

# ISO 18960:2025-08 (E)

## Security controls and implementation for third party payment service providers - Guidance and requirements

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms .....	2
5	Security governance controls .....	3
5.1	Service security policies .....	3
5.1.1	Establishment of information security policy .....	3
5.1.2	PII protection policy .....	3
5.1.3	User permission .....	4
5.1.4	User complaint handling policy .....	4
5.2	Roles and responsibilities .....	4
5.2.1	TPPSP security management organization .....	4
5.2.2	Guide for users about security considerations .....	5
5.3	Risk management .....	5
5.3.1	Establishing risk management process .....	5
5.3.2	Performing risk assessment and treatment .....	5
5.4	Documentation .....	6
5.4.1	Documented information .....	6
5.4.2	Management of documented information .....	6
5.5	Monitoring, review and improvement .....	6
5.5.1	Preservation of logs on incident responses and monitoring .....	6
5.5.2	Regular security review .....	7
5.5.3	Continual improvement .....	7
6	Cross-functional controls .....	7
6.1	Asset management .....	7
6.2	Access management .....	8
6.2.1	Access management of administrators .....	8
6.2.2	Access management of administrator programs .....	8
6.2.3	Designation and access management of terminals .....	8
6.3	Supplier security .....	9
6.3.1	Selection and management of suppliers .....	9
6.3.2	Identification and management of the use of cloud services .....	9
6.4	Data security .....	10
6.5	TPP service continuity .....	10
7	Function specific controls .....	11
7.1	Vulnerability management .....	11
7.1.1	Preparation of incident response procedures .....	11
7.1.2	Education and training for incident response .....	11
7.1.3	Documentation of vulnerability management policy .....	12
7.2	Human security .....	12
7.2.1	Establishment and implementation of information security education plans .....	12

7.2.2	Completion of information security education .....	12
7.2.3	Confidentiality and non-disclosure agreement .....	12
7.2.4	Segregation of duties .....	13
7.2.5	Removal or adjustment of access rights at termination and change of employment .....	13
7.3	Physical security .....	13
7.3.1	Designation of secure area and entry control .....	13
7.3.2	Management of check-in and check-out of secure area .....	14
7.3.3	Management of working environment security .....	14
7.4	Server security .....	15
7.4.1	Prevention of malware infection and information leakage .....	15
7.4.2	Removal of unnecessary functions .....	15
7.4.3	Important service operation on dedicated server .....	16
7.4.4	Public web server security .....	16
7.4.5	Security patch management .....	16
7.4.6	Data sanitization .....	17
7.5	Network security .....	17
7.5.1	Control on remote management through Internet .....	17
7.5.2	Demilitarized zone configuration .....	17
7.5.3	Use of private IP and network segregation .....	17
7.5.4	Wireless network security .....	18
7.5.5	Application of secure communication when communicating with external organizations .	18
7.6	TPP application security .....	19
7.6.1	Identification of security requirements during design stage .....	19
7.6.2	Web application security .....	19
7.6.3	Mobile application security .....	21
Annex A (informative) Relation between ISO 18960 and ISO 23195 .....		22
Bibliography .....		24