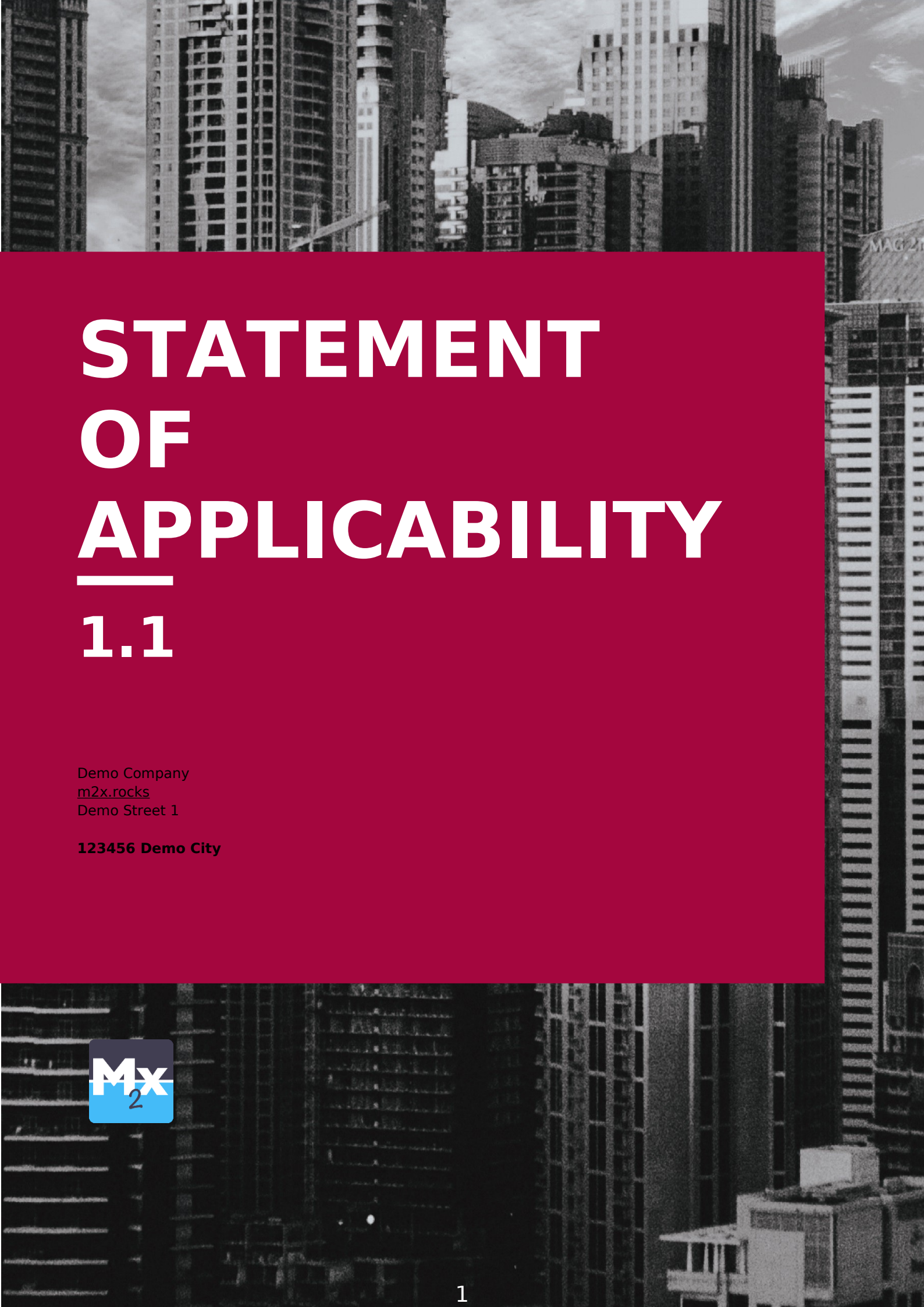

STATEMENT OF APPLICABILITY

1.1

Demo Company
m2x.rocks
Demo Street 1

123456 Demo City

DEMO: Statement of Applicability

5 Organizational controls

5.1 POLICIES FOR INFORMATION SECURITY

APPLICABLE

• 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

APPLICABLE

• Define clear roles and responsibilities for information security within the organization.

• Ensure responsibilities are communicated to all relevant parties.

