

INFORMATION SECURITY POLICY PRESENTATION



INTRODUCTION

A comprehensive information security policy is essential for any organization to protect its information assets and ensure data integrity, confidentiality, and availability. Jetzy has developed a robust information security policy to safeguard its digital environment against evolving threats.

Jetzy's approach includes implementing advanced technologies, fostering a culture of security awareness among employees, and complying with industry standards and regulations to protect user data and business operations.



ORGANIZATION OVERVIEW

Jetzy is a leading social media application designed for travelers. It connects users, enabling them to share experiences, find and book hotels, make restaurant reservations, and enjoy various travel related services. With a focus on creating a seamless travel experience, Jetzy provides users with the tools they need to plan and share their journeys.

Key Services:



Post uploading and sharing



User groups and messaging



Hotel booking



Restaurant reservations



Paid membership features

INFORMATION SECURITY VISION AND PURPOSE

Vision:

Jetzy aims to be the global leader in social networking platforms by fostering an ethical, safe, and trustworthy digital environment. The vision focuses on leveraging advanced and robust technologies to protect the privacy and integrity of user data against ever evolving information security threats.

INFORMATION SECURITY VISION AND PURPOSE

Statement of Purpose:

The purpose of this Information Security Policy is to establish a framework to safeguard Jetzy's information assets. This policy outlines strategic and procedural measures necessary to protect the platform's infrastructure, user data, and business operations from potential security threats and vulnerabilities.

SCOPE AND OBJECTIVES

This policy applies to all employees, contractors, third party vendors, and any other individuals or organizations interacting with Jetzy's information systems and data. It ensures comprehensive protection over all physical and virtual aspects of Jetzy's operations, including devices, networks, applications, and external services.



OBJECTIVES

By implementing this policy, Jetzy aims to:

Ensure compliance with relevant laws, regulations, and industry standards.

Foster a culture of cybersecurity awareness among employees, partners, and users.

Implement a security first approach to development and incorporate DevSecOps practices.

Strengthen existing security measures to guarantee that only authenticated and authorized individuals access Jetzy's data.


Develop incident response, disaster recovery, and business continuity plans to ensure uninterrupted operations.

ROLES & RESPONSIBILITIES

CEO: Ensures that the organization's information security strategy aligns with its business objectives and regulatory requirements. Approves the information security policy and allocates necessary resources.




CISO: Develops, implements, and manages the organization's information security policies and practices. Oversees risk management, incident response, and compliance.



CIO: Collaborates with the CISO to integrate information security into the organization's IT strategy and ensures the IT team is trained and aware of their responsibilities.

ROLES & RESPONSIBILITIES

DPO: Manages compliance with data protection regulations such as GDPR and CCPA.



IT Security Team: Implements security measures, monitors security systems, and responds to incidents.



Compliance Officer: Ensures compliance with all relevant laws, regulations, and industry standards.



Developers and Engineers: Follow secure coding practices and integrate security into the development lifecycle.



All Employees: Adhere to security policies and procedures, report security incidents, and participate in security training programs.

PHYSICAL SECURITY POLICY

Jetzy implements strict physical security measures to protect its infrastructure and data. Key policies include:



ACCESS CONTROLS: ONLY JETZY ISSUED DEVICES ARE ALLOWED TO CONNECT TO THE SYSTEMS. BIOMETRIC AUTHENTICATION, KEY CARD ACCESS, AND CCTV SURVEILLANCE ARE IN PLACE.



DEMILITARIZED ZONES (DMZ): EQUIPMENT IN DMZ AREAS MUST ADHERE TO STRICT SECURITY STANDARDS, UNDERGO REGULAR AUDITS, AND USE SECURE ADMINISTRATION PROTOCOLS.



INFORMATION & EQUIPMENT DISPOSAL: ALL TECHNOLOGY EQUIPMENT MUST BE SECURELY ERASED AND DISPOSED OF FOLLOWING INDUSTRY BEST PRACTICES TO PREVENT DATA BREACHES.

NETWORK SECURITY

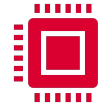
Jetzy's network security policies ensure the protection of data in transit and at rest. Key policies include:



Network Segmentation:
Segregating external, internal, sensitive, and highly sensitive networks based on roles and access levels.



Remote Access:
Only Jetzyissued or verified devices are permitted for remote access to the network, ensuring secure VPN connections.



Server Security:
Servers must comply with configuration guides, undergo regular compliance monitoring, and have the latest security patches installed.

COMMUNICATIONS SECURITY

Jetzy's communication security policies safeguard the confidentiality and integrity of data transmitted over networks. Key policies include:



Email Security: All email communications must use encryption. Automatic forwarding to thirdparty systems is prohibited to prevent data leaks.



Internet Usage: Internet access is granted based on business needs and is monitored for compliance with the organization's policies.



Wireless Communication: Devices must meet specified security standards, use approved protocols, and ensure secure authentication.



