Access Control Policy for Mozart ltd

1. Purpose

This Access Control Policy establishes the requirements and guidelines for managing access to Mozart ltd's information systems, networks, and data. It aims to protect the confidentiality, integrity, and availability of company resources while ensuring compliance with GDPR and other applicable regulations. The policy outlines the principles and procedures for granting, reviewing, and revoking access rights to information and systems.
The policy is designed to minimize security risks associated with unauthorized access, data breaches, and non-compliance, particularly considering Mozart ltd's handling of Personally Identifiable Information (PII) and remote work environment. It provides a framework that balances security requirements with operational efficiency, supporting Mozart ltd's growth trajectory of 21-50% annual headcount increase while maintaining appropriate security controls.

2. Scope

This policy applies to all Mozart ltd employees, contractors, consultants, temporary workers, and other business partners who require access to Mozart ltd's information systems, applications, networks, and data resources. It covers all company-owned and managed systems, SaaS applications, cloud services, network infrastructure, and data repositories containing company information regardless of location or access method, with special attention to systems containing or processing Personally Identifiable Information (PII) subject to GDPR requirements.

3. Policy

Mozart ltd shall implement appropriate access controls to protect information assets based on business requirements and the principle of least privilege, ensuring that users are granted only the minimum necessary access rights to perform their job functions. All access to information systems shall be authorized, authenticated, and audited in accordance with this policy. The management team is responsible for ensuring policy compliance, with the IT/Security team handling implementation and enforcement of technical controls. All users are required to adhere to this policy as a condition of access to Mozart ltd systems and information.

4. Access Control Policy

Mozart ltd adopts a Role-Based Access Control (RBAC) model combined with the principle of Least Privilege as the primary approach to managing access permissions. Under this model, access rights are assigned based on predefined roles that correspond to job functions within the organization. This approach is appropriate for Mozart ltd's size (11-50 employees) and expected growth (21-50% annually), as it provides a scalable framework that can accommodate organizational changes while maintaining security. Each role is configured with the minimum permissions necessary to perform associated job functions, aligning with the principle of least privilege.

As Mozart ltd grows and operates in a remote work environment with primarily SaaS applications, the RBAC model will be supplemented with elements of Zero Trust architecture, requiring verification for anyone attempting to access resources regardless of their location or network connection. This hybrid approach provides the necessary security controls for protecting PII data subject to GDPR requirements while maintaining the flexibility needed for remote operations. The model will be regularly reviewed and adjusted to address evolving business needs and security requirements.

5. Access to Networks and Network Services

Access to Mozart ltd's networks and network services shall be restricted to authorized users and devices through secure authentication methods. For remote workers, secure VPN connections with multi-factor authentication shall be required when accessing internal resources. Network segmentation shall be implemented to isolate systems containing PII data from general purpose networks. All network access shall be logged and monitored for suspicious activities, with logs retained in accordance with GDPR requirements. Users shall only be provided access to the specific network services they have been explicitly authorized to use, and all unnecessary services shall be disabled by default.

6. User Access Management

User access management at Mozart ltd encompasses the processes and procedures for requesting, approving, creating, modifying, reviewing, and revoking user access to information systems and applications. The HR department, in coordination with IT/Security, shall maintain accurate records of all users and their access privileges. Access management processes shall be documented, followed consistently, and periodically audited for compliance. All changes to access rights shall be approved by appropriate managers or system owners, with higher scrutiny applied to privileged access or access to systems containing PII data.

6.1 User Registration and Deregistration

A formal user registration and deregistration process shall be implemented to enable the assignment and revocation of access rights. For new employees, HR shall initiate the registration process as part of onboarding, providing necessary information including role, department, and access requirements. For contractors and temporary workers, the sponsoring manager shall submit registration requests. All requests shall be documented and approved by appropriate authorities before access is granted. Upon termination of employment or contract, HR or the responsible manager shall promptly notify IT/Security to initiate the deregistration process, ensuring all access rights are revoked within 24 hours. The process shall be integrated with HR systems to facilitate timely notification of personnel changes affecting access requirements.

