Information Security Policy

1. Purpose

This Information Security Policy establishes guidelines and requirements for the protection of information assets within Mozart ltd. As a B2B software provider handling Personally Identifiable Information (PII) under GDPR requirements, Mozart ltd recognizes that information security is essential to maintaining customer trust, legal compliance, and business continuity.
The policy aims to ensure that all employees, contractors, and relevant third parties understand their responsibilities in safeguarding Mozart ltd's information assets, including client data, intellectual property, and business information, against unauthorized access, disclosure, alteration, or destruction.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at Mozart ltd, including all personnel affiliated with third parties who access Mozart ltd systems and data. It encompasses all information assets, IT systems, networks, data storage systems, applications, and devices used to conduct business operations, whether on-premises or in cloud environments.

3. Policy

Mozart ltd is committed to implementing and maintaining appropriate technical, organizational, and physical safeguards to protect the confidentiality, integrity, and availability of information assets in compliance with GDPR and industry best practices. All employees and relevant third parties must adhere to this policy and related procedures to ensure information security across all business activities.

4. Security Responsibilities

The management team at Mozart ltd holds primary responsibility for information security governance, including the allocation of resources, approval of policies, and oversight of implementation. A designated Information Security Officer (ISO) is responsible for the day-to-day management of the information security program, including policy development, risk assessments, security awareness training, and incident response coordination.
All employees are responsible for complying with this policy, reporting security incidents promptly, participating in security awareness training, and protecting information assets they access or control. Department managers are responsible for implementing security controls within their areas of responsibility and ensuring their team members understand and comply with security requirements. Third-party providers must comply with security controls as defined in their contracts and service level agreements.

5. Device & Endpoint Security

All devices used to access Mozart ltd systems and data, including company-issued and personal devices under the hybrid work model, must be properly secured against unauthorized access and malware. Devices must have current operating systems with the latest security patches applied, endpoint protection software installed and regularly updated, secure configuration settings, and disk encryption enabled.
Employees must use strong authentication mechanisms, including multi-factor authentication where available, and ensure their devices are physically secured when not in use. Regular security scans and vulnerability assessments will be conducted on endpoints to identify and remediate security issues. Users are prohibited from disabling security features or installing unauthorized software on company-owned devices.

6. Application & Infrastructure Security

Mozart ltd's applications and infrastructure must be designed, developed, and maintained with security as a foundational requirement. All software development must follow secure coding practices, with security testing integrated throughout the development lifecycle, including regular code reviews, vulnerability scanning, and penetration testing appropriate for a small to medium-sized organization.
Infrastructure components, including servers, networks, and cloud environments, must be hardened according to industry standards, with unnecessary services disabled, access controls enforced, and monitoring in place to detect unauthorized activity. Regular backups of critical data and systems must be performed, tested, and stored securely. All production changes must follow an established change management process to minimize security risks and service disruptions.

7. Incident Response & Reporting

Mozart ltd maintains a structured approach to managing information security incidents to minimize damage, reduce recovery time, and ensure compliance with GDPR reporting requirements. All employees must immediately report suspected security incidents, data breaches, or vulnerabilities to the Information Security Officer or IT department through designated channels.
Upon notification of a security incident, the response team will assess the situation, contain the incident, eradicate the cause, recover affected systems, and document lessons learned. For incidents involving personal data, Mozart ltd will determine if notification to supervisory authorities and affected individuals is required under GDPR, ensuring notifications are made within the mandated 72-hour timeframe when applicable.

8. Whistleblower Policy

Mozart ltd encourages employees to report suspected violations of information security policies, procedures, or regulations without fear of retaliation. Employees may report concerns anonymously to the Information Security Officer, Human Resources, or management. All reports will be investigated promptly while maintaining the confidentiality of the reporting individual to

the extent permitted by law.

9. Fraud Reporting

Employees must report suspected fraudulent activities, including but not limited to unauthorized data access, identity theft, financial fraud, or misuse of company resources, to the Information Security Officer and management. Mozart ltd is committed to investigating all reports thoroughly, taking appropriate action against confirmed fraud cases, and implementing controls to prevent future occurrences while ensuring compliance with GDPR and other relevant regulations.

10. Mobile Device Policy

Mobile devices used to access Mozart ltd systems and data must be protected with strong passwords or biometric authentication, encryption, and the ability to remotely wipe data in case of loss or theft. Employees must promptly report lost or stolen devices, avoid connecting to unsecured public Wi-Fi networks when accessing company information, and keep mobile operating systems and applications updated with the latest security patches.

11. Third-Party & Vendor Security

Mozart ltd will assess the security posture of third-party vendors before engaging their services, especially when they will process, store, or transmit Mozart ltd data or PII. Assessments will be proportional to the sensitivity of data involved and the criticality of the service, with more rigorous evaluations for vendors handling sensitive information or providing critical services. Contracts with vendors must include security requirements, data protection obligations, right-to-audit clauses, breach notification requirements, and compliance with applicable regulations including GDPR. Mozart ltd will periodically review vendor security practices, particularly after significant changes to services or following security incidents. Access granted to vendors will follow the principle of least privilege, providing only the minimum necessary to perform their contracted services.

