mitsoft

Qualified Trust Service Provider

Qualified Trust Services Practice Statement

QTSP/PS

Version 1.20

Valid since 2026-09-01

UAB „MIT-SOFT“, Kalvarijų st. 276-100, LT-08316 Vilnius, Tel. +370 5 233 3922, www.mitsoft.lt, info@mitsoft.lt, Company ID 120792080, VAT payer code LT207920811

Approvals

Revision history

Version	Valid since	Description
1.00	2024-10-01	First official version of the document
1.20	2026-09-01	Updated according to new requirements

Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2026-07-20	
Approved by	Antanas Mitašiūnas	2026-07-20	

Table of content

1. INTRODUCTION 4
1.1. Overview 4
1.2. Contact information 4
2. References 5
3. Definitions of terms and abbreviations 6
4. MitSoft QTSP: General Concepts 7
5. Risk assessment 8
6. POLICIES AND PRACTICES 9
6.1. Qualified trust services practice statement 9
6.1.1. QTSP obligations 9
6.2. Terms and conditions 10
6.3. Information security policy 10
7. QTSP MANAGEMENT AND OPERATION 12
7.1. Internal organization 12
7.1.1. Organization reliability 12
7.1.2. Segregation of duties 12
7.2. Human resources 12
7.3. Asset management 14
7.3.1. General 14
7.3.2. Assets inventory and classifications 14
7.3.3. Storage media handling 14
7.4. Access control 14
7.5. Cryptographic controls 15
7.6. Physical and environmental security 15
7.7. Operation security 16
7.8. Network security 17
7.9. Vulnerabilities and Incident management 18
7.10. Collection of evidence 19
7.11. Business continuity management 19
7.12. QTSP termination and termination plans 19
7.13. Compliance 20
7.14. Supply chain 20
7.14.1. Supply chain policy 21
7.14.2. Supply chain procedures and processes 21
7.14.3. Responsibility, third-party agreements and SLA 21

1. INTRODUCTION

The joint stock company "MIT-SOFT" (further – the MitSoft) was established on August 1, 1991 and since 1996 is working in software development and services provision for creation and verification of electronic documents having the same legal effect as hand signed paper documents. Information about the MitSoft is available on the website http://www.mitsoft.lt/.

MitSoft has divided its Practice Statements into three parts:

- Qualified Trust Services Practice Statement (QTS PS) describes general practices common to all qualified trust services;
- Preservation Practice Statement (QLPS PS) and Time-Stamping Practice Statement (QTSS PS) describe parts that are specific to each qualified service.

1.1. Overview

The present Qualified Trust Services Practice Statement (QTS PS) is based upon the following legal acts and normative documents:

a) The Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [eIDAS];

b) ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

Note regarding the definitions. Everything that is said in the document applies solely to the MitSoft QTSP.

The version of the QTS PS in effect is available on the website of MitSoft.

1.2. Contact information

The QTSP is managed by the joint stock company "MIT-SOFT", which contact information is given in the Table 2.

Table 2. Contact information of the QTSP

QTSP:	The joint stock company "MIT-SOFT"
Address:	Kalvarijų str. 276-100, LT-08316 Vilnius
Phone:	+370 5 233 3922
URL:	https://www.mitsoft.lt/
E-mail:	info@mitsoft.lt

2. References

[eIDAS] – Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2025/2530] – Commission implementing Regulation (EU) 2025/2530 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards requirements for qualified trust service providers providing qualified trust services.

[Law on Cybsec] Law on Cybersecurity of the Republic of Lithuania

[Resolution Gov] The Resolution of the Government of the Republic of Lithuania on implementation of the Law on Cybersecurity of the Republic of Lithuania

[EN 319 102-1] – ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[EN 319 401] – ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[ISO 27002] – ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection – Information security management systems - Requirements".

[ISO 27005] – ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection – Guidance on managing security risks".

[RFC 3161] – RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).

[RFC 5816] – RFC 5816 ESSCertIDv2 Update for RFC 3161.

