable work environment by considering employees' health and safety in office designs, workstation ergonomics, and technology setups. For remote workers, we provide ergonomic furniture and health guidelines to minimize physical and mental stress. By maintaining a healthy workplace, we enable employees to focus on their roles without the distractions or discomfort that could compromise adherence to security protocols. Employee wellness programs also help mitigate burnout, ensuring productivity and maintaining a secure operational environment.

6.16 Information Security Assessment

Zyeta regularly conducts information security risk assessments to identify and manage potential threats to our operations and data. We assess risks periodically, describe them in detail, and develop corrective action plans where necessary. The results from these assessments guide our risk management strategy and help us ensure that sensitive information is adequately protected.

6.17 Physical Security

Zyeta implements comprehensive physical security measures to protect its offices and data centers. Access is restricted to authorized personnel through the use of secure access cards and identity verification systems. Surveillance cameras are installed to monitor all entry points, and security personnel are tasked with ensuring compliance with security protocols. These physical security measures help safeguard critical infrastructure from unauthorized access, theft, or vandalism, reducing the risk of physical breaches that could compromise both physical and digital assets. Regular security audits are conducted to evaluate and improve physical security practices.

6.18 Confidentiality Breach Response Plan

Zyeta has developed a comprehensive Incident Response Plan (IRP) to address information security breaches. The plan outlines steps to detect, respond to, and limit the impact of security incidents. We ensure that all employees are trained on the IRP and are equipped to act swiftly to contain breaches and prevent further damage.

6.19 Vendor Data Safeguards

Zyeta ensures that third-party data is protected from unauthorized access or disclosure through strict access controls, encryption, and regular monitoring. We limit access to sensitive third-party data to authorized personnel only and implement both physical and digital security measures to prevent data breaches.

7. ESG Objectives

Sl. No.	Sustainability Issue	Objective	Measure	Target Value for April 2025-March 2026
1	Record Retention Plan	Implement a systematic approach for record retention.	Percentage of records managed according to retention policies	100%(→)
2	Acceptable Use of IT Resources	Ensure proper use of IT resources within the organization.	Percentage of employees adhering to acceptable use policy	100%(→)
3	Stakeholder Consent Procedures	Obtain and manage stakeholder consent for data processing.	Percentage of stakeholders providing consent for data usage	100%(→)
4	Data Security and Privacy	Implement data protection measures to ensure privacy and security of sensitive information.	Percentage of sensitive data encrypted	100%(→)
5	Information Security Control Audits	Conduct audits to verify the effectiveness of information security controls.	Number of security audits completed per year	1/year(↑)

ESG- POLICY MANUAL - IT

6	Software Usage	Ensure legal and compliant use of software within the organization.	Percentage of software usage reviewed for compliance	100%(→)
7	Third-Party Security Assessment	Conduct security assessments for third-party vendors.	Percentage of third-party vendors assessed for security risks	100%(→)
8	Incident Reporting and Compliance	Ensure prompt reporting and compliance with security incidents.	Percentage of incidents reported within 24 hours	100%(→)
9	Data Security Management	Ensure secure collection, processing, and storage of organizational data.	Percentage of data securely processed and stored	100%(→)
10	Information Security Training	Ensure all employees are trained on information security best practices.	Percentage of employees completing information security training	100%(→)
11	Access Control and Authentication	Implement strong access control measures and authentication protocols.	Percentage of systems with two-factor authentication enabled	100%(→)
12	Data Integrity and Backup	Ensure data integrity and implement effective backup systems.	Percentage of critical data backed up regularly	100%(→)
13	Communication Security	Ensure secure communication methods within and outside the organization.	Percentage of communications encrypted	100%(→)
14	Whistleblower Security Reporting Process	Provide secure and anonymous channels for whistleblowers.	Percentage of whistleblower reports securely submitted	100%(→)
15	Employee Health, Safety, and Well-being	Promote employee well-being and secure working conditions.	Percentage of employees receiving health and safety training	100%(→)
16	Information Security Assessment	Regularly assess the organization's information security posture.	Number of security assessments conducted annually	1/year (↑)

ESG- POLICY MANUAL - IT

17	Physical Security	Safeguard physical assets and infrastructure from unauthorized access.	Percentage of physical locations secured with access control	100%(→)
18	Confidentiality Breach Response Plan	Develop and implement plans to address data confidentiality breaches.	Percentage of incidents responded to within 24 hours	100%(→)
19	Vendor Data Safeguards	Ensure third-party data protection standards meet or exceed company policies.	Percentage of third-party contracts with data protection clauses	100%(→)

8. Disciplinary Actions for Policy Violations

Failure to comply with Zyeta's information security policy will lead to disciplinary actions, depending on the severity of the breach. Consequences may range from formal warnings to suspension, termination, or legal action if warranted. Employees and contractors are required to acknowledge their understanding of this policy during onboarding and annual reviews. This acknowledgment ensures that all personnel are aware of their responsibilities and the potential repercussions for failing to maintain the company's high standards of information security. Consistent adherence to the policy is crucial to safeguarding both organizational assets and sensitive information from security threats.

9. Distribution

Zyeta's information security policy will be widely distributed to all employees, contractors, and relevant third parties to ensure comprehensive understanding and compliance. The policy will be incorporated into employee handbooks, made available through the company's intranet, and communicated during onboarding and ongoing training sessions. Regular reminders and updates will be sent to reinforce the importance of information security. Additionally, employees will be required to acknowledge receipt and understanding of the policy, ensuring full accountability across all levels of the organization. This approach ensures that information security is prioritized in all aspects of Zyeta's operations.

10. Annual Review

This IT Policy will be reviewed regularly by the IT department to ensure its relevance and effectiveness. Any necessary updates or modifications will be communicated to employees accordingly. By accepting this policy, employees acknowledge their understanding and commitment to comply with its provisions. The information security policy will undergo an annual review to ensure its relevance, effectiveness, and alignment with evolving legal, technological, and regulatory requirements. Senior management, alongside the Information Security Officer, will assess the policy's implementation and impact, identify areas for improvement, and recommend necessary updates. This review process will include feedback from employees and stakeholders, as well as an evaluation of any security incidents or vulnerabilities. Any changes to the policy will be communicated to all personnel, ensuring continued adherence and enhancing Zyeta's ability to protect sensitive data and information systems.

11. Conclusion

Zyeta understands the critical need to protect information assets and is committed to providing a secure environment for both employees and clients. This policy reflects our dedication to maintaining the trust of our stakeholders by safeguarding sensitive data and information systems. Adherence to this policy is essential to mitigate risks and prevent security breaches. Through stringent security measures, continuous awareness programs, and ongoing compliance, Zyeta aims to uphold the highest standards of information security. By doing so, we ensure the integrity, confidentiality, and availability of all information, reinforcing our reputation as a responsible and secure organization.

Acknowledgement of Receipt for Policy

I hereby acknowledge that I have received a copy of the Policy. I understand that it is my responsibility to thoroughly read the contents of the Policy and adhere to the policies, rules, and regulations outlined therein.

By signing below, I confirm my commitment to comply with the principles and guidelines stated in the Policy.

Signature

:



Name

: Akshay BP | Studio Director

Date

: 5th February, 2024