

ISO 22342:2023-04 (E)

Security and resilience - Protective security - Guidelines for the development of a security plan for an organization

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Security planning	1
5	Components of the security plan	2
5.1	General	2
5.2	Governance	2
5.2.1	General	2
5.2.2	Security objectives	2
5.2.3	Scope of the security plan	3
5.2.4	Leadership	3
5.2.5	Legal and regulatory	3
5.2.6	Roles, accountabilities and responsibilities	4
5.2.7	Communication	4
5.2.8	Documented information	4
5.2.9	Reporting	4
5.2.10	Evaluation	4
5.2.11	Continuous improvement	5
5.3	Management of risk	5
5.3.1	General	5
5.3.2	Security risk scope, context and criteria	6
5.3.3	Assessment	6
5.3.4	Treatment	6
5.3.5	Acceptance level for residual security risk	6
5.3.6	Communication and consultation	7
5.3.7	Monitoring and review	7
5.3.8	Documentation management and recording	7
5.4	Security controls	7
5.4.1	General	7
5.4.2	Levels of protection	7
5.4.3	Procedures for security controls	8
5.4.4	Operational level controls and treatments	8
5.4.5	Contingency planning for low likelihood and unforeseen situations	9
5.4.6	Timelines for security activities	9
5.5	Security controls process	9
5.5.1	General	9
5.5.2	Selection	9
5.5.3	Implementation, testing and evaluation	9
5.5.4	Monitoring activities	10
5.5.5	Determining effectiveness	10
Bibliography		11