

ISO/IEC TR 27563:2023-05 (E)

Security and privacy in artificial intelligence use cases - Best practices

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	2
5	Analysis of security and privacy	3
5.1	General	3
5.2	Application domains in ISO/IEC TR 24030:2021 use cases	3
5.3	Security in ISO/IEC TR 24030:2021 use cases	3
5.4	Privacy in ISO/IEC TR 24030:2021 use cases	4
6	Templates for analysis	5
7	Supporting information	6
7.1	Describe ecosystem	6
7.2	Provide assessment of systems of interest	7
7.3	Identify security and privacy concerns	7
7.4	Identify security and privacy risks	9
7.5	Identify security and privacy controls	11
7.6	Identify security and privacy assurance concerns	15
7.7	Identify security and privacy plan requirements	16
Annex A (informative) Additional use cases		18
Bibliography		28