

Zydus Affiliates

October 2025

Information Security Policy

INDEX

Introduction.....	4
Scope	4
Policy Statement.....	4

Introduction

The purpose of this Information Security Policy is to safeguard the interests of internal and external stakeholders by securing Zydus's information and associated assets

Scope

This policy applies to all information and associated assets owned, managed, or entrusted to Zydus Affiliates*.

Policy Statement

Zydus is committed to protecting the confidentiality, integrity, and availability of all organizational information assets.

Zydus intend to meet the Information security objectives mentioned below:

Risk Management: Identifying, assessing, and managing risks to information security, and implementing appropriate measures to mitigate identified risks.

Regulatory Compliance: Adhering to applicable laws, regulations, and contractual obligations to ensure the organization meets applicable legal and regulatory requirements related to information security.

Incident Management: Establishing a systematic approach to identify, analyse, respond to, and manage security incidents to minimize their impact and prevent recurrence.

Governance: Defining roles and responsibilities, setting policies, and establishing processes to ensure that security measures are aligned with business goals and objectives.

Continuous Improvement: Regularly reviewing and improving the ISMS to adapt to changing security threats and business needs, promoting ongoing enhancement of security measures.

Stakeholder Engagement and Awareness: Involving relevant stakeholders in the development and maintenance of the ISMS. Providing continuous training and awareness programs to keep stakeholders informed about security policies and best practices.

We take full responsibility for the implementation and maintenance of our Information Security Management System (ISMS), ensuring the protection of our information assets and the continuous improvement of our security practices.

*Zydus Affiliates refers for Zydus group of entities as per Information Security Management System framework.

Zydus Affiliates

October 2025

Information Security Management Policy

INDEX

1. Introduction	5
2. Scope	5
3. Policy Statement	6
4. Information Security management guidelines:.....	7
4.1. Management Support towards Information Security.....	7
4.2. Information Security Roles and Responsibilities	7
4.3. Contact with Authorities and Special interest Group:	8
4.4. Segregation of Duties	8
5. Definitions.....	9
6. References	9

1. Introduction

1.1. Objective

The purpose of this Information Security Management Policy is to define and clarify the responsibilities of management in establishing, implementing, and maintaining effective information security practices. It ensures that management provides the necessary leadership, resources, and oversight to protect the organization's information assets. It supports the organization's ability to manage Information security Management effectively.

This policy reinforces the confidentiality, integrity, and availability of organizational information and associated assets by establishing appropriate management practices at Zydus. It aligns with ISO/IEC 27001:2022 5.2, 5.3, 5.4, 5.5, and 5.6 and associated ISO/IEC 27002:2022 guidance.

1.2. Applicability

This policy applies to relevant management and stakeholders at Zydus.

1.3. Responsibilities

IT Management Team: Responsible for ensuring that IT systems and infrastructure are designed, implemented, and maintained in accordance with the Information Security Management Policy. They oversee the integration of security requirements into IT operations, including access control, system hardening, and change management. The team collaborates with the Cybersecurity Head to support risk mitigation and respond effectively to security incidents.

2. Scope

This policy applies to all assets owned, managed, or entrusted to Zydus Affiliates.

3. Policy Statement

- 3.1. Management at Zydus shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies, and procedures of the organization.
- 3.2. At Zydus, information security roles and responsibilities shall be defined and allocated according to the organization's needs.
- 3.3. At Zydus, conflicting duties and conflicting areas of responsibility shall be segregated to reduce the risk of fraud, error, and bypassing of information security controls.
- 3.4. Management shall establish and maintain contact with special interest groups, specialist security forums, professional associations, and relevant authorities.

4. Information Security management guidelines:

Information Security Management Guidelines will help management establish effective policies and procedures to protect organizational information. They will guide management in assessing risks, allocating resources, and enforcing security controls. By following these guidelines, management will ensure the organization's information remains secure and compliant.

4.1. Management Support towards Information Security

4.1.1. Management will support IT Security Team to ensure:

- All personnel briefed on their information security roles and responsibilities prior to being granted access to Zydus information systems, data, and associated assets.
- Role-specific information security expectations will be documented and communicated through defined guidelines aligned with the individual's duties within the organization.
- All employees and relevant third parties will be mandated to comply with the overarching information security policy and relevant topic-specific policies as a condition of access and ongoing engagement.
- Ensure that individuals achieve and maintain an adequate level of information security awareness appropriate to their roles and responsibilities.
- Compliance with all applicable terms and conditions of employment, contracts, and agreements including adherence to Zydus information security policies and secure work practices will be enforced.
- A confidential whistleblower mechanism will be made available, allowing personnel to report violations of security policies or procedures. This may include anonymous reporting or restricted-access reporting to protect the identity of the reporting individual.

