□ ÖFFENTLICH | PUBLIC

ISO/IEC 27001

Statement of Applicability [SoA]

SAE IT-systems GmbH & Co. KG

Publisher	SAE IT-systems GmbH & Co. KG Im Gewerbegebiet Pesch 14 50767 Köln (Cologne, Germany)
File	Statement of Applicability [SoA]
Version	1.1
Date	08.05.2023
Created by	Markus Dewerny (ISO)
Classification	Public

A.5 Information Security Policies

A.5.1 Management Direction for Information Security

A.5.1.1	Policies for Information Security	✓
A.5.1.2	Review of the Policies for Information Security	✓

A.6 Organization of Information Security

A.6.1 Internal Organization

A.6.1.1	Information Security Roles & Responsibilities	✓
A.6.1.2	Segregation of Duties	✓
A.6.1.3	Contact with Authorities	✓
A.6.1.4	Contact with Special Interest Groups	✓
A.6.1.5	Information Security in Project Management	✓

A.6.2 Mobile Devices & Teleworking

A.6.2.1	Mobile Device Policy	✓
A.6.2.2	Teleworking	✓

A.7 Human Resource Security

A.7.1 Prior to Employment

A.7.1.1	Screening	✓
A.7.1.2	Terms & Conditions of Employment	✓

A.7.2 During Employment

A.7.2.1	Management Responsibilities	✓
A.7.2.2	Information Security Awareness, Education & Training	✓
A.7.2.3	Disciplinary Process	✓

A.7.3 Termination & Change of Employment

A.7.3.1	Termination or Change of Employment Responsibilities	✓

A.8 Asset Management

A.8.1 Prior to Employment

A.8.1.1	Inventory of Assets	✓
A.8.1.2	Ownership of Assets	✓
A.8.1.3	Acceptable Use of Assets	✓
A.8.1.4	Return of Assets	✓

A.8.2 Information Classification

A.8.2.1	Classification of Information	✓
A.8.2.2	Labelling of Information	✓
A.8.2.3	Handling of Assets	✓

A.8.3 Media Handling

A.8.3.1	Management of Removable Media	✓
A.8.3.2	Disposal of Media	✓
A.8.3.3	Physical Media Transfer	✓

A.9 Access Control

A.9.1 Access Control Policy

A.9.1.1	Access Control Policy	✓
A.9.1.2	Access to Networks & Network Services	✓

A.9.2 Management Direction for Information Security

A.9.2.1	User Registration & De-Registration	✓
A.9.2.2	User Access Provisioning	✓
A.9.2.3	Management of Privileged Access Rights	✓
A.9.2.4	Management of Secret Authentication Information of Users	✓
A.9.2.5	Review of User Access Rights	✓
A.9.2.6	Removal or Adjustment of Access Rights	✓

A.9.3 User Responsibilities

A.9.3.1	Use of Secret Authentication Information	✓

A.9.4 System and Application Access Control

A.9.4.1	Information Access Restriction	✓
A.9.4.2	Secure Log-On Procedures	✓
A.9.4.3	Password Management Systems	✓
A.9.4.4	Use of Privileged Utility Programs	✓
A.9.4.5	Access Control to Program Source Code	✓

A.10 Cryptography

A.10.1 Cryptographic Controls

A.10.1.1	Policy on the Use of Cryptographic Controls	✓
A.10.1.2	Key Management	✓

A.11 Physical & environmental Security

A.11.1 Secure Areas

A.11.1.1	Physical Security Perimeter	✓
A.11.1.2	Physical Entry Controls	✓
A.11.1.3	Securing Offices, Rooms & Facilities	✓
A.11.1.4	Protecting against External & Environmental Threats	✓
A.11.1.5	Working in Secure Areas	✓
A.11.1.6	Delivery & Loading Areas	✓

A.11.2 Equipment

A.11.2.1	Equipment Siting & Protection	✓
A.11.2.2	Supporting Utilities	✓
A.11.2.3	Cabling Security	✓
A.11.2.4	Equipment Maintenance	✓
A.11.2.5	Removal of Assets	✓
A.11.2.6	Security of Equipment & Assets off-premises	✓
A.11.2.7	Secure Disposal or Re-Use of Equipment	✓
A.11.2.8	Unattended User Equipment	✓
A.11.2.9	Clear Desk & Clear Screen Policy	✓

