

Statement of Applicability

1.0 / 2024-12-08

Demo Company  
m2x.rocks  
Demo Street 1  
  
**123456 Demo City**

# 5 Organizational controls

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Applicable** | **Implementation** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1 | Policies for Information Security | Y | * Develop and maintain an information security policy aligned with organizational objectives. * Review the policy annually or upon significant changes. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.2 | Information Security Roles and Responsibilities | Y | * Define clear roles and responsibilities for information security within the organization. * Ensure responsibilities are communicated to all relevant parties. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.3 | Segregation of Duties | Y | * Implement controls to ensure critical tasks are divided among individuals to reduce risks. * Review roles and privileges periodically to prevent unauthorized access. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.4 | Management Responsibilities | Y | * Ensure top management demonstrates commitment to the information security program. * Allocate resources for maintaining and improving the ISMS. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5 | Contact With Authorities | Y | * Establish protocols for contacting local authorities in case of a security incident. * Maintain an updated list of contact details for regulatory bodies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.6 | Contact With Special Interest Groups | Y | * Participate in relevant information security communities or groups. * Exchange best practices and threat intelligence. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.7 | Threat Intelligence | Y | * Establish processes for gathering, analyzing, and acting on threat intelligence. * Integrate findings into risk management and incident response plans. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.8 | Information Security in Project Management | Y | * Incorporate security requirements into the project lifecycle. * Conduct security risk assessments for all major projects. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.9 | Inventory of Information and Other Associated Assets | Y | * Create and maintain an up-to-date inventory of information assets. * Classify assets based on sensitivity and importance. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.10 | Acceptable Use of Information and Other Associated Assets | Y | * Develop an acceptable use policy outlining proper handling of information assets. * Provide regular training on acceptable use practices. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.11 | Return of Assets | Y | * Ensure employees return all issued assets upon termination or role change. * Verify returned assets are in good condition and properly accounted for. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.12 | Classification of Information | Y | * Define and apply information classification schemes (e.g., public, confidential). * Ensure proper handling of classified information based on its level. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.13 | Labelling of Information | Y | * Establish labeling guidelines for sensitive and critical information. * Ensure labels are applied consistently and reviewed regularly. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.14 | Information Transfer | Y | * Define procedures for securely transferring sensitive information. * Ensure encryption is used during transmission. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.15 | Access Control | Y | * Implement access control policies to limit access to authorized users only. * Conduct regular audits of access privileges. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.16 | Identity Management | Y | * Adopt robust identity verification mechanisms (e.g., multi-factor authentication). * Ensure identities are securely stored and managed. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.17 | Authentication Information | Y | * Securely store and manage authentication credentials (e.g., passwords). * Enforce strong password policies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.18 | Access Rights | Y | * Assign access rights based on the principle of least privilege. * Review access rights periodically to ensure compliance. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.19 | Information Security in Supplier Relationships | Y | * Establish security requirements for third-party suppliers. * Monitor supplier compliance with agreed security terms. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.20 | Addressing Information Security Within Supplier Agreements | Y | * Include information security clauses in all supplier agreements. * Perform due diligence before signing new contracts. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.21 | Managing Information Security in the ICT Supply Chain | Y | * Implement controls to manage supply chain risks. * Conduct periodic assessments of critical suppliers. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.22 | Monitoring, Review and Change Management of Supplier Services | Y | * Regularly monitor supplier services to ensure compliance. * Manage changes to supplier agreements systematically. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.23 | Information Security for Use of Cloud Services | Y | * Evaluate cloud providers based on their security certifications. * Implement controls to monitor cloud service usage and risks. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.24 | Information Security Incident Management Planning and Preparation | Y | * Develop an incident response plan for potential security breaches. * Conduct regular training and simulations for the response team. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.25 | Assessment and Decision on Information Security Events | Y | * Establish criteria to assess the severity of security events. * Ensure decisions are documented and communicated effectively. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.26 | Response to Information Security Incidents | Y | * Define steps to contain and mitigate security incidents. * Ensure incident response is timely and well-coordinated. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.27 | Learning From Information Security Incidents | Y | * Analyze incidents to identify root causes and lessons learned. * Update security controls and processes accordingly. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.28 | Collection of Evidence | Y | * Follow legal and organizational guidelines for evidence collection. * Ensure evidence integrity for potential legal proceedings. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.29 | Information Security During Disruption | Y | * Establish plans to ensure business continuity during disruptions. * Test plans regularly to ensure effectiveness. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.30 | ICT Readiness for Business Continuity | Y | * Ensure ICT systems can support critical operations during emergencies. * Maintain redundant systems for high availability. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.31 | Legal, Statutory, Regulatory and Contractual Requirements | Y | * Identify and comply with all relevant legal and contractual obligations. * Maintain records of compliance for audits and reviews. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.32 | Intellectual Property Rights | Y | * Protect intellectual property through proper agreements and licenses. * Monitor for unauthorized use of organizational IP. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.33 | Protection of Records | Y | * Implement controls to protect records from unauthorized access and loss. * Ensure record retention policies comply with legal requirements. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.34 | Privacy and Protection of PII | Y | * Establish procedures to protect personally identifiable information (PII). * Ensure compliance with applicable data protection regulations. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.35 | Independent Review of Information Security | Y | * Conduct periodic independent reviews of the ISMS. * Implement recommendations from the reviews to improve security posture. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.36 | Compliance With Policies, Rules and Standards for Information Security | Y | * Monitor compliance with internal and external security standards. * Document and address any non-compliance issues promptly. |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.37 | Documented Operating Procedures | Y | * Maintain documented operating procedures for all critical processes. * Ensure procedures are regularly reviewed and updated. |