4.1.2. Adequate resources, time, and support will be allocated by management for the planning and implementation of information security controls and related security initiatives across the organization.

4.1.3. Zydus Management will designate a dedicated Head of Cybersecurity responsible for coordinating enterprise-wide security initiatives, supporting risk identification efforts, and overseeing implementation of appropriate controls.

4.2. Information Security Roles and Responsibilities

4.2.1. At Zydus, allocation of information security roles and responsibilities will be carried out in alignment with the overarching Information Security Policy and relevant topic-specific policies.

4.2.2. Zydus will define and manage responsibilities for the following domains:

- To execute information security processes / information security result areas as per applicable ISO 27001:2022 Annexure A controls, such as asset management and secure configuration, change management, security incident management, vulnerability management, and system monitoring.
- For conducting risk assessments, managing mitigation plans, and formally accepting residual risks.

4.2.3. While individuals assigned to information security responsibilities may delegate specific tasks, they will retain overall accountability and must ensure delegated responsibilities are executed accurately and completely as per defined RACI (Responsible, Accountable,

Consulted, and Informed) to achieve Key result areas for defined information security processes.

- 4.2.4. Each area of security responsibility will be clearly defined, documented, and communicated, including any associated authorization levels required to perform assigned duties.

4.3. Contact with Authorities and Special interest Group:

- 4.3.1. At Zydus, management will specify when and by whom authorities such as law enforcement and regulatory bodies shall be contacted.
- 4.3.2. Management will ensure that identified critical information security incidents are reported promptly and through the proper channels.
- 4.3.3. Management and Information security team will also maintain contact with these authorities to stay informed about current and upcoming information security regulations and expectations.
- 4.3.4. At Zydus, Management will consider membership in special interest groups or forums to improve knowledge of best practices and stay updated with relevant security information. This membership will ensure that the organization's understanding of the information security environment remains current and help receive early warnings about alerts, advisories, and patches related to attacks and vulnerabilities. Additionally, it will provide access to specialist advice, facilitate the sharing of information on new technologies and threats, and offer appropriate liaison points for managing information security incidents.

4.4. Segregation of Duties

- 4.4.1. At Zydus, management will ensure segregation of duties and areas of responsibility by separating conflicting tasks among different individuals or teams.
- 4.4.2. Management will identify which duties require segregation to prevent any one individual or team from having control over conflicting activities. This approach will help reduce risks and maintain strong internal controls.
- 4.4.3. At Zydus, management will develop a RACI matrix (Responsible, Accountable, Consulted, and Informed) for the defined Key Result Areas related to information security to clearly define roles and responsibilities.

5. Definitions

- 5.1. Information Security: The practice of protecting information from unauthorized access, disclosure, alteration, and destruction to ensure its confidentiality, integrity, and availability.
- 5.2. Information Assets: Any data, system, application, or infrastructure owned, managed, or entrusted to Zydus that is critical to business operations and must be protected.
- 5.3. Information Security Management System (ISMS): A structured framework of policies, procedures, and controls designed to manage and protect organizational information assets in alignment with ISO/IEC 27001:2022 standards.
- 5.4. Roles and Responsibilities: Clearly defined duties assigned to individuals or teams to ensure effective implementation and maintenance of information security controls. These are documented and aligned with business needs and risk management practices.
- 5.5. RACI Matrix: A responsibility assignment model used to define roles in terms of who is Responsible, Accountable, Consulted, and Informed for specific tasks or decisions related to information security.
- 5.6. Segregation of Duties: A control mechanism that separates conflicting responsibilities among individuals or teams to reduce the risk of fraud, error, or misuse of information systems.
- 5.7. Cybersecurity Head: A designated individual responsible for coordinating enterprise-wide security initiatives, overseeing risk identification, and ensuring implementation of appropriate controls.
- 5.8. Special Interest Groups: External forums, associations, or communities that provide insights, updates, and best practices related to information security, helping Zydus stay informed and proactive.
- 5.9. Security Incident: Any event that compromises the confidentiality, integrity, or availability of information assets, including unauthorized access, data breaches, or system failures.
- 5.10. Whistleblower Mechanism: A confidential reporting system that allows employees to report violations of security policies or procedures without fear of retaliation.

6. References

- Information Security Management System (ISO/IEC 27001:2022) standard
- Information Security, Cybersecurity and Privacy protection- Information security controls (ISO/IEC 27002:2022)