6.2 User Access Provisioning

Access provisioning shall follow a defined workflow to ensure appropriate controls are maintained. The process includes:

- All access requests must be formally documented through the approved request system

- Requests must specify the user's identity, role, required systems, and access level
- Approval must be obtained from the relevant system owner or department manager
- Access shall be provisioned according to predefined role templates where possible
- Special access rights beyond standard role definitions require additional justification and approval
- Temporary access shall have a defined expiration date
- For SaaS applications, single sign-on (SSO) shall be implemented where supported
- Provisioning shall be documented with date, approver, and specific access granted
- All privileged access provisioning shall be logged and subject to additional review

6.3 Management of Privileged Access

Privileged access rights (administrator, super-user, root access) shall be allocated and controlled on a need-to-use basis. Such access shall be strictly limited, documented, and subject to more frequent review than standard access. Privileged accounts shall use strong authentication (including MFA), and privileged actions shall be logged and monitored. Shared privileged accounts shall be avoided when possible, and when necessary, their passwords shall be secured in an approved password management system with controlled access and regular rotation.

6.4 User Access Reviews

Access rights for all users shall be reviewed at regular intervals to ensure alignment with business needs and security requirements. Department managers shall conduct quarterly reviews of their team members' access rights to verify they remain appropriate for current roles and responsibilities. Systems containing PII data shall be subject to monthly access reviews. The IT/Security team shall provide reports to facilitate these reviews, and any discrepancies shall be documented and addressed promptly. Evidence of completed reviews shall be maintained for audit and compliance purposes. Additionally, a comprehensive organization-wide access review shall be conducted annually to identify any accumulated access rights or role misalignments.

6.5 Removal & Adjustment of Access Rights

Upon change in job role, transfer between departments, or termination of employment, user access rights shall be promptly reviewed and adjusted or removed as appropriate. Managers shall notify HR and IT/Security of any role changes requiring access adjustments. For terminations, all access shall be revoked immediately, with priority given to critical systems and those containing PII data. System credentials shall be changed if shared access was provided. Temporary access granted for specific projects shall be automatically revoked upon expiration of the defined timeframe.

6.6 Access Provisioning, Deprovisioning, and Change Procedure

Mozart ltd shall follow formalized procedures for provisioning, deprovisioning, and changing user access as detailed in Appendix A. These procedures shall ensure consistent implementation of access controls, maintain appropriate documentation, and support compliance requirements. All access changes shall be requested through the designated

system, include appropriate approvals, and be tracked to completion. Emergency access protocols shall be defined for situations requiring immediate access changes while maintaining security controls and documentation.

6.7 Segregation of Duties

Mozart ltd shall implement segregation of duties to reduce the risk of accidental or deliberate system misuse. Responsibilities shall be divided among different individuals where possible to ensure no single person can compromise a critical system or process. For critical functions related to financial systems or PII data processing, conflicting duties and responsibilities shall be separated. Where complete segregation is not practical due to company size, compensating controls such as monitoring, auditing, and management oversight shall be implemented. The access control matrix shall identify and prevent potentially conflicting role combinations.

7. User Responsibility for the Management of Secret Authentication Information

Users at Mozart ltd are responsible for safeguarding their authentication credentials (passwords, security tokens, certificates, etc.) used to access company systems and applications. Users shall treat all authentication information as strictly confidential, never sharing credentials with others, including IT staff or management. Any suspected compromise of authentication information shall be reported immediately to IT/Security, and users shall be held accountable for activities performed under their credentials. Regular security awareness training shall be provided to reinforce these responsibilities and ensure users understand the importance of proper credential management, particularly when working remotely.

7.1 Password Policy

Mozart ltd enforces the following password requirements for all systems and applications:

- Minimum password length of 12 characters
- Complexity requirements including uppercase, lowercase, numbers, and special characters
- Password expiration period of 90 days for standard users
- Password expiration period of 60 days for privileged accounts
- Password history enforcement preventing reuse of the last 8 passwords
- Account lockout after 5 consecutive failed login attempts
- Temporary lockout duration of 15 minutes, increasing with repeated failures
- Prohibition on sharing passwords between users
- Prohibition on using the same password across multiple systems
- Prohibition on storing passwords in unencrypted documents or notes
- Requirement to use the approved password manager for storing and generating passwords
- Different passwords required for work and personal accounts

8. System and Application Access

Access to Mozart ltd systems and applications shall be controlled through secure login procedures, with access limited to authorized users. System and application access shall be granted based on business requirements and the principle of least privilege. Critical systems and those processing PII data shall implement additional access controls, including multi-factor authentication and IP restrictions where appropriate. Inactive sessions shall be automatically terminated after a defined period of inactivity. All access attempts, successful and unsuccessful, shall be logged and monitored for suspicious patterns or potential security incidents.

8.1 Secure Log-on Procedures

Secure log-on procedures shall be implemented to minimize the risk of unauthorized access. These procedures include: displaying a general notice warning against unauthorized access; not displaying system or application identifiers until successful login; validating login information only upon completion of input; protecting against brute force login attempts; logging successful and failed login attempts; not transmitting passwords in clear text; implementing multi-factor authentication for all SaaS applications and critical systems, especially those containing PII data; and implementing appropriate session timeouts based on system sensitivity. For remote access, additional security measures including VPN and device posture checks shall be required before granting system access.

8.2 Password Management System

Mozart ltd shall implement a centralized password management system to facilitate secure password practices. The system shall support secure storage of passwords with strong encryption, generation of complex passwords, controlled sharing of credentials when necessary, and multi-factor authentication for access to the password management system itself. All employees shall use the approved password management system for storing and managing work-related credentials. The system shall be managed by the IT/Security team, with appropriate backup and recovery procedures in place. Administrators shall have the ability to reset user access to the password management system and enforce password policies.

8.3 Use of Privileged Utility Programs

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. Installation and use of such utilities shall require formal approval and be limited to personnel with a legitimate business need. All actions performed using privileged utility programs shall be logged and regularly reviewed. When not in use, these utilities shall be removed from systems or otherwise protected against unauthorized access. The IT/Security team shall maintain an inventory of approved utility programs and regularly review their necessity and usage patterns.

8.4 Access to Program Source Code

Access to program source code and related development tools shall be restricted to authorized development personnel only. Source code repositories shall be secured with appropriate access controls, and changes shall be tracked through version control systems. Non-developers shall not have access to production source code. Development, testing, and production environments shall be separated, with strict controls governing the movement of code between environments.

Code reviews shall be conducted prior to deployment to production, and access to deployment tools shall be restricted to authorized personnel. All source code shall be backed up regularly and stored securely.

9. Exceptions

Exceptions to this Access Control Policy may be granted only in exceptional circumstances where business requirements cannot be met within the established framework. All exceptions must be formally requested, documented, and approved by both the department head and the IT/Security Manager. Exceptions shall be temporary whenever possible, with a defined expiration date and plan for compliance. All exceptions shall be reviewed quarterly, documented in the risk register, and compensating controls shall be implemented where appropriate to mitigate potential security risks created by the exception.

10. Violations & Enforcement

Violations of this Access Control Policy may result in disciplinary action, up to and including termination of employment or contract. The severity of the disciplinary action will be determined based on the nature and impact of the violation, whether it was intentional or accidental, and whether it is a repeat offense. All suspected violations shall be reported to the IT/Security team and investigated promptly. If a violation results in a data breach, particularly involving PII data, appropriate incident response procedures shall be followed, including any required notifications under GDPR. The policy shall be enforced consistently across the organization regardless of role or position.

APPENDIX A - Access Management Procedure

This appendix outlines the detailed procedures for requesting, approving, implementing, and revoking access to Mozart ltd systems and information. These procedures shall be followed for all access management activities to ensure consistent application of access controls and maintain appropriate documentation for compliance purposes.

Access Request and Approval Process

- Employee or manager initiates access request through the designated request system
- Request must include:
    - User's full name and employee ID
    - Department and job role
    - Systems/applications requiring access
    - Type of access required (standard role or specific permissions)
    - Business justification
    - Duration (permanent or temporary with end date)
- Request is routed to appropriate approvers based on the systems involved:
    - Department manager for standard access
    - System owner for application-specific access
    - IT/Security Manager for privileged access
    - Data Protection Officer for access to systems containing PII

- Approved requests are implemented by the IT team within 24 hours (standard) or 4 hours (urgent)
- User and requestor are notified upon completion
- All requests and approvals are documented and retained for audit purposes

Access Modification and Removal Process

- For role changes:
    - HR or manager submits access modification request
    - Current access is reviewed against new role requirements
    - Unnecessary access is removed and new access is granted
    - Changes are documented and implemented within 24 hours
- For terminations:
    - HR notifies IT/Security immediately upon knowledge of termination
    - All system access is revoked within 24 hours (voluntary termination) or immediately (involuntary termination)
    - Shared credentials are changed if the departing user had knowledge of them
    - Remote access is disabled first, followed by application and network access
    - Company-owned devices are recovered and wiped
    - Final access termination report is provided to HR for documentation
- For emergency access revocation:
    - Emergency revocation can be initiated by manager, HR, Legal, or IT/Security
    - Access is immediately suspended pending review
    - Incident is documented and investigated
    - Restoration of access requires formal approval based on investigation results