# 6 People controls

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Applicable** | **Implementation** |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1 | Screening | Y | * Conduct background checks on all new hires. * Verify employment history and references. |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.2 | Terms and Conditions of Employment | Y | * Include security responsibilities in employment contracts. * Ensure contracts comply with organizational security policies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.3 | Information Security Awareness, Education and Training | Y | * Provide regular security awareness training for all employees. * Develop targeted training for specific roles (e.g., IT staff). |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.4 | Disciplinary Process | Y | * Define a clear disciplinary process for security violations. * Ensure employees are aware of consequences for non-compliance. |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.5 | Responsibilities After Termination or Change of Employment | Y | * Ensure access rights are revoked immediately upon termination. * Conduct exit interviews to reinforce confidentiality agreements. |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.6 | Confidentiality or Non-Disclosure Agreements | Y | * Require employees and contractors to sign NDAs before accessing sensitive information. * Periodically review and update confidentiality agreements. |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.7 | Remote Working | Y | * Implement security controls for remote work environments (e.g., VPNs). * Conduct regular audits of remote work policies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.8 | Information Security Event Reporting | Y | * Establish a centralized system for reporting security incidents. * Train employees on recognizing and reporting security events promptly. |

# 7 Physical controls

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Applicable** | **Implementation** |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.1 | Physical Security Perimeters | N | Remote only company; use external service providers for infrastructure |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.2 | Physical Entry | Y | * Implement access control systems for entry points. * Use biometric or badge-based authentication for secure entry. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.3 | Securing Offices, Rooms and Facilities | Y | * Ensure all offices and facilities have secure locks. * Install alarms for unauthorized access attempts. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.4 | Physical Security Monitoring | Y | * Deploy surveillance systems like CCTV cameras. * Monitor entry logs and respond to anomalies promptly. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.5 | Protecting Against Physical and Environmental Threats | Y | * Conduct risk assessments for environmental threats. * Implement fire suppression and flood prevention systems. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.6 | Working In Secure Areas | Y | * Define rules for working in secure areas (e.g., no mobile phones). * Ensure authorized access is monitored. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.7 | Clear Desk and Clear Screen | Y | * Enforce policies for clearing desks of sensitive documents. * Enable automatic screen locks after inactivity. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.8 | Equipment Siting and Protection | Y | * Position equipment in secure, low-risk areas. * Provide physical protection for critical devices. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.9 | Security of Assets Off-Premises | Y | * Maintain inventory of off-premises assets. * Ensure secure transport and storage of equipment. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.10 | Storage Media | Y | * Define protocols for securely storing media (e.g., encryption). * Ensure proper labeling and access controls. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.11 | Supporting Utilities | Y | * Ensure backup power supply for critical systems. * Maintain HVAC systems to protect equipment. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.12 | Cabling Security | Y | * Conceal cables to prevent tampering. * Secure cable paths in conduits or ducts. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.13 | Equipment Maintenance | Y | * Schedule regular maintenance for all critical equipment. * Ensure maintenance activities are logged and reviewed. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.14 | Secure Disposal or Re-Use of Equipment | Y | * Define procedures for secure equipment disposal. * Ensure data is completely wiped before reuse or recycling. |