12. Clear Screen / Clear Desk Policy

Employees must secure physical and digital information when workstations are unattended, including locking computer screens when stepping away, storing sensitive documents securely when not in use, disposing of sensitive materials using secure methods such as shredding, and ensuring that whiteboards and other visual displays are cleared of sensitive information after meetings. This policy applies to both office and home work environments in the hybrid work model.

13. Remote Access Policy

Remote access to Mozart ltd systems and data must be conducted securely using company-approved VPN technology with multi-factor authentication. Employees working remotely must ensure their home networks are secured with strong encryption (WPA2/WPA3), unique passwords, and regularly updated firmware on routers and networking equipment. Public

Wi-Fi networks should be avoided when accessing sensitive company information; if unavoidable, a VPN connection must be established.
Employees must ensure that unauthorized individuals, including family members, cannot view or access company information on their screens or devices. Remote access privileges will be regularly reviewed and promptly revoked when no longer needed. All remote working arrangements must comply with GDPR requirements for data protection, including proper data transfer mechanisms and security controls equivalent to those in the office environment.

14. Acceptable Use Policy

Mozart ltd provides IT resources, including computers, networks, email, internet access, and software, for legitimate business purposes. Employees are expected to use these resources responsibly, ethically, and in compliance with this policy and applicable laws. Limited personal use is permitted provided it does not interfere with job performance, consume significant resources, or violate any Mozart ltd policies.
All communications through company systems should maintain professional standards and protect confidential information. Employees should have no expectation of privacy when using company IT resources, as Mozart ltd reserves the right to monitor usage for security, compliance, and operational purposes, subject to applicable laws and regulations including GDPR.

15. Unacceptable Use

The following activities are strictly prohibited when using Mozart ltd IT resources:

- Accessing, creating, or distributing offensive, illegal, or inappropriate content, including material that violates anti-harassment policies
- Unauthorized access to systems or data, attempts to circumvent security controls, or use of another user's credentials
- Installation of unauthorized software, including peer-to-peer file sharing applications, games, or unlicensed programs
- Transmission of confidential information or PII without appropriate security measures or authorization
- Use of company resources for personal gain, unauthorized commercial activities, or political campaigns
- Sending mass emails without proper authorization or engaging in spamming activities
- Knowingly introducing malware, disabling security software, or interfering with IT operations
- Excessive use of bandwidth for non-business purposes such as video streaming or large personal downloads
- Sharing internal information on social media or external forums without authorization
- Violating intellectual property rights through unauthorized copying or distribution of protected materials

16. Email and Communication Activities

The following guidelines apply to email and other electronic communications:

- Always include a clear, appropriate subject line in email communications

- Exercise caution with email attachments and links, verifying sender identity before opening
- Do not automatically forward Mozart ltd emails to personal email accounts
- Use encrypted communication channels when sharing sensitive information or PII
- Include appropriate confidentiality notices in external communications containing sensitive information
- Avoid using email for urgent communications that require immediate attention
- Report suspicious emails to IT security without opening attachments or clicking links
- Exercise professional judgment in tone and content of all business communications
- Never send passwords, access credentials, or highly sensitive information via unencrypted email

17. Compliance & Audits

Mozart ltd will conduct regular security assessments and audits to evaluate compliance with this policy, GDPR requirements, and industry best practices. These assessments may include vulnerability scans, penetration testing, policy compliance reviews, and data protection impact assessments. The scope and frequency of audits will be proportionate to Mozart ltd's size, the sensitivity of data processed, and applicable regulatory requirements.

18. Policy Review & Updates

This Information Security Policy will be reviewed at least annually and updated as needed to address changes in the business environment, technology landscape, threat environment, or regulatory requirements. All employees will be notified of policy updates, and training will be provided as necessary. The Information Security Officer is responsible for initiating and overseeing the review process, with final approval from management.

19. Violations & Enforcement

Violations of this Information Security Policy may result in disciplinary action, up to and including termination of employment or contract termination for third parties. The severity of disciplinary action will depend on the nature and impact of the violation, whether it was intentional or accidental, and whether it is a repeat offense. In cases involving illegal activities, Mozart ltd may involve law enforcement agencies and pursue legal remedies.

20. Policy Compliance

All employees must acknowledge receipt and understanding of this Information Security Policy upon joining Mozart ltd and after significant policy updates. Regular security awareness training will be provided to ensure ongoing compliance. Managers are responsible for monitoring compliance within their teams and reporting issues to the Information Security Officer. Mozart ltd may use technical controls to enforce certain aspects of this policy automatically where appropriate and permitted by applicable laws and regulations.