[TS 119 312] – ETSI TS 119 312 "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

3. Definitions of terms and abbreviations

Archival time stamp: ArchiveTimeStamp for XAdES signatures, archive-time-stamp for CAdES signatures, or DocumentTimeStamp for PAdES signatures.

Compromise: a loss, theft, modification, illegal use, or any other security violation of the confidential data.

Data object: actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type.

Metadata: data about other data.

Proof of existence: evidence that proves that an object existed at a specific date/time.

Signer: entity being the creator of a digital signature.

Subscriber: legal or natural person bound by agreement with a qualified trust service provider to any subscriber obligations.

Time stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time (= electronic time stamp [eIDAS]).

Trusted list: list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

Validation data: data that is used to validate a digital signature.

ETSI – European Telecommunications Standards Institute
OID – Object identifier
PS - Practice Statement
QLPS – Qualified Long-term Preservation Service
QTS - Qualified Trust Services
QTSP – Qualified Trust Service Provider
QTSS – Qualified Time-Stamping Service
RRT – Communications Regulatory Authority of the Republic of Lithuania
TSA – Time-stamping authority

4. MitSoft QTSP: General Concepts

MitSoft QTSP provides the following qualified trust services:

- qualified long-term preservation services;
- qualified time-stamping service.

MitSoft QTSP satisfies general policy requirements for trust service providers specified in standard ETSI EN 319 401.

5. Risk assessment

The QTSP carries out a risk assessment to identify, analyse, and evaluate threats to the business assets taking into account business and technical issues. Based on the risk assessment results, the appropriate risk treatment measures are selected, which ensure that the level of security is commensurate to the degree of risk.

The QTSP determines all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the practice statements (QTS PS, QLPS PS, QTSS PS).

The risk assessment is approved and the residual risks are accepted by the director of the MitSoft.

QTSP regularly (at least once per year) review and revise the risk assessment.

6. POLICIES AND PRACTICES

6.1. Qualified trust services practice statement

The QTSP ensures that it demonstrates the reliability necessary for providing qualified trust services. In particular:

a) According to agreement DELSKA data centre is the host of MitSoft QTSP qualified trust services. DELSKA is ISO 27000 certified and TIER3 Facility certified data centre.

   DELSKA data centre provides dedicated server service for remote backup of MitSoft QTSP data under conditions defined in agreement.

b) The Practice statements and other relevant documentation, as necessary to assess conformance to the qualified trust services policies, are available to subscribers and relying parties on the website of MitSoft and provided upon request.

c) The director of the MitSoft has overall responsibility for the QTSP with final authority for approving the Practice statements.

d) The director of the MitSoft ensures the implementation of the practices by communicating them to the personnel as appropriate.

e) The MitSoft QTSP has Practices review process, including maintaining the Practice statements.

f) The QTSP gives a due notice of changes it intends to make in its Practice statements and, following approval as in (c) above, makes the revised Practice statements immediately available as required under (b) above.

g) The provisions made for termination of service are stated in the section 7.12 QTSP termination and termination plans.

6.1.1. QTSP obligations

6.1.1.1. QTSP obligations towards subscribers

The QTSP meets its claims as given in its published terms and conditions.

6.1.1.2. Liability

QTSP liability and obligations are defined in the Subscriber agreements for provision of service in effect.

6.1.1.3. Legal provisions and interpretations

6.1.1.3.1. The main legal acts

Provision of qualified trust services, requirements for the providers, and liability is regulated by:

a) The Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

b) The Law on electronic identification and trust services for electronic transactions of the Republic of Lithuania issued on April 26, 2018.

c) The Law on Cybersecurity of the Republic of Lithuania issued on December 11, 2014.

d) The Resolution of the Government of the Republic of Lithuania on implementation of the Law on Cybersecurity of the Republic of Lithuania No. 818 of 13 August 2018.

e) Council of the Communications Regulatory Authority of the Republic of Lithuania, Resolution No. TN-276, On the Approval of the Description of the Procedure for Granting the Status of a Qualified Trust Service Provider and the Performance of Certain Operational Requirements (June 23, 2026).

