ETDA Recommendation on ICT Standard

for Electronic Transactions

ETDA Rec 35-2567

ELECTRONIC MESSAGE GENERATION, DELIVERY OR STORAGE SERVICE

Version 1.1

Electronic Transactions Development Agency

Ministry of Digital Economy and Society

ICS 35.030

ETDA Recommendation on ICT Standard for Electronic Transactions

ELECTRONIC MESSAGE GENERATION, DELIVERY OR STORAGE SERVICE

ETDA Rec. 35-2567

Electronic Transactions Development Agency

The Government Complex Commemorating His Majesty the King's 80th Birthday Anniversary, (Building B) 6th Floor, 120 Moo 3 Chaengwattana Road, Thungsonghong, Lak Si District, Bangkok 10210

Tel: +66 0 2123 1234 Fax: +66 0 2123 1200

This ETDA Recommendation on ICT Standards dealing with electronic message generation delivery or storage services is intended to provide an overview of electronic message generation delivery or storage services, electronic message generation or delivery services requirements, and information security requirements. It serves as a guideline for service providers, providing secure electronic message generation delivery or storage services and for helping build confidence among those who use electronic message generation delivery or storage services to send and receive data that their data is protected against the risk of loss, theft, or any unauthorized alteration.

There will be a general presentation and public hearing, as well as consideration of information, observations and opinions from experts and related agencies to improve this Recommendation to make it more complete and thorough, as well as effectively applicable in practice.

This ETDA Recommendation on ICT Standards dealing with electronic message generation delivery or storage services was prepared by the Electronic Transactions Development Agency

Electronic Transactions Development Agency (Public Organization)
The Ninth Tower Grand Rama 9 (Building B), 21st floor, 33/4 Rama IX Rd,
Huai Khwang Subdistrict, Huai Khwang District, Bangkok 10310
Tel: 0 2123 1234 Fax: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

Foreword

In the present, electronic transactions play an important role in conducting business in the modern economy. Consequently, entrepreneurs shall develop an information technology infrastructure to make electronic transactions convenient, fast, and efficient. However, due to the time needed and high cost of development, many entrepreneurs aim to reduce the time and cost of developing an information technology infrastructure, and so turn to the services of service providers who provide electronic message generation delivery or storage services between entrepreneurs and government agencies or with other entrepreneurs. These service providers therefore play an important role in supporting electronic transactions that allow for networking connections, the shared use of resources, and the processing and distribution of data among various agencies, making it necessary to safeguard the integrity, availability and reliability of electronic information and data security.

For this reason, the Electronic Transactions Development Agency has prepared this ETDA Recommendation on ICT Standard for Electronic Transactions on Electronic Message Generation Delivery or Storage Service to provide an overview of electronic message generation delivery or storage services , electronic message generation or delivery services requirements, and information security requirements. It serves as a guideline for service providers, providing secure electronic message generation delivery or storage services and for helping build confidence among those who use electronic message generation delivery or storage services. This Recommendation can be used with electronic message generation delivery or storage services to the Revenue Department, electronic message generation delivery or storage services among agencies connected to the National Single Window (NSW) system or other electronic message generation delivery or storage services that require reliability in sending or receiving data message.

Table of Contents

Table of Figures

Table Index

ETDA Recommendation on ICT Standard for Electronic Transactions

Electronic Delivery Service

1. Scope

This Recommendation provides an overview of electronic message generation delivery or storage services, electronic message generation or delivery services requirements, and information security requirements. It serves as a guideline for service providers, in providing secure electronic message generation delivery or storage services and for helping build confidence among those who use electronic message generation delivery or storage services to send and receive data that their data is protected against the risk of loss, theft, or any unauthorized alteration.

This Recommendation can be used with electronic message generation delivery or storage service providers such as:

- Electronic message generation delivery or storage service providers to the Revenue Department.
- Electronic message generation delivery or storage service providers among agencies linked to the National Single Window (NSW) system.
- Other electronic message generation delivery or storage service providers who want reliability in electronic delivery.

However, according to this Recommendation, electronic message generation delivery or storage services have not specifically identified the use of any one method, such as an electronic message delivery model, a messaging protocol, a message format, or evidence format for sending and receiving messages. Therefore, each electronic message generation delivery or storage service providers can use different methods in accordance with the criteria set forth by regulatory authorities or agencies related to electronic message generation delivery or storage services.

