

Our Policies

Information Security Policy

August 2024 - vs. 1



Information Security Policy

Introduction

Information security is important for Zentiva as it safeguards the sensitive data and systems that underpin our operations. Protecting customer information, intellectual property, and business processes from threats and unauthorized access is essential for maintaining trust and ensuring compliance with industry regulation. Our Information Security policy reflects our commitment to implementing effective security measures and to continuously improving the defense of our Information Systems and Assets (ISA). By prioritizing information security, we aim to minimize risks, prevent data breaches, and ensure the confidentiality, integrity and availability of our services. Regular risk assessments are conducted to evaluate potential threats and vulnerabilities, enabling us to implement appropriate controls and continuously improve our security posture.

Policy Purpose

The purpose of this policy is to outline Zentiva's Information Security efforts and clarify the key tenets of Zentiva's approach to protecting its information assets.

Scope

This policy is company-wide in scope and applies to all employees, board members and people working for Zentiva as well as to all subsidiaries, and affiliated companies of the Zentiva Group. It encompasses all aspects of our company and its subsidiaries and extends to our suppliers and partners where applicable.

Alignment with Zentiva Purpose and Values

Purpose: Zentiva's purpose is to provide health and wellbeing for all generations. This purpose is embedded in our long-term business strategy and also reflected in our commitment to Information security.

Values: Our core values - Accountability, Authenticity, Courage, Collaboration, and Trust - drive our efforts. These values guide our actions and decisions, ensuring that we remain committed to our responsibilities and the communities we serve.

Alignment with Zentiva Sustainability Strategy

Zentiva's Sustainability strategy is built on three pillars: People, Partners, and Planet, and adheres to the principles of ESG (Environmental, Social, Governance). Our Information Security policy is an integral part of this strategy..

Our Sustainability commitments are summarized in our corporate policies and published on the Zentiva website. Our global policies may be supplemented by local policies as needed.

Zentiva's Sustainability Priorities

People: We are building Zentiva as a great place to work where authenticity is embraced. We take care of our employees, their families and those we serve. Through transparent communication and a united approach, we create value as ONE team, We take our role as a Corporate Citizen with great responsibility.

Partners: We endeavor to establish and maintain trustworthy partnerships across our value chain, working with partners who share our values. We actively encourage our partners to engage in dialogue, sharing experiences, exchanging expectations, and collaborating hand in hand towards a more sustainable business.

Planet: We are dedicated to fostering a greener planet, aiming to achieve carbon neutrality for Scope 1 and 2 by 2030. This commitment entails implementing a comprehensive climate strategy aimed at reducing carbon emissions, sourcing renewable energy, optimizing water and energy consumption, and investing in circular economy practices to minimize waste. Additionally, we contribute to the planet's health through tree planting initiative and biodiversity restoration efforts.

Complementarity with Other Key Zentiva Policies

Our policies are designed to meet high standards and are continuously updated to stay aligned with the latest industry practices and regulatory requirements.

Zentiva's Information Security policy is highly interwoven with Zentiva's privacy policy, which complies with all local legislation, including the General Data Protection Regulation (GDPR) in the European Union and other applicable data protection laws. This integrated approach ensures that both the confidentiality and privacy of personal and sensitive information are protected, reinforcing our commitment to safeguarding data and maintaining the trust of our customers, employees, and stakeholders.

Related Zentiva Policies and Documents

- Business Ethics Commitment / Code of Ethics
- General Terms of Delivery
- Privacy Notice
- Corporate Policy on Personal Data Processing
- Suppliers Code of Conduct
- Whistleblower- / Speak-Up-Policy

Governance of Information Security within Zentiva

Role	Responsibility
Cybersecurity Manager	The Cybersecurity manager is responsible for all entities within the Zentiva Group. This role oversees and shapes all aspects of information security, its definition, implementation and monitoring.
Cybersecurity Committee	The Cybersecurity Committee assists the Zentiva Executive Committee in fulfilling its oversight responsibilities with respect to Zentiva's information technology use and protection of the Zentiva's information technology, including but not limited to data governance, privacy, compliance, and cybersecurity.
Audit Committee/Ethical Compliance Committee	The Audit Committee reviews and approves financial statements, internal control & audit and ensures compliance with all relevant regulations including Information and Cybersecurity.

Policy Implementation

The use of Information Systems (ISA) by Zentiva's employees, suppliers, and other stakeholders must comply with this policy, all related internal guidelines, and applicable local regulations. All users of ISA are required to complete necessary training and demonstrate their understanding of the guidelines and this policy.

Risk Assessment

Risk assessment is a critical component of Zentiva's Information Security policy, designed to identify, evaluate, and mitigate risks to our company's information assets. This process involves the following steps:

1. **Identification and Evaluation:** Identify all ISA, including hardware, software, data, as well as users and experts. Recognize potential threats such as cyber-attacks, natural disasters, human error, and insider threats. Evaluate the vulnerabilities of each asset using tools and techniques such as vulnerability scanning, penetration testing, and security audits.
2. **Impact and Risk Analysis:** Assess the potential impact of each identified threat on the organization, considering factors such as financial loss, reputational damage, operational disruption, and legal consequences. Prioritize risks based on their likelihood and potential impact, often using a risk matrix to classify risks into categories like low, medium, and high.
3. **Mitigation and Control Implementation:** Develop and implement strategies to mitigate identified risks. These strategies may include technical controls (e.g., firewalls, encryption), administrative controls (e.g., policies, procedures), and physical controls (e.g., access restrictions). Ensure these measures are effective and properly maintained.
4. **Monitoring and Review:** Continuously monitor the effectiveness of implemented controls and reassess risks on a regular basis. Document the findings and updates in a comprehensive report, and conduct periodic reviews to ensure the risk assessment process remains relevant and effective. Regularly update documentation to reflect changes in the threat landscape and organizational environment.

By systematically identifying and addressing risks, Zentiva aims to protect its ISA, ensure compliance with regulatory requirements, and support the continuity of business operations.

Access and Disclosure Controls

Access to sensitive information is restricted to authorized personnel only, based on their roles and responsibilities. All access rights are regularly reviewed and updated to ensure compliance with the principle of least privilege. Disclosure of information is strictly controlled and monitored to prevent unauthorized access and data breaches.

Incident Response Procedure

Zentiva has implemented a procedure to quickly respond to any breaches. The procedure includes internal management and external stakeholder communication, assessment and containment of incidents, and transparent notification of affected parties as well as all compulsory notification of authorities. A post-incident analysis is conducted to improve future responses and enhance overall security.

Goals

We aim to have at least 99% of our employees undergo a minimum of three Information Security training sessions per year.

Employee Training

All employees are required to complete periodic awareness training on Information Security. Key personnel, particularly IT-experts who are directly responsible for implementing the policy, undergo regular, specialized training to enhance their capacity for managing Information Security at Zentiva. These employees are promptly informed of any updates to the policy to ensure they remain knowledgeable and effective in safeguarding our information assets.

Suppliers and Information Security


As per the General Terms of Delivery, Zentiva suppliers agree to participate in the Cybersecurity training provided by Zentiva Group and to comply with all Zentiva security.

Whistleblower- / Speak-Up-Policy

Zentiva has a whistleblowing procedure accessible both internally and externally to assist in reporting security breaches and any non-compliance. The whistleblower procedure has a dedicated, confidential line of communication and guaranteed non-retaliation.

Information Security Policy Communication

All employees as well as all stakeholders have access to the policy that is made publicly available on www.zentiva.com.



Josef Matousek
Head of Global IT