6.1.1.3.2. Dispute settlement

Any disputes between the QTSP and its end-users are resolved by positive-minded negotiations. In a case of failing to settle the dispute, it is addressed to the institutions of law enforcement.

6.1.1.4. Charges

QTSP may set the prices for its qualified trust services.

6.1.1.5. Intellectual property rights

When citing any documentation of the QTSP, it is required to provide a reference to its source.

6.2. Terms and conditions

The QTSP discloses to all subscribers and potential relying parties the terms and conditions regarding the provision of its qualified trust service.

These terms and conditions specify the following:

a) Any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations.
b) The subscriber's obligations, if any.
c) The period of time during which QTSP event logs are retained.
d) Limitations of liability.
e) The applicable legal system.
f) Procedures for settlement of complaints and disputes.
g) The QTSP contact information.
h) Any undertaking regarding availability.

This information is available on the website of MitSoft in a readily understandable language, and may be complemented by the Subscriber agreements between the QTSP and the subscribers.

6.3. Information security policy

The QTSP has an information security policy which is approved by the director of the MitSoft and which sets out the organization's approach to managing its information security.

The QTSP ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practice. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the QTSP's assets.

The QTSP retains responsibility for all aspects of the provision of qualified trust services within the scope of the QTSP, whether or not functions are outsourced to subcontractors. The MitSoft QTSP retains responsibility for the disclosure of relevant practices of all the parties participating in the provision of qualified trust services.

The responsibility for defining the guidelines for information security, continuous maintaining of infrastructure, documentation, management, and implementation of security measures and operational procedures for the QTSP equipment, premises, systems and information assets as well as protection of information and other assets is

undertaken by the director of the MitSoft. The QTSP ensures the communication of security guidelines and rules to all related personnel who need them in their work.

Security measures and operational procedures for the equipment, premises, systems, and information assets required for provision of qualified trust services are documented, managed, and followed.

The QTSP establishes procedures to notify of important changes in the provision of the trust service to the appropriate parties in accordance with business requirements and relevant laws and regulations, including changes in the provision of trust services and the intention to cease on its provision.

Information security infrastructure necessary for ensuring security is maintained permanently. Any changes affecting security are approved by the director of the MitSoft.

7. QTSP MANAGEMENT AND OPERATION

The QTSP follows all the practices indicated in the following clauses.

The provision of a qualified trust service in response to a request is at the discretion of the QTSP depending on the agreements with the subscriber.

7.1. Internal organization

7.1.1. Organization reliability

The QTSP ensures that its organization is reliable. In particular:

a) The QTSP is a legal entity according to the law of the Republic of Lithuania, registered in the Register of Legal Entities as UAB "MIT-SOFT"; entity's code is 120792080.

b) The QTSP has a system for quality and information security management appropriate for the trust services it is providing.

c) It employs a sufficient number of personnel having the education, training, technical knowledge, and experience adequate to provision of the qualified trust services.

d) Policies and practices under which the QTSP operates are based on international standards and are non-discriminatory.

e) QTSP's services are accessible to all applicants whose activities fall within its declared field of operation, and that agree to abide by their obligations as specified by the QTSP.

f) The QTSP has adequate arrangements and resources, in accordance with the Regulation (EU) No 910/2014 and national law, to cover liabilities arising from its operations and activities.

g) The QTSP has the financial stability and resources required to operate in conformity with the Practices statements, including the requirements for QTSP termination.

h) The policies and procedures for the resolution of complaints and disputes about the provisioning of the qualified trust services or any other related matters are specified as defined in the Terms and conditions.

i) The QTSP has a documented agreement and contractual relationship in place where the provisioning of service involves third parties.

7.1.2. Segregation of duties

Conflicting duties and areas of responsibility are segregated as defined in the QTSP's information security policy (see the section 6.3. Information security policy) to reduce opportunities for unauthorized or unintentional modification or misuse of the QTSP assets.

