Document Title	Statement of Applicability
Document Owner	Karly Kaufman
Data Classification	Public

Version	Modified Date	Approved Date	Responsible	Reason/Comments
0.1	12.8.2020		Rudi Coetzee	Initial Creation
0.2	01.1.2021		Suela Kodra	Added reference documents and reasons for controls
0.3	28.1.2021		Stephan Adler	Review and Update
1.0	28.1.2021	28.1.2021	Heiko Will	Approved

1.1	21.4.2021		Suela Kodra;
			Stefan Sowa;
			Stephan Adler
				Updated with added references and date format in version history

2.0		4.5.2021	Heiko Will	Approved

2.1	12.5.2021		Suela Kodra;
			Stefan Sowa;
			Stephan Adler
				Review and Update

2.2	26.04.2023	26.04.2023	Karly Kaufman; Stephan Adler	Review and Update; Approved
2.3	01.04.2024		Karly Kaufman	Updated to the new ISO standard;
3.0		09.04.2024	Stephan Adler	Approved
3.1	07.06.2024	07.06.2024	Karly Kaufman; Stephan Adler	Updated evidence to reflect current state; Approved

Statement of Applicability

Section	Information security control	Evidence/Notes	Applicable
A5	**Organizational controls**		
A.5.1	Policies for information security	Information Security Policy; ISMS Manual; Security Concept; Export of Policies/Procedures on the Safety io wiki space	Yes
A.5.2	Information security roles and responsibilities	ISMS Manual; Information Security Policy; Job Descriptions;	Yes
A.5.3	Segregation of duties	ISMS Manual; Information Security Policy; Access Control Policy; Segregation of Duties Screenshots; Security Specialist Job Description, SWAPP Promotion Process; Org Chart Miro	Yes
A.5.4	Management responsibilities	Information Security Policy, ISMS Manual, Computer Security Incident Response Plan, Budget Plan showing Penetration Testing	Yes
A.5.5	Contact with authorities	Computer Security Incident Response Plan (Annex II);	Yes
A.5.6	Contact with special interest groups	Computer Security Incident Response Plan (Annex II); Security Scorecard Safety io Detailed Report	Yes
A.5.7	Threat intelligence	Vulnerability Management Policy; AWS GuardDuty; MendIO; SonarCloud	Yes
A.5.8	Information security in project management	Information Security Risk Management Policy; Software Development Process; Threat modeling process wiki; SWAPP Software Development Plan Deliverables	Yes
A.5.9	Inventory of information and other associated assets	ISMS Asset Inventory; Audit Log Screenshot	Yes
A.5.10	Acceptable use of information and other associated assets	Acceptable Use Policy	Yes
A.5.11	Return of assets	Safety io Arbeitsvertrag_AT; off-boarding checklist	Yes
A.5.12	Classification of information	Data Classification Policy	Yes
A.5.13	Labelling of information	Security Concept; Data Classification Policy; DP Permission Management Wiki; Salesforce PII labeling evidence;	Yes
A.5.14	Information transfer	Data Classification Policy	Yes
A.5.15	Access control	Access Control Policy; Workplace Visitor Process; Key Fob Log (Internal and External); Draft IAM Procedure; Privileged Access Screenshots; Access Control List wiki; AWS Access Request; Periododic Access Reviews; Audit Log	Yes
A.5.16	Identity management	Access Control Policy; Privileged Access Screenshots; Access Control List wiki; AWS Privledged Access Evidence	Yes
A.5.17	Authentication information	Access Control Policy; Privileged Access Screenshots; Access Control List wiki; AWS Privledged Access Evidence	Yes
A.5.18	Access rights	Access Control Policy; Privileged Access Screenshots; Access Control List wiki; AWS Privledged Access Evidence	Yes

Statement of Applicability

Section	Information security control	Evidence/Notes	Applicable
A.5.19	Information security in supplier relationships	Supplier Security Policy;AWS NDA; Safety io Information Security Questionnaire; Safety io Vendors & Suppliers	Yes
A.5.20	Addressing information security within supplier agreements	Supplier Security Policy; AWS_NDA; Safety io Work for Hire Agreement; Vendor/Supplier Confluence Page; Accionlabs Contract;	Yes
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	Supplier Security Policy; Vendor/Supplier Confluence Page	Yes
A.5.22	Monitoring, review and change management of supplier services	Supplier Security Policy; Vendor/Supplier Confluence Page; Apple Business Manager Screenshot	Yes
A.5.23	Information security for use of cloud services	Draft Cloud Security Policy with AWS; AWS Shared Responsibility Model;	Yes
A.5.24	Information security incident management planning and preparation	Computer Security Incident Response Plan; Crowdstrike Executive Tabletop Exercise	Yes
A.5.25	Assessment and decision on information security events	Computer Security Incident Response Plan; Crowdstrike Executive Tabletop Exercise	Yes
A.5.26	Response to information security incidents	Computer Security Incident Response Plan; Crowdstrike Executive Tabletop Exercise	Yes
A.5.27	Learning from information security incidents	Computer Security Incident Response Plan; Crowdstrike Executive Tabletop Exercise	Yes
A.5.28	Collection of evidence	Computer Security Incident Response Plan; Crowdstrike Executive Tabletop Exercise	Yes
A.5.29	Information security during disruption	Computer Security Incident Response Plan; Show SDP Health Dashboard in real time.	Yes
A.5.30	ICT readiness for business continuity	MSA's Business Continuity Plan	Yes
A.5.31	Legal, statutory, regulatory and contractual requirements	Legal, regulatory and contractual requirements	Yes
A.5.32	Intellectual property rights	NPD N4 Intellectual Property; Leverage Intellectual Property SharePoint site from Renee; Security Concept	Yes
A.5.33	Protection of records	Data Classification Policy; S3 backup screenshot	Yes
A.5.34	Privacy and protection of personal identifiable information (PII)	Legal, regulatory and contractual requirements; Data Classification Policy; MSA's Privacy Statement	Yes
A.5.35	Independent review of information security	ISMS Manual; Internal Audit Process; Internal Audit Report; Internal and External Audit Jira Ticket Screenshots	Yes
A.5.36	Compliance with policies, rules and standards for information security	ISMS Manual; Internal Audit Process; Safety io Refresher and New-Hire Training Screenshots; Clear desk evidence; SDP Health evidence	Yes
A.5.37	Documented operating procedures	ISMS Manual; Internal Audit Process; Safety io Office How tos wiki space; Safety io Office How tos MacBook Cleanup	Yes
A6	**People controls**		
A.6.1	Screening	On/Off Boarding Checklists	Yes
A.6.2	Terms and conditions of employment	Safety io Arbeitsvertrag_AT; Safety io South Africa Employment Agreement Template; Letter of Acceptance	Yes

Statement of Applicability

Section	Information security control	Evidence/Notes	Applicable
A.6.3	Information security awareness, education and training	ISMS Manual; KnowBe4 Training Platform; Safety io new hire and annual refresher training screenshots	Yes
A.6.4	Disciplinary process	Information Security Policy; Progressive Discipline Policy	Yes
A.6.5	Responsibilities after termination or change of employment	Letter of Acceptance; Off-Boarding Checklist	Yes
A.6.6	Confidentiality or non-disclosure agreements	Supplier Security Policy; Safety io Work Agreement; Safety io Arbeitsvertrag_AT; South Africa NDA for Tenacious	Yes
A.6.7	Remote working	Teleworking Policy; Mobile Device and Removable Media Policy	Yes
A.6.8	Information security event reporting	Computer Security Incident Response Plan; Security training screenshot	Yes
A7	**Physical controls**		
A.7.1	Physical security perimeters	Security Concept; Entrance Photos for Berlin and South Africa	Yes
A.7.2	Physical entry	Access Control Policy; Berlin/Johannesburg/Capetown Photos	Yes
A.7.3	Securing offices, rooms and facilities	Security Concept; Access Control Policy; Berlin/Johannesburg/Capetown Photos	Yes
A.7.4	Physical security monitoring	Surveillance Camera Evidence; Berlin/Johannesburg/Capetown Photos	Yes
A.7.5	Protecting against physical and environmental threats	Security Concept; Berlin photos	Yes
A.7.6	Working in secure areas	Security Concept; Berlin/Johannesburg/Capetown Photos	Yes
A.7.7	Clear desk and clear screen	Security Concept; Clear Workstation Evidence; Jira ticket regarding walk audit; Clear Desk and Clear Screen Policy	Yes
A.7.8	Equipment siting and protection	Security Concept; Berlin photos	Yes
A.7.9	Security of assets off-premises	Security Concept; Mobile Device and Removable Media Policy; AWS SOC 2 Report	Yes
A.7.10	Storage media	Security Concept; Mobile Device and Removable Media Policy; Macbook Decomm how to	Yes
A.7.11	Supporting utilities	Security Concept; agreement with utility providers in all locations	Yes
A.7.12	Cabling security	Security Concept; Berlin photos	Yes
A.7.13	Equipment maintenance	Security Concept; Berlin agreements;	Yes
A.7.14	Secure disposal or re-use of equipment	Security Concept; Macbook wipe process wiki; Stefan Sowa office photos	Yes
A8	**Technological controls**		
A.8.1	User end point devices	Berlin IT Inventory Wiki PDF; InTune screenshots	Yes
A.8.2	Privileged access rights	Access Control Policy; Administrators Policy; Privileged Access Screenshots; IAM Identity Center; ISMS AWS Access Request	Yes
A.8.3	Information access restriction	Data Classification Policy; Access Control Policy; Privileged Access Screenshots; IAM Identity Center; ISMS AWS Access Request	Yes
A.8.4	Access to source code	Access Control Policy/Pull Request screenshots with approvals	Yes