5.3 SEGREGATION OF DUTIES

APPLICABLE

• 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

APPLICABLE

• Ensure top management demonstrates commitment to the information security program.

• Allocate resources for maintaining and improving the ISMS.

5.5 CONTACT WITH AUTHORITIES

APPLICABLE

• 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

APPLICABLE

• Participate in relevant information security communities or groups.

• Exchange best practices and threat intelligence.

5.7 THREAT INTELLIGENCE

APPLICABLE

• 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

APPLICABLE

• Incorporate security requirements into the project lifecycle.

• Conduct security risk assessments for all major projects.

5.9 INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS

APPLICABLE

• 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

APPLICABLE

• Develop an acceptable use policy outlining proper handling of information assets.

• Provide regular training on acceptable use practices.

5.11 RETURN OF ASSETS

APPLICABLE

• 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

APPLICABLE

• 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

APPLICABLE

• Establish labeling guidelines for sensitive and critical information.

• Ensure labels are applied consistently and reviewed regularly.

5.14 INFORMATION TRANSFER

APPLICABLE

• Define procedures for securely transferring sensitive information.

• Ensure encryption is used during transmission.

5.15 ACCESS CONTROL

APPLICABLE

• Implement access control policies to limit access to authorized users only.

• Conduct regular audits of access privileges.

5.16 IDENTITY MANAGEMENT

APPLICABLE

• Adopt robust identity verification mechanisms (e.g., multi-factor authentication).

• Ensure identities are securely stored and managed.

5.17 AUTHENTICATION INFORMATION

APPLICABLE

• Securely store and manage authentication credentials (e.g., passwords).

• Enforce strong password policies.

5.18 ACCESS RIGHTS

APPLICABLE

• Assign access rights based on the principle of least privilege.

• Review access rights periodically to ensure compliance.

5.19 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS

APPLICABLE

• Establish security requirements for third-party suppliers.

• Monitor supplier compliance with agreed security terms.

5.20 ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS

APPLICABLE

• 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

APPLICABLE

• Implement controls to manage supply chain risks.

• Conduct periodic assessments of critical suppliers.

5.22 MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES

APPLICABLE

• Regularly monitor supplier services to ensure compliance.

• Manage changes to supplier agreements systematically.

5.23 INFORMATION SECURITY FOR USE OF CLOUD SERVICES

APPLICABLE

• 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

APPLICABLE

• 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

APPLICABLE

• Establish criteria to assess the severity of security events.

• Ensure decisions are documented and communicated effectively.

5.26 RESPONSE TO INFORMATION SECURITY INCIDENTS

APPLICABLE

• Define steps to contain and mitigate security incidents.

• Ensure incident response is timely and well-coordinated.

5.27 LEARNING FROM INFORMATION SECURITY INCIDENTS

APPLICABLE

• Analyze incidents to identify root causes and lessons learned.

• Update security controls and processes accordingly.

5.28 COLLECTION OF EVIDENCE

APPLICABLE

• Follow legal and organizational guidelines for evidence collection.

• Ensure evidence integrity for potential legal proceedings.

5.29 INFORMATION SECURITY DURING DISRUPTION

APPLICABLE

• Establish plans to ensure business continuity during disruptions.

• Test plans regularly to ensure effectiveness.

5.30 ICT READINESS FOR BUSINESS CONTINUITY

APPLICABLE

• Ensure ICT systems can support critical operations during emergencies.

• Maintain redundant systems for high availability.

5.31 LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS

APPLICABLE

• Identify and comply with all relevant legal and contractual obligations.

• Maintain records of compliance for audits and reviews.

5.32 INTELLECTUAL PROPERTY RIGHTS

APPLICABLE

• Protect intellectual property through proper agreements and licenses.

• Monitor for unauthorized use of organizational IP.

5.33 PROTECTION OF RECORDS

APPLICABLE

• 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

APPLICABLE

• Establish procedures to protect personally identifiable information (PII).

• Ensure compliance with applicable data protection regulations.

5.35 INDEPENDENT REVIEW OF INFORMATION SECURITY

APPLICABLE

• 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

APPLICABLE

• Monitor compliance with internal and external security standards.

• Document and address any non-compliance issues promptly.

5.37 DOCUMENTED OPERATING PROCEDURES

APPLICABLE

• Maintain documented operating procedures for all critical processes.

• Ensure procedures are regularly reviewed and updated.