2. Definitions

The meaning of the terms used in this Recommendation is as follows.

2.1 “Electronic message generation delivery or storage service” means a service that enables a sender and a recipient to send and receive data through electronic means, helps record evidence of the transmission of data, and protects data against the risk of loss, theft, or any unauthorized alteration.

2.2 “Service provider” means an agency which provides an electronic message generation delivery or storage service.

2.3 “Original sender” means the individual who sends data message before it is retained for delivery by the method prescribed by that person. Original sender may send the data message by herself or himself, or have the data message sent in her/his name or on her/his behalf. This definition does not include individuals who are service providers.

2.4 “Final recipient” means the individual to whom the sender wishes to send data message and who receives this data message. This definition does not include individuals who are service providers.

3. Overview of Electronic Message Generation Delivery or Storage Services

An electronic message generation delivery or storage service is the transmission of data between the original sender and the final recipient through an electronic message generation delivery or storage service provider, where the service provider has the responsibility to provide evidence that the data was sent and received in order to confirm the events that occurred in transmission (for example, evidence that the service provider received the original data from the sender and evidence that confirms that the service provider sent the data to the recipient). This is similar to the registered mail service used for sending paper documents which are important evidence. Evidence of the transmission and receipt of the data can be used to prove that the data delivery transaction took place between the sender and the recipient of the relevant data and occurred at the time shown in the evidence.

The details of electronic message generation delivery or storage services are as follows.

3.1 Electronic message generation services

Service providers or original senders generate electronic messages in accordance with the criteria set forth by regulatory authorities or relevant agencies. The electronic messages will include a mechanism that allows the final recipient to verify any modifications to the electronic messages.

3.2 Electronic delivery services

Electronic delivery services may have different message delivery models, but this does not include cases where the original sender sends the data directly to the final recipient, such as sending data from the server of the original sender to the server of the final recipient.

The general model of electronic delivery can be described in detail as follows.

3.2.1 3-corner electronic delivery model

The 3-corner electronic delivery model (as shown in Figure 1) is the transmission of data between the original sender and the final recipient through an electronic delivery

service provider by a user agent system of the original sender and the final recipient as an application that interacts directly with individual users (e.g., a web application or a mobile device application) or an enterprise application (e.g., an organizational resource management system) that may or may not involve individual users.

In the user agent system, the original sender takes the responsibility for preparing the original data and sending it to the service provider, and may also support the use of digital signatures in conjunction with the original data or end-to-end encryption between the original sender and the final recipient [1] The original sender or final recipient may themselves be the developer of the system or may use software services from an external agency that is an application service provider.

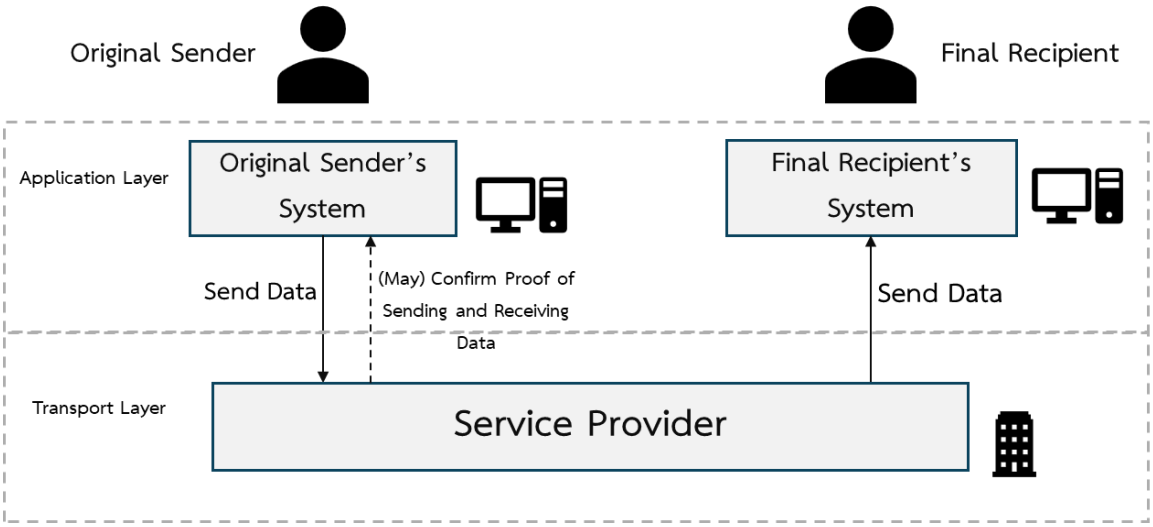

Figure 1 3-corner electronic delivery model

The 3-corner electronic delivery model has the following general steps:

(1) The original sender authenticates to access electronic delivery services.

