Pulsar Group ISMS

Statement of Applicability v4.0

Classification: PUBLIC

Justification

Applicable - implemented	This control is deemed to be applicable based on risk assessment and the control has been implemented.
Applicable - not implemented	This control is deemed to be applicable but the level of risk has been deemed acceptable by risk assessment and the control has not been implemented.
Not Applicable	This control has been identified as “Not Applicable” and is not relevant to the scope of the ISMS. This has been confirmed through risk assessment.

Applicability	**ID**	**Control / Activity**	**Objective / Deliverable**
Applicable - implemented	A.5.1	Policies for information security	Organizational controls
Applicable - implemented	A.5.2	Information security roles and responsibilities	Organizational controls
Applicable - implemented	A.5.3	Segregation of duties	Organizational controls
Applicable - implemented	A.5.4	Management responsibilities	Organizational controls
Applicable - implemented	A.5.5	Contact with authorities	Organizational controls
Applicable - implemented	A.5.6	Contact with special interest groups	Organizational controls
Applicable - implemented	A.5.7	Threat intelligence	Organizational controls
Applicable - implemented	A.5.8	Information security in project management	Organizational controls
Applicable - implemented	A.5.9	Inventory of information and other associated assets	Organizational controls
Applicable - implemented	A.5.10	Acceptable use of information and other associated assets	Organizational controls
Applicable - implemented	A.5.11	Return of assets	Organizational controls
Applicable - implemented	A.5.12	Classification of information	Organizational controls
Applicable - implemented	A.5.13	Labelling of information	Organizational controls
Applicable - implemented	A.5.14	Information transfer	Organizational controls
Applicable - implemented	A.5.15	Access control	Organizational controls
Applicable - implemented	A.5.16	Identity management	Organizational controls
Applicable - implemented	A.5.17	Authentication information	Organizational controls
Applicable - implemented	A.5.18	Access rights	Organizational controls

Applicable - implemented	A.5.19	Information security in supplier relationships	Organizational controls
Applicable - implemented	A.5.20	Addressing information security within supplier agreements	Organizational controls
Applicable - implemented	A.5.21	Managing information security in the ICT supply chain	Organizational controls
Applicable - implemented	A.5.22	Monitoring, review and change management of supplier services	Organizational controls
Applicable - implemented	A.5.23	Information security for use of cloud services	Organizational controls
Applicable - implemented	A.5.24	Information security incident management planning and preparation	Organizational controls
Applicable - implemented	A.5.25	Assessment and decision on information security events	Organizational controls
Applicable - implemented	A.5.26	Response to information security incidents	Organizational controls
Applicable - implemented	A.5.27	Learning from information security incidents	Organizational controls
Applicable - implemented	A.5.28	Collection of evidence	Organizational controls
Applicable - implemented	A.5.29	Information security during disruption	Organizational controls
Applicable - implemented	A.5.30	ICT readiness for business continuity	Organizational controls
Applicable - implemented	A.5.31	Legal, statutory, regulatory and contractual requirements	Organizational controls
Applicable - implemented	A.5.32	Intellectual property rights	Organizational controls
Applicable - implemented	A.5.33	Protection of records	Organizational controls
Applicable - implemented	A.5.34	Privacy and protection of PII	Organizational controls
Applicable - implemented	A.5.35	Independent review of information security	Organizational controls
Applicable - implemented	A.5.36	Compliance with policies, rules and standards for information security	Organizational controls
Applicable - implemented	A.5.37	Documented operating procedures	Organizational controls
Applicable - implemented	A.6.1	Screening	People controls
Applicable - implemented	A.6.2	Terms and conditions of employment	People controls
Applicable - implemented	A.6.3	Information security awareness, education and training	People controls
Applicable - implemented	A.6.4	Disciplinary process	People controls
Applicable - implemented	A.6.5	Responsibilities after termination or change of employment	People controls
Applicable - implemented	A.6.6	Confidentiality or non-disclosure agreements	People controls
Applicable - implemented	A.6.7	Remote working	People controls
Applicable - implemented	A.6.8	Information security event reporting	People controls
Applicable - implemented	A.7.1	Physical security perimeter	Physical controls
Applicable - implemented	A.7.2	Physical entry	Physical controls
Applicable - implemented	A.7.3	Securing offices, rooms and facilities	Physical controls
Applicable - implemented	A.7.4	Physical security monitoring	Physical controls
Applicable - implemented	A.7.5	Protecting against physical and environmental threats	Physical controls

Not Applicable	A.7.6	Working in secure areas	Physical controls
Applicable - implemented	A.7.7	Clear desk and clear screen	Physical controls
Applicable - implemented	A.7.8	Equipment siting and protection	Physical controls
Applicable - implemented	A.7.9	Security of assets off-premises	Physical controls
Applicable - implemented	A.7.10	Storage media	Physical controls
Applicable - implemented	A.7.11	Supporting utilities	Physical controls
Applicable - implemented	A.7.12	Cabling security	Physical controls
Applicable - implemented	A.7.13	Equipment maintenance	Physical controls
Applicable - implemented	A.7.14	Secure disposal or re-use of equipment	Physical controls
Applicable - implemented	A.8.1	User endpoint devices	Technological controls
Applicable - implemented	A.8.2	Privileged access rights	Technological controls
Applicable - implemented	A.8.3	Information access restriction	Technological controls
Applicable - implemented	A.8.4	Access to source code	Technological controls
Applicable - implemented	A.8.5	Secure authentication	Technological controls
Applicable - implemented	A.8.6	Capacity management	Technological controls
Applicable - implemented	A.8.7	Protection against malware	Technological controls
Applicable - implemented	A.8.8	Management of technical vulnerabilities	Technological controls
Applicable - implemented	A.8.9	Configuration management	Technological controls
Applicable - implemented	A.8.10	Information deletion	Technological controls
Applicable - implemented	A.8.11	Data masking	Technological controls
Applicable - implemented	A.8.12	Data leakage prevention	Technological controls
Applicable - implemented	A.8.13	Information backup	Technological controls
Applicable - implemented	A.8.14	Redundancy of information processing facilities	Technological controls
Applicable - implemented	A.8.15	Logging	Technological controls
Applicable - implemented	A.8.16	Monitoring activities	Technological controls
Applicable - implemented	A.8.17	Clock synchronization	Technological controls
Applicable - implemented	A.8.18	Use of privileged utility programs	Technological controls
Applicable - implemented	A.8.19	Installation of software on operational systems	Technological controls
Applicable - implemented	A.8.20	Networks security	Technological controls
Applicable - implemented	A.8.21	Security of network services	Technological controls
Applicable - implemented	A.8.22	Segregation in networks	Technological controls
Applicable - implemented	A.8.23	Web filtering	Technological controls
Applicable - implemented	A.8.24	Use of cryptography	Technological controls

Applicable - implemented	A.8.25	Secure development life cycle	Technological controls
Applicable - implemented	A.8.26	Application security requirements	Technological controls
Applicable - implemented	A.8.27	Secure system architecture and engineering principles	Technological controls
Applicable - implemented	A.8.28	Secure coding	Technological controls
Applicable - implemented	A.8.29	Security testing in development and acceptance	Technological controls
Applicable - implemented	A.8.30	Outsourced development	Technological controls
Applicable - implemented	A.8.31	Separation of development, test and production environments	Technological controls
Applicable - implemented	A.8.32	Change management	Technological controls
Applicable - implemented	A.8.33	Test information	Technological controls
Applicable - implemented	A.8.34	Protection of information systems during audit testing	Technological controls