A.12 Operational Security

A.12.1 Operational Procedures & Responsibilities

A.12.1.1	Documented Operating Procedures	✓
A.12.1.2	Change Management	✓
A.12.1.3	Capacity Management	✓
A.12.1.4	Separation of Development, Testing & Operational Environments	✓

A.12.2 Protection from Malware

A.12.2.1	Controls against Malware	✓

A.12.3 Backup

A.12.3.1	Information Backup	✓

A.12.4 Logging & Monitoring

A.12.4.1	Event logging	✓
A.12.4.2	Protection of log Information	✓
A.12.4.3	Administrator & Operator logs	✓
A.12.4.4	Clock Synchronization	✓

A.12.5 Control of Operational Software

A.12.5.1	Installation of Software on Operational Systems	✓

A.12.6 Technical Vulnerability Management

A.12.6.1	Management of Technical Vulnerabilities	✓
A.12.6.2	Restrictions on Software Installation	✓

A.12.7 Information Systems Audit Considerations

A.12.7.1	Information Systems Audit Controls	✓

A.13 Communications Security

A.13.1 Network Security Management

A.13.1.1	Network Controls	✓
A.13.1.2	Security of Network Services	✓
A.13.1.3	Segregation in Networks	✓

A.13.2 Information Transfers

A.13.2.1	Information Transfer Policies & Procedures	✓
A.13.2.2	Agreements on Information Transfer	✓
A.13.2.3	Electronic Messaging	✓
A.13.2.4	Confidentiality or Non-Disclosure Agreements	✓

A.14 System Acquisition, Development & Maintenance

A.14.1 Security Requirements of Information Systems

A.14.1.1	Information Security Requirements Analysis & Specification	✓
A.14.1.2	Securing Application Services on Public Networks	✓
A.14.1.3	Protecting Application Services Transactions	✓

A.14.2 Security in Development & Support Processes

A.14.2.1	Secure Development Policy	✓
A.14.2.2	System Change Control Procedures	✓
A.14.2.3	Technical Review of Applications after Operating Platform Changes	✓
A.14.2.4	Restrictions on Changes to Software Packages	✓
A.14.2.5	Secure System Engineering Principles	✓
A.14.2.6	Secure Development Environment	✓
A.14.2.7	Outsourced Development	✓
A.14.2.8	System Security Testing	✓
A.14.2.9	System Acceptance Testing	✓
A.14.2.10 ENR	Least Functionality	✓

A.14.3 Test Data

A.14.3.1	Protection of Test Data	✓

A.15 Supplier Relationship

A.15.1 Information Security in Supplier Relationships

A.15.1.1	Information Security Policy for Supplier Relationships	✓
A.15.1.2	Addressing Security within Supplier Agreements	✓
A.15.1.3	Information & Communication Technology Supply Chain	✓

A.15.2 Supplier Service Delivery Management

A.15.2.1	Monitoring & Review of Supplier Services	✓
A.15.2.2	Managing Changes to Supplier Services	✓

A.16 Information Security Incident Management

A.16.1 Management of Information Security Incidents & Improvements

A.16.1.1	Responsibilities & Procedures	✓
A.16.1.2	Reporting Information Security Events	✓
A.16.1.3	Reporting Information Security Weaknesses	✓
A.16.1.4	Assessment of & Decision on Information Security Events	✓
A.16.1.5	Response to Information Security Incidents	✓
A.16.1.6	Learning from Information Security Incidents	✓
A.16.1.7	Collection of Evidence	✓

A.17 Information Security Aspects of Business Continuity

A.17.1 Information Security Continuity

A.17.1.1	Planning Information Security Continuity	✓
A.17.1.2	Implementing Information Security Continuity	✓
A.17.1.3	Verify, Review & Evaluate Information Security Continuity	✓

A.17.2 Redundancies

A.17.2.1	Availability of Information Processing Facilities	✓

A.18 Compliance

A.18.1 Compliance with Legal & Contractual Requirements

A.18.1.1	Identification of Applicable Legislation & Contractual Requirements	✓
A.18.1.2	Intellectual Property Rights	✓
A.18.1.3	Protection of Records	✓
A.18.1.4	Privacy & Protection of Personally Identifiable Information	✓
A.18.1.5	Regulation of Cryptographic Controls	✓

A.18.2 Information Security Reviews

A.18.2.1	Independent Review of Information Security	✓
A.18.2.2	Compliance with Security Policies & Standards	✓
A.18.2.3	Technical Compliance Review	✓