Remote Access: Secure connections using encryption protocols such as VPNs are mandatory for remote access to the corporate network.

INFORMATION SECURITY POLICY

Jetzy classifies its data into different sensitivity levels to apply appropriate security measures. Key elements include:

Data Classification: Data is categorized into low, medium, and high sensitivity levels, each with specific security measures.

Data Protection: All data must be encrypted both at rest and in transit to protect against unauthorized access.

Credentials: Credentials must be stored securely, separate from application code, and accessed securely.

Passwords: Passwords must meet minimum requirements, including length and complexity, and use multifactor authentication.

APPLICATION SECURITY



Secure Coding Practices: Developers must follow secure coding practices for Flutter and Elixir, the technologies used in Jetzy's applications.



Regular Security Training: Ongoing training for developers on secure coding and security best practices.



Security Assessments: Regular use of static and dynamic application security testing tools to identify vulnerabilities during development and deployment.



Dependency Scanning: Tools to identify and remediate vulnerabilities in thirdparty libraries and components.



Threat Modeling: Prioritizing potential security risks through threat modeling exercises.

OPERATIONAL SECURITY

Access Controls:

Permissions are managed meticulously, ensuring adherence to the principles of least privilege and separation of duties.

Incident Response Planning:

A dedicated incident response team develops comprehensive plans to manage and recover from security incidents.

Risk Management: Tailored security measures are developed based on data classification and regular risk assessments.

PERSONNEL SECURITY



IMPLEMENTATION PLAN AND COMPLIANCE

Planning: Risk assessments are conducted to identify potential threats. A stepbystep implementation plan is developed to address these risks.

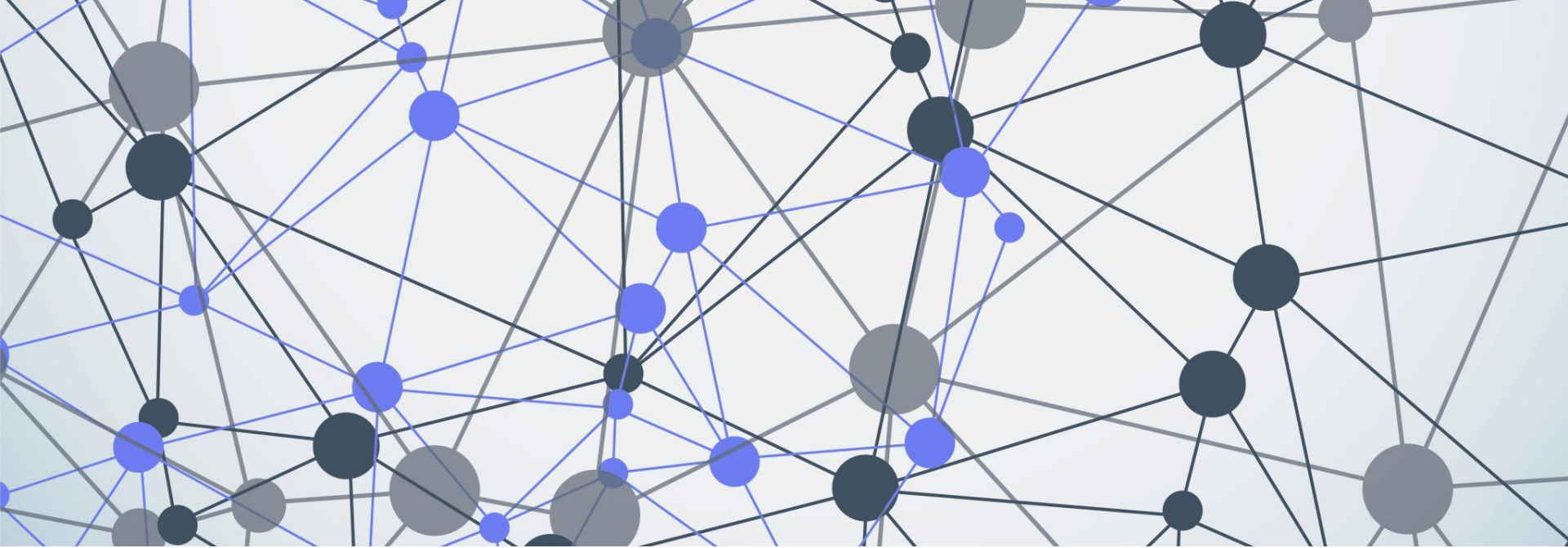
Execution: The security measures and policies are implemented across the organization.

Review: Regular reviews and updates to the security policies to ensure effectiveness and compliance with evolving standards.

IMPLEMENTATION PLAN AND COMPLIANCE

Jetzy adheres to industry standards and regulations to ensure the security of its information systems. Regular audits and assessments are conducted to maintain compliance.





CONCLUSION

Jetzy is committed to providing a secure, reliable, and innovative platform for travelers. By implementing robust information security policies and continuously improving security measures, Jetzy aims to protect its digital environment and maintain the trust and confidence of its users and stakeholders.