6 People controls

6.1 SCREENING

APPLICABLE

• Conduct background checks on all new hires.

• Verify employment history and references.

6.2 TERMS AND CONDITIONS OF EMPLOYMENT

APPLICABLE

• Include security responsibilities in employment contracts.

• Ensure contracts comply with organizational security policies.

6.3 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

APPLICABLE

• Provide regular security awareness training for all employees.

• Develop targeted training for specific roles (e.g., IT staff).

6.4 DISCIPLINARY PROCESS

APPLICABLE

• 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

APPLICABLE

• Ensure access rights are revoked immediately upon termination.

• Conduct exit interviews to reinforce confidentiality agreements.

6.6 CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS

APPLICABLE

• Require employees and contractors to sign NDAs before accessing sensitive information.

• Periodically review and update confidentiality agreements.

6.7 REMOTE WORKING

APPLICABLE

• Implement security controls for remote work environments (e.g., VPNs).

• Conduct regular audits of remote work policies.

6.8 INFORMATION SECURITY EVENT REPORTING

APPLICABLE

• Establish a centralized system for reporting security incidents.

• Train employees on recognizing and reporting security events promptly.

7 Physical controls

7.1 PHYSICAL SECURITY PERIMETERS

NOT APPLICABLE

Remote only company; use external service providers for infrastructure

7.2 PHYSICAL ENTRY

APPLICABLE

• Implement access control systems for entry points.

• Use biometric or badge-based authentication for secure entry.

7.3 SECURING OFFICES, ROOMS AND FACILITIES

APPLICABLE

• Ensure all offices and facilities have secure locks.

• Install alarms for unauthorized access attempts.

7.4 PHYSICAL SECURITY MONITORING

APPLICABLE

• Deploy surveillance systems like CCTV cameras.

• Monitor entry logs and respond to anomalies promptly.

7.5 PROTECTING AGAINST PHYSICAL AND ENVIRONMENTAL THREATS

APPLICABLE

• Conduct risk assessments for environmental threats.

• Implement fire suppression and flood prevention systems.

7.6 WORKING IN SECURE AREAS

APPLICABLE

• Define rules for working in secure areas (e.g., no mobile phones).

• Ensure authorized access is monitored.

7.7 CLEAR DESK AND CLEAR SCREEN

APPLICABLE

• Enforce policies for clearing desks of sensitive documents.

• Enable automatic screen locks after inactivity.

7.8 EQUIPMENT SITING AND PROTECTION

APPLICABLE

• Position equipment in secure, low-risk areas.

• Provide physical protection for critical devices.

7.9 SECURITY OF ASSETS OFF-PREMISES

APPLICABLE

• Maintain inventory of off-premises assets.

• Ensure secure transport and storage of equipment.

7.10 STORAGE MEDIA

APPLICABLE

• Define protocols for securely storing media (e.g., encryption).

• Ensure proper labeling and access controls.

7.11 SUPPORTING UTILITIES

APPLICABLE

• Ensure backup power supply for critical systems.

• Maintain HVAC systems to protect equipment.

7.12 CABLING SECURITY

APPLICABLE

• Conceal cables to prevent tampering.

• Secure cable paths in conduits or ducts.

7.13 EQUIPMENT MAINTENANCE

APPLICABLE

• Schedule regular maintenance for all critical equipment.

• Ensure maintenance activities are logged and reviewed.

7.14 SECURE DISPOSAL OR RE-USE OF EQUIPMENT

APPLICABLE

• Define procedures for secure equipment disposal.

• Ensure data is completely wiped before reuse or recycling.

8 Technological controls

8.1 USER ENDPOINT DEVICES

APPLICABLE

• Implement security controls for all user devices.

• Ensure regular updates and patches are applied.

8.2 PRIVILEGED ACCESS RIGHTS

APPLICABLE

• Restrict and monitor the use of privileged accounts.

• Implement multi-factor authentication for access.

8.3 INFORMATION ACCESS RESTRICTION

APPLICABLE

• Use role-based access control (RBAC) to restrict access.

• Audit access logs regularly to detect anomalies.

8.4 ACCESS TO SOURCE CODE

APPLICABLE

• Implement version control systems with restricted access.

• Regularly review code repositories for unauthorized changes.

8.5 SECURE AUTHENTICATION

APPLICABLE

• Use strong authentication mechanisms like MFA.