(2) The original sender or the original sender's system prepares the original data. This may contain a digital signature used to identify and authenticate the original sender.

(3) The original sender's system sends the original data to the service provider.

(4) When the service provider produces evidence to confirm that the service provider has received the original data, the service provider may send this

evidence to the original sender or store that evidence for a period of time for later access by the relevant parties.

(5) The service provider sends the data to the system of the final recipient.

(6) When the service provider produces evidence to confirm that the service provider has sent the original data to the final recipient, the service provider may send that evidence to the original sender or store that evidence for a period of time for later access by the relevant parties.

(7) The final recipient authenticates to access the electronic delivery service.

(8) The final recipient or the final recipient's system accesses the data from the electronic delivery service.

3.2.2 4-corner electronic delivery model

The 4-corner electronic delivery model (as shown in Figure 2) is the transmission of data between the original sender (C1) and the final recipient (C4) through a service provider on the side of the original sender (C2) and a service provider on the side of the final recipient (C3), since the original sender and the final recipient may voluntarily use or be connected to different electronic delivery service providers. The 4-corner model identifies the original sender, the service provider on the side of the original sender, the service provider on the side of the final recipient, and final recipient as C1, C2, C3, and C4, respectively.

In addition, the service provider on the side of the original sender and the service provider on the side of the final recipient will establish agreements necessary in various areas to achieve effective interoperability, such as the reliability of the service systems,

the messaging protocol, the message format, the evidence format, or the fees that may be incurred.

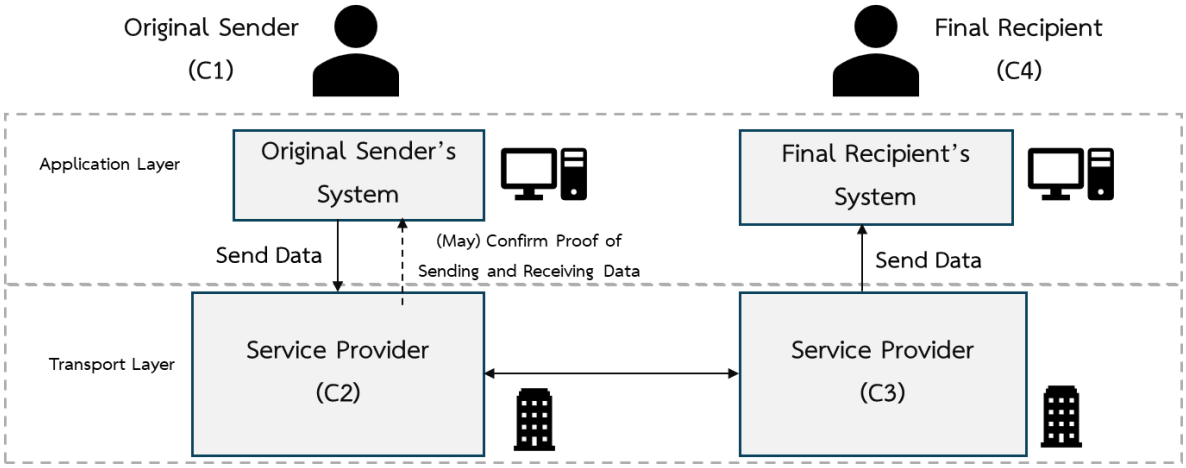

Figure 2 4-corner electronic delivery model

The 4-corner electronic delivery model has the following general steps:

(1) C1 authenticates to access the electronic delivery service.

(2) C1 and C1's system prepare the original data. The original data may contain a digital signature used to identify and authenticate C1.

(3) C1's system sends the original data to C2.

(4) C2 provides evidence to confirm that C2 has received the original data. C2 may send that evidence to C1 or store that evidence for a period of time for later access by the relevant parties.

(5) C2 sends the data to C3 in accordance with the agreement on data transmission.

(6) C3 provides evidence to confirm that C3 has received the original data from C2. C3 may send that evidence to C2 or store that evidence for a period of time for later access by the relevant parties. C2 may then send that evidence to C1.

(7) C3 sends the data to C4.

(8) C3 provides evidence to confirm that C3 has sent the data to C4. C3 may send that evidence to C2 or store that evidence for a period of time for later access by the relevant parties. C2 may then send that evidence to C1.

(9) C4 authenticates to access the electronic delivery service.

(10) C4 and C4's system access the data from electronic delivery service.

In some cases, electronic delivery may have one or more service providers (e.g. C5) between the C2 and C3 service providers, adding to the 4-corner model to make it an

extended model. In such cases, all service providers (e.g. C5) located between C2 and C3 shall comply with the necessary agreements in various areas to achieve effective collaboration, in the same way as C2 and C3.

3.3 Electronic storage services

In cases where electronic storage services are provided, the service provider must ensure the security and integrity of the electronic messages. The information security policy include details on message storage, which must at least cover the following aspects: encryption of electronic data, access control, and classification of information according to the organization's information security standards.

Electronic message generation or delivery services are governed by both the electronic message generation or delivery services requirements under Chapter 4 and the information security requirements under Chapter 5. However, for electronic storage services, there are no specific operational requirements; therefore, the information security requirements under Chapter 5 are applied.

4. Electronic Message Generation or Delivery Services Requirements

There are 6 requirements for the electronic message generation or delivery services as follows:

(1) Use of a protected communication channel to ensure the integrity and confidentiality of data during delivery.
(2) Message encryption so that only the final recipient can access the data.
(3) Identification of the original sender (sender identification) to verify information about the identity of the original sender.
(4) Identification of the final recipient (recipient identification) to verify information about the identity of the final recipient before data delivery.
(5) Time reference to specify the date and time when the data is sent and is received.
(6) Evidence of sending and receiving to provide the original sender and final recipient with evidence of sending and receiving the data.

The details of the requirements of electronic message generation or delivery services are given in in Table 1, which is based on the 4-corner electronic delivery model. In the case of the 3-corner electronic delivery model, the service provider shall comply with both the requirements of C2 and C3

Table 1 Requirements of Electronic Message Generation or Delivery Services

Requirements of Electronic Message Generation or Delivery Services	Original Sender (C1)	Service Provider on the side of the Original Sender (C2)	Service Provider on the side of the Final Recipient (C3)	Final Recipient (C4)
4.1 Use of a Protected Communication Channel				
(1) C1, C2, C3 and, C4 shall use secure communication channels using Transport Layer Security (TLS) criteria such as TLS 1.2 or higher versions, which help maintain the complete accuracy and confidentiality of the data through symmetric-key encryption in electronic delivery. In the case of an extended electronic delivery model, all service providers (e.g. C5) shall use the same secure communication channels. Note: The criteria of the use of Secure Sockets Layers (SSL) and Transport Layer Security (TLS) in versions lower than TLS 1.2 have been declared revoked for reasons of security as follows: – SSL 2.0 was declared revoked by RFC 6176 [2] – SSL 3.0 was declared revoked by RFC 7568 [3] – TLS 1.0 and TLS 1.1 were declared revoked by RFC 8996 [4]	✓	✓	✓	✓

Requirements of Electronic Message Generation or Delivery Services	Original Sender (C1)	Service Provider on the side of the Original Sender (C2)	Service Provider on the side of the Final Recipient (C3)	Final Recipient (C4)
4.2 Message Encryption				
(1) If the data to be sent is sensitive data or C1 intends that only C4 can access it, C1 can operate end-to-end encryption with C4's public key. (2) C1 or C2 shall generate electronic messages in accordance with the criteria set forth by regulatory authorities or relevant agencies for electronic message generation or delivery services. The electronic messages shall include a mechanism that allows the final recipient (C4) to verify any modifications to the electronic messages.	✓	✓		

Requirements of Electronic Message Generation or Delivery Services	Original Sender (C1)	Service Provider on the side of the Original Sender (C2)	Service Provider on the side of the Final Recipient (C3)	Final Recipient (C4)
4.3 Original Sender Identification				
(1) C2 shall authenticate the identity of C1 which can be done through TLS in any of the following ways. (1.1) In the case of one-way TLS, C2 authenticates C1 by using something that identifies C1 such as a user account or password. (1.2) In the case of two-way TLS, C2 authenticates C1 by checking C1's client certificate, which is a form of mutual authentication. In both cases, C1 can authenticates C2 by checking C2's server certificate. (2) If C1 includes a digital signature in the original information, C2 can authenticates C1 by checking C1's client certificate so that C2 and C3 (and all other service providers, if any, such as C5) do not need a digital signature included in the data. However, C2 can include a signature in the original information instead of C1 to maintain message integrity for C1 if this is agreed between C1 and C2.		✓		

4.4 Final Recipient Identification				
(1) C3 shall authenticates C4 before allowing C4 to receive the data, which can be done through one of these TLS protocols: (1.1) In the case of a one-way TLS, C3 authenticates C4 by using something that identifies C4 such as a user account and password for identity verification. (1.2) In the case of a two-way TLS, C3 authenticates C4 by checking C4's client certificate, which is mutual authentication. In both cases, C4 can authenticates C3 by checking C3's server certificate.			✓	
4.5 Time Reference				
(1) C2 and C3 (including all service providers, if applicable, such as C5) shall use reliable date and time references in the preparation of evidence of sending and receiving data to confirm the events that occur at the time shown in the evidence. The date and time can be referenced from the internal system (system clock) or from the time-stamping service of a time-stamping authority. [1]		✓	✓	

[1] Details of time-stamping services are in accordance with the ETDA Recommendation on ICT Standard for Electronic Transactions on Electronic Time-Stamping ETDA Rec. No. 33.

4.6 Evidence of Sending and Receiving Data				
(1) C2 and C3 (together with all other service providers, if any, such as C5) shall store evidence of at least as follows: — Data identifying or confirming the identity of the relevant users. — Evidence that shows that data about the identity of the original sender has been verified. — Evidence that shows that data about the identity of the final recipient has been verified. — Evidence that shows that the original data was not altered during transmission, such as a message digest of the original data. — A log of events that occurred during the transmission of data (for example the event[2] of a service provider having received the original data, of a service provider having received the data from the previous service provider, and of a service provider having sent the data to the final recipient). (2) C2 and C3 (together with all other service providers, if any, such as C5) shall store evidence for a specified period of time so that relevant parties can access it, and may send evidence of events that occurred during data transmission to those involved.		✓	✓	

[2] Examples of events that occur during data delivery can refer to ETSI EN 319 522-1 item 6, ERDS events and evidence set. [1]

5. Information Security Requirements

The information security requirements of electronic message generation delivery or storage services include information security risk management and information security controls

5.1 Information Security Risk Management

(1) Service providers shall conduct an information security risk assessment of their electronic delivery service as follows:

- Establish and maintain risk criteria, which include risk acceptance criteria and risk assessment criteria.
- Identify information security risks, namely the use of information security risk assessment processes to identify risks related to confidentiality, integrity, and availability of information within the scope of electronic message generation delivery or storage services, including identification of risk owners.
- Analyze information security risks by assessing the impact and opportunities that may arise from the risk, including determining the level of risk.
- Evaluate the results of the risk analysis against risk criteria and prioritize risks for treatment

(2) A service provider shall implement an information security risk treatment plan and shall retain documented information showing risk management outcomes.

(3) A service provider shall regularly review the information security risk assessment and management of electronic message generation delivery or storage services.

5.2 Information Security Controls

Information security controls of electronic message generation delivery or storage services refer to controls and guidance from ISO/IEC 27002:2022 [5] which consists of 93 controls that divided into 4 areas as follows:

(1) Organizational controls
(2) Personnel controls
(3) Physical controls
(4) Technological controls

However, this Recommendation applies all controls of ISO/IEC 27002:2022 to analyze the context and issues related to electronic message generation delivery or storage services, and prioritizes controls according to the level of need. as follows:

(1) Mandatory controls 50 controls
(2) Optional controls 33 controls

(3) Conditional controls 10 controls

To be in compliance with this Recommendation, a service provider shall implement all mandatory controls and implement the conditional controls if the service provider's system meets the conditions specified such as in the case that an external agency is given the responsibility to act on its behalf, in the case of using cloud services, or in the case where the agency is itself the developer of the system.

In addition, service providers can consider implementing additional optional controls to comply with information security risk assessments and the criteria of the regulatory body for each type of electronic delivery service.

5.2.1 Organizational controls

No.	Control	Necessity	Guidance
1	**Policies for information security** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.1
2	**Information security roles and responsibilities** Information security roles and responsibilities shall be defined and allocated according to the organization needs.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.2
3	**Segregation of duties** Conflicting duties and conflicting areas of responsibility shall be segregated.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.3
4	**Management responsibilities** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.4
5	**Contact with authorities** The organization shall establish and maintain contact with relevant authorities.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.5

No.	Control	Necessity	Guidance
6	**Contact with special interest groups** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.6
7	**Threat intelligence** Information relating to information security threats shall be collected and analysed to produce threat intelligence.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.7
8	**Information security in project management** Information security shall be integrated into project management.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.8
9	**Inventory of information and other associated assets** An inventory of information and other associated assets, including owners, shall be developed and maintained.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.9
10	**Acceptable use of information and other associated assets** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.10
11	**Return of assets** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.11
12	**Classification of information** Information shall be classified according to the information security needs of the organization based on confidentiality integrity, availability and relevant interested party requirements.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.12

No.	Control	Necessity	Guidance
13	**Labelling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.13
14	**Information transfer** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.14
15	**Access control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.15
16	**Identity management** The full life cycle of identities shall be managed.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.16
17	**Authentication information** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.17
18	**Access rights** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.18
19	**Information security in supplier relationships** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	conditional (When a supplier provides the service on behalf)	Details are in accordance with ISO/IEC 27002:2022 No. 5.19

No.	Control	Necessity	Guidance
20	**Addressing information security within supplier agreements** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	conditional (When a supplier provides the service on behalf)	Details are in accordance with ISO/IEC 27002:2022 No. 5.20
21	**Managing information security in the ICT supply chain** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT (Information and Communication Technology) products and services supply chain.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.21
22	**Monitoring, review and change management of supplier services** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	conditional (When a supplier provides the service on behalf)	Details are in accordance with ISO/IEC 27002:2022 No. 5.22
23	**Information security for use of cloud services** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	conditional (When using cloud services)	Details are in accordance with ISO/IEC 27002:2022 No. 5.23
24	**Information security incident management planning and preparation** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.24
25	**Assessment and decision on information security events** The organization shall assess information security events and decide if they are to be categorized as information security incidents.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.25
26	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.26

No.	Control	Necessity	Guidance
27	**Learning from information security incidents** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.27
28	**Collection of evidence** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.28
29	**Information security during disruption** The organization shall plan how to maintain information security at an appropriate level during disruption.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.29
30	**ICT readiness for business continuity** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.30
31	**Legal, statutory, regulatory and contractual requirements** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.31
32	**Intellectual property rights** The organization shall implement appropriate procedures to protect intellectual property rights.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.32
33	**Protection of records** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.33

No.	Control	Necessity	Guidance
34	**Privacy and protection of PII (personal identifiable information)** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.34
35	**Independent review of information security** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 5.35
36	**Compliance with policies, rules and standards for information security** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.36
37	**Documented operating procedures** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 5.37

5.2.2 Physical controls

No.	Control	Necessity	Guidance
38	**Physical security perimeters** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.1
39	**Physical entry** Secure areas shall be protected by appropriate entry controls and access points.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.2

No.	Control	Necessity	Guidance
40	**Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and implemented.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.3
41	**Physical security monitoring** Premises shall be continuously monitored for unauthorized physical access.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.4
42	**Protecting against physical and environmental threats** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.5
43	**Working in secure areas** Security measures for working in secure areas shall be designed and implemented.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.6
44	**Clear desk and clear screen** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 7.7
45	**Equipment siting and protection** Equipment shall be sited securely and proted.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 7.8
46	**Security of assets off-premises** Off-site assets shall be protected.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 7.9
47	**Storage media** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.10

No.	Control	Necessity	Guidance
48	**Supporting utilities** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 7.11
49	**Cabling security** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 7.12
50	**Equipment maintenance** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 7.13
51	**Secure disposal or re-use of equipment** Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 7.14

5.2.3 People controls

No.	Control	Necessity	Guidance
52	**Screening** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 6.1
53	**Terms and conditions of employment** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 6.2

No.	Control	Necessity	Guidance
54	**Information security awareness, education and training** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 6.3
55	**Disciplinary process** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 6.4
56	**Responsibilities after termination or change of employment** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 6.5
57	**Confidentiality or non-disclosure agreements** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 6.6
58	**Remote working** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 6.7
59	**Information security event reporting** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 6.8

5.2.4 Technological controls

No.	Control	Necessity	Guidance
60	**User endpoint devices** Information stored on, processed by or accessible via user end point devices shall be protected.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.1
61	**Privileged access rights** The allocation and use of privileged access rights shall be restricted and managed.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.2
62	**Information access restriction** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.3
63	**Access to source code** Read and write access to source code, development tools and software libraries shall be appropriately managed.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.4
64	**Secure authentication** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.5
65	**Capacity management** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.6
66	**Protection against malware** Protection against malware shall be implemented and supported by appropriate user awareness.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.7

No.	Control	Necessity	Guidance
67	**Management of technical vulnerabilities** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.8
68	**Configuration management** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.9
69	**Information deletion** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.10
70	**Data masking** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.11
71	**Data leakage prevention** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.12
72	**Information backup** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.13
73	**Redundancy of information processing facilities** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.14

No.	Control	Necessity	Guidance
74	**Logging** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.15
75	**Monitoring activities** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.16
76	**Clock synchronization** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.17
77	**Use of privileged utility programs** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.18
78	**Installation of software on operational systems** Procedures and measures shall be implemented to securely manage software installation on operational systems.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.19
79	**Networks security** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.20
80	**Security of network services** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.21
81	**Segregation of networks** Groups of information services, users and information systems shall be segregated in the organization's networks.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.22

No.	Control	Necessity	Guidance
82	**Web filtering** Access to external websites shall be managed to reduce exposure to malicious content.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.23
83	**Use of cryptography** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.24
84	**Secure development life cycle** Rules for the secure development of software and systems shall be established and applied.	conditional (When the service provider develops the system itself)	Details are in accordance with ISO/IEC 27002:2022 No. 8.25
85	**Application security requirements** Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.26
86	**Secure system architecture and engineering principles** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	conditional (When the service provider develops the system itself)	Details are in accordance with ISO/IEC 27002:2022 No. 8.27
87	**Secure coding** Secure coding principles shall be applied to software development.	conditional (When the service provider develops the system itself)	Details are in accordance with ISO/IEC 27002:2022 No. 8.28
88	**Security testing in development and acceptance** Security testing processes shall be defined and implemented in the development life cycle.	conditional (When the service provider develops the system itself)	Details are in accordance with ISO/IEC 27002:2022 No. 8.29
89	**Outsourced development** The organization shall direct, monitor and review the activities related to outsourced system development.	conditional (When the service provider develops the system itself)	Details are in accordance with ISO/IEC 27002:2022 No. 8.30

No.	Control	Necessity	Guidance
90	**Separation of development, test and production environments** Development, testing and production environments shall be separated and secured.	conditional (When the service provider develops the system itself)	Details are in accordance with ISO/IEC 27002:2022 No. 8.31
91	**Change management** Changes to information processing facilities and information systems shall be subject to change management procedures.	mandatory	Details are in accordance with ISO/IEC 27002:2022 No. 8.32
92	**Test information** Test information shall be appropriately selected, protected and managed.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.33
93	**Protection of information systems during audit testing** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	optional	Details are in accordance with ISO/IEC 27002:2022 No. 8.34

References

[1] European Telecommunications Standards Institute, "ETSI EN 319 522-1 V1.1.1 – Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture", September 2018.

[2] Internet Engineering Task Force, "RFC 6176: Prohibiting Secure Sockets Layer (SSL) Version 2.0", March 2011. Available: https://www.rfc-editor.org/rfc/rfc6176.

[3] Internet Engineering Task Force, "RFC 7568: Deprecating Secure Sockets Layer Version 3.0", June 2015. Available: https://www.rfc-editor.org/rfc/rfc7568.

[4] Internet Engineering Task Force, "RFC 8996: Deprecating TLS 1.0 and TLS 1.1", March 2021. Available: https://datatracker.ietf.org/doc/html/rfc8996.

[5] International Organization for Standardization, “ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls”, March 2022.

[6] European Telecommunications Standards Institute, "ETSI EN 319 521 V1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers", February 2019.

[7] European Commission, "eDelivery Building Block, Security Controls, Linking eIDAS (Q)ERDS & eDelivery", Version 1.20, April 2022.

[8] Electronic Transactions Act, B.E. 2544 (2001) and its amendments.