Statement of Applicability

Section	Information security control	Evidence/Notes	Applicable
A.8.5	Secure authentication	Safety io VPN wiki pages; screenshots of remote Berlin users authenticating	Yes
A.8.6	Capacity management	AWS Autoscaling Screenshot; Software Development Plan; Sample of Performance Testing Screenshot; Software Development Plan Deliverables	Yes
A.8.7	Protection against malware	Security Concept; InTune screenshots	Yes
A.8.8	Management of technical vulnerabilities	Vulnerability Management Policy; Vulnerability Management Jira Space	Yes
A.8.9	Configuration management	Anonymized data screenshot; code repository in the CLI space; System and Organization Controls Report; AWS SOC2 Report;	Yes
A.8.10	Information deletion	S3 Screenshot Retention Policy; Microsoft Teams Retention Period screenshot; Microsoft Teams Channel Screenshot;	Yes
A.8.11	Data masking	Amazon Macie - Wiki; Amazon Macie ticket screenshot; Data masking test evidence pdf; Data masking Jira ticket;	Yes
A.8.12	Data leakage prevention	Data Classification Policy; Mobile Device and Removable Storage Policy; Data Loss Prevention Document; Security Scorecard Screenshot; Office 365 Offerings;	Yes
A.8.13	Information backup	Security Concept; Backup Overview; Backup Retention Policy; Jenkins backup screenshots; AWS Back-Ups DevOps	Yes
A.8.14	Redundancy of information processing facilities	AWS screenshot on zones.	Yes
A.8.15	Logging	Security Concept; AWS Event Logging Screenshot; DataDog Log Evidence; GuardDuty Screenshot; Log Management Data Security; Log Storage Evidence	Yes
A.8.16	Monitoring Activities	Security Concept; AWS Event Logging Screenshot; DataDog Log Evidence; GuardDuty Screenshot;	Yes
A.8.17	Clock synchronization	Security Concept; AWS Clock Synchronization	Yes
A.8.18	Use of privileged utility programs	Intune Evidence Descripton	Yes
A.8.19	Installation of software on operational systems	Administrators Policy; Security Concept; Approved Software Sources wiki;	Yes
A.8.20	Networks security	Security Concept; Network Diagram; Network Segmentation	Yes
A.8.21	Security of network services	Security Concept; AWS shared responsibility model	Yes
A.8.22	Segregation of networks	Security Concept; Network Diagram; Network Segmentation	Yes
A.8.23	Web filtering	Reference ticket: https://msasafety.atlassian.net/browse/SIOOFFICE-510 (screenshot in folder, pull up ticket in real time with attachments).	Yes
A.8.24	Use of cryptography	Cryptographic Key Management Policy; AWS Key Management Service	Yes
A.8.25	Secure development life cycle	SonarCube and MendIO Evidence; Software Development Plan	Yes
A.8.26	Application security requirements	Threat Modeling Grid Summon PDF; Threat Modeling Summary; Application Security Requirements Pictures	Yes
A.8.27	Secure system architecture and engineering principles	Software Development Plan Process and Deliverables	Yes
A.8.28	Secure coding	Software Development Plan Process and Deliverables; SonarCube Evidence; MendIO Evidence; Amazon Macie Evidence	Yes

Statement of Applicability

Section	Information security control	Evidence/Notes	Applicable
A.8.29	Security testing in development and acceptance	SonarCube Static Code Analysis; MendIO Security Scanning; Pen Test on Grid Web and Grid Mobile App (December 2023); Security Gates Information	Yes
A.8.30	Outsourced development	Contracts with Accionlabs/Convivo	Yes
A.8.31	Separation of development, test and production environments	Software Development Plan Process and Deliverables; Stephan to show AWS test and prod environments in real time	Yes
A.8.32	Change management	Software Development Process; Security Concept; Example of a Pull Request; Software Development Plan Deliverables	Yes
A.8.33	Test information	Anonymized data screenshot; AWS Macie with a planned completion date	Yes
A.8.34	Protection of information systems during audit testing	Anonymized data screenshot; AWS Macie with a planned completion date	Yes