# 8 Technological controls

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Applicable** | **Implementation** |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.1 | User Endpoint Devices | Y | * Implement security controls for all user devices. * Ensure regular updates and patches are applied. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.2 | Privileged Access Rights | Y | * Restrict and monitor the use of privileged accounts. * Implement multi-factor authentication for access. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.3 | Information Access Restriction | Y | * Use role-based access control (RBAC) to restrict access. * Audit access logs regularly to detect anomalies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.4 | Access to Source Code | Y | * Implement version control systems with restricted access. * Regularly review code repositories for unauthorized changes. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.5 | Secure Authentication | Y | * Use strong authentication mechanisms like MFA. * Regularly review and update authentication protocols. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.6 | Capacity Management | Y | * Ensure sufficient resources are available for critical systems. * Regularly monitor and plan for capacity needs. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.7 | Protection Against Malware | Y | * Deploy antivirus and anti-malware solutions. * Regularly update malware definitions. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.8 | Management of Technical Vulnerabilities | Y | * Conduct regular vulnerability assessments. * Implement timely patch management processes. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.9 | Configuration Management | Y | * Maintain an inventory of system configurations. * Ensure changes are tracked and approved. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.10 | Information Deletion | Y | * Define processes for secure data deletion. * Ensure compliance with data retention policies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.6 | Capacity Management | Y | * Ensure sufficient resources are available for critical systems. * Regularly monitor and plan for capacity needs. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.7 | Protection Against Malware | Y | * Deploy antivirus and anti-malware solutions. * Regularly update malware definitions. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.8 | Management of Technical Vulnerabilities | Y | * Conduct regular vulnerability assessments. * Implement timely patch management processes. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.9 | Configuration Management | Y | * Maintain an inventory of system configurations. * Ensure changes are tracked and approved. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.10 | Information Deletion | Y | * Define processes for secure data deletion. * Ensure compliance with data retention policies. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.16 | Monitoring Activities | Y | * Implement continuous monitoring for security threats. * Ensure monitoring covers all critical systems and networks. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.17 | Clock Synchronization | Y | * Ensure time synchronization across all systems. * Use secure NTP servers for synchronization. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.18 | Use of Privileged Utility Programs | Y | * Restrict access to utility programs with elevated privileges. * Regularly audit the use of such programs. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.19 | Installation of Software on Operational Systems | Y | * Implement strict controls for software installation. * Use only approved and tested software. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.20 | Networks Security | Y | * Deploy firewalls and intrusion detection systems (IDS). * Encrypt sensitive data transmitted over networks. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.21 | Security of Network Services | N | Using managed services of external service providers only |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.22 | Segregation of Networks | Y | * Isolate sensitive network segments from public access. * Use VLANs or subnets for logical segregation. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.23 | Web Filtering | Y | * Implement web filtering solutions to block malicious websites. * Define policies to restrict access to non-work-related sites. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.24 | Use of Cryptography | Y | * Encrypt sensitive data in transit and at rest. * Implement secure key management practices. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.25 | Secure Development Life Cycle | Y | * Integrate security measures at every stage of development. * Conduct regular security code reviews and testing. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.26 | Application Security Requirements | Y | * Define clear security requirements for applications. * Ensure security is built into the design phase. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.27 | Secure System Architecture and Engineering Principles | Y | * Follow best practices for secure system architecture. * Document and review security measures regularly. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.28 | Secure Coding | Y | * Train developers on secure coding practices. * Use tools to identify vulnerabilities in code. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.29 | Security Testing in Development and Acceptance | Y | * Conduct regular security tests during development. * Include penetration testing in acceptance criteria. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.30 | Outsourced Development | Y | * Ensure vendors comply with security standards. * Include security requirements in contracts. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.31 | Separation of Development, Test and Production Environments | Y | * Physically or logically separate development, test, and production systems. * Restrict access to production systems. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.32 | Change Management | Y | * Document all changes and obtain approval. * Assess the security impact of each change. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.33 | Test Information | Y | * Ensure test data is anonymized or obfuscated. * Restrict access to test environments. |

|  |  |  |  |
| --- | --- | --- | --- |
| 8.34 | Protection of Information Systems During Audit Testing | Y | * Ensure audit tests do not impact production systems. * Follow guidelines to maintain data confidentiality during audits. |