• Regularly review and update authentication protocols.

8.6 CAPACITY MANAGEMENT

APPLICABLE

• Ensure sufficient resources are available for critical systems.

• Regularly monitor and plan for capacity needs.

8.7 PROTECTION AGAINST MALWARE

APPLICABLE

• Deploy antivirus and anti-malware solutions.

• Regularly update malware definitions.

8.8 MANAGEMENT OF TECHNICAL VULNERABILITIES

APPLICABLE

• Conduct regular vulnerability assessments.

• Implement timely patch management processes.

8.9 CONFIGURATION MANAGEMENT

APPLICABLE

• Maintain an inventory of system configurations.

• Ensure changes are tracked and approved.

8.10 INFORMATION DELETION

APPLICABLE

• Define processes for secure data deletion.

• Ensure compliance with data retention policies.

8.6 CAPACITY MANAGEMENT

APPLICABLE

• Ensure sufficient resources are available for critical systems.

• Regularly monitor and plan for capacity needs.

8.7 PROTECTION AGAINST MALWARE

APPLICABLE

• Deploy antivirus and anti-malware solutions.

• Regularly update malware definitions.

8.8 MANAGEMENT OF TECHNICAL VULNERABILITIES

APPLICABLE

• Conduct regular vulnerability assessments.

• Implement timely patch management processes.

8.9 CONFIGURATION MANAGEMENT

APPLICABLE

• Maintain an inventory of system configurations.

• Ensure changes are tracked and approved.

8.10 INFORMATION DELETION

APPLICABLE

• Define processes for secure data deletion.

• Ensure compliance with data retention policies.

8.16 MONITORING ACTIVITIES

APPLICABLE

• Implement continuous monitoring for security threats.

• Ensure monitoring covers all critical systems and networks.

8.17 CLOCK SYNCHRONIZATION

APPLICABLE

• Ensure time synchronization across all systems.

• Use secure NTP servers for synchronization.

8.18 USE OF PRIVILEGED UTILITY PROGRAMS

APPLICABLE

• Restrict access to utility programs with elevated privileges.

• Regularly audit the use of such programs.

8.19 INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS

APPLICABLE

• Implement strict controls for software installation.

• Use only approved and tested software.

8.20 NETWORKS SECURITY

APPLICABLE

• Deploy firewalls and intrusion detection systems (IDS).

• Encrypt sensitive data transmitted over networks.

8.21 SECURITY OF NETWORK SERVICES

NOT APPLICABLE

Using managed services of external service providers only

8.22 SEGREGATION OF NETWORKS

APPLICABLE

• Isolate sensitive network segments from public access.

• Use VLANs or subnets for logical segregation.

8.23 WEB FILTERING

APPLICABLE

• Implement web filtering solutions to block malicious websites.

• Define policies to restrict access to non-work-related sites.

8.24 USE OF CRYPTOGRAPHY

APPLICABLE

• Encrypt sensitive data in transit and at rest.

• Implement secure key management practices.

8.25 SECURE DEVELOPMENT LIFE CYCLE

APPLICABLE

• Integrate security measures at every stage of development.

• Conduct regular security code reviews and testing.

8.26 APPLICATION SECURITY REQUIREMENTS

APPLICABLE

• Define clear security requirements for applications.

• Ensure security is built into the design phase.

8.27 SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES

APPLICABLE

• Follow best practices for secure system architecture.

• Document and review security measures regularly.

8.28 SECURE CODING

APPLICABLE

• Train developers on secure coding practices.

• Use tools to identify vulnerabilities in code.

8.29 SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE

APPLICABLE

• Conduct regular security tests during development.

• Include penetration testing in acceptance criteria.

8.30 OUTSOURCED DEVELOPMENT

APPLICABLE

• Ensure vendors comply with security standards.

• Include security requirements in contracts.

8.31 SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS

APPLICABLE

• Physically or logically separate development, test, and production systems.

• Restrict access to production systems.

8.32 CHANGE MANAGEMENT

APPLICABLE

• Document all changes and obtain approval.

• Assess the security impact of each change.

8.33 TEST INFORMATION

APPLICABLE

• Ensure test data is anonymized or obfuscated.

• Restrict access to test environments.

8.34 PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING

APPLICABLE

• Ensure audit tests do not impact production systems.

• Follow guidelines to maintain data confidentiality during audits.