7.2. Human resources

The QTSP ensures that all personnel and contractors apply information security in accordance with the established information security policy, topic-specific policies and procedures of the QTSP.

The QTSP ensures that personnel and hiring practices enhance and support the trustworthiness of the QTSP's operations. In particular:

a) The QTSP employs personnel fulfilling the requirement of "expert knowledge, experience and qualifications" appropriate to the job functions through formal training and credentials, or actual experience, or a combination of the two.

b) Personnel's compliance with qualification requirements includes regular updates (at least every 12 months) on new threats and current security practices.

c) The QTSP identifies two persons (System administrators) responsible for network and information security and reporting to top management.

d) Appropriate disciplinary sanctions are applied to personnel violating QTSP's policies or procedures.

e) Personnel's security roles and responsibilities, as specified in the QTSP's information security policy, are documented in their job descriptions. Trusted roles, on which the security of the QTSP's operation is dependent, are clearly identified.

f) QTSP personnel (both temporary and permanent) have job descriptions defined from the point of view of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. The job descriptions include skills and experience requirements.

g) Personnel exercise administrative and management procedures and processes that are in line with the QTSP's information security management procedures.

h) QTSP employs managerial personnel who possess:
   - Knowledge of qualified long-term preservation of digital signatures technology.
   - Knowledge of digital signature technology.
   - Familiarity with security procedures for personnel with security responsibilities.
   - Experience with information security and risk assessment.

i) All QTSP personnel in trusted roles are free from conflict of interest that might prejudice the impartiality of the QTSP operations.

j) Trusted roles are defined in the QTSP's information security policy and include roles that involve the following responsibilities:
   - Security officers: overall responsibility for administering the implementation of the security practices.
   - System administrators: authorized to install, configure, and maintain the QTSP trustworthy systems for qualified trust services.
   - System operators: responsible for operating the QTSP trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.
   - System auditors: authorized to view archives and audit logs of the QTSP trustworthy systems.

k) QTSP personnel are formally appointed to trusted roles by the senior management responsible for security.

l) Personnel have no access to the trusted functions until any necessary checks are completed.

m) When personnel are working remotely, QTSP implements cybersecurity measures to protect information accessed, processed or stored outside the QTSP's premises.

n) QTSPs allowing remote working activities issues a topic-specific policy on remote working that defines the relevant cybersecurity conditions and restrictions.

The director of the MitSoft is responsible for employing the personnel complying with these requirements as well as testing their skills and reliability, defining and

describing the roles of personnel (including the trusted functions) in their job descriptions.

All the personnel can perform the operations defined by their roles only.

7.3. Asset management

7.3.1. General

The QTSP ensures that its information and other assets, including the assets provided through a supply chain, receive an appropriate protection.

7.3.2. Assets inventory and classifications

The QTSP maintains an accurate inventory of assets as a prerequisite for effective technical vulnerability management and consistent with the risk assessment. The asset's classification level is assigned based on requirements for protecting confidentiality, integrity, authenticity, and availability, and in accordance to its business value.

The availability requirements of each asset are aligned with the delivery and recovery objectives as described in the business continuity plan.

The QTSP conducts periodic reviews of the inventory of the assets.

The QTSP has defined and implement rules/procedures for the acceptable use and handling of information and other associated assets.

The QTSP procedures for change/termination process of personnel (internal and external), contractors, and other third parties include the return of all previously issued physical and electronic assets owned by or entrusted to the QTSP.

7.3.3. Storage media handling

All storage media are managed through its life cycle of acquisition, use, transportation, and disposal in accordance with the QTSP's classification scheme and handling requirements.

All media are handled securely in accordance with the requirements of the information classification scheme. Media containing sensitive data are securely disposed of when no longer required.

Storage media used within the QTSP's systems are securely handled to protect storage media from damage, theft, unauthorized access, and obsolescence.

Storage media management procedