

ISO/IEC TR 27550:2019 (E)

Information technology — Security techniques — Privacy engineering for system life cycle processes

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Abbreviated terms
5	Privacy engineering
5.1	General
5.2	Relationship with system and software engineering
5.3	Relationship with security engineering
5.4	Relationship with risk management
6	Integration of privacy engineering in ISO/IEC/IEEE 15288
6.1	General
6.2	Acquisition and supply processes
6.3	Human resources management process
6.4	Knowledge management process
6.5	Risk management process
6.6	Stakeholder needs and requirements definition process
6.7	System requirements definition process
6.8	Architecture definition process
6.9	Design definition process
Annex A	(informative) Additional guidance for privacy engineering objectives
A.1	NIST Privacy engineering objectives
A.1.1	General
A.1.2	Predictability
A.1.3	Manageability
A.1.4	Disassociability
A.2	ULD Privacy protection goals
A.2.1	General
A.2.2	Unlinkability
A.2.3	Transparency
A.2.4	Intervenability
A.2.5	Confidentiality
A.2.6	Integrity
A.2.7	Availability
Annex B	(informative) Additional guidance for privacy engineering practice
B.1	Applicability to domains and ecosystems
B.2	Applicability to software environments
B.2.1	Agile programming
B.2.2	Support for small organizations
Annex C	(informative) Catalogues
C.1	General
C.2	PII processing risks

- C.3 Privacy threats**
- C.4 Risks to individuals**
- C.5 Examples of privacy controls**
- C.6 Privacy management services**
- C.7 Mitigation strategies and privacy measures**

Annex D (informative) Examples of risk models and methodologies

- D.1 General**
- D.2 NIST privacy risk analysis**
- D.3 CNIL privacy risk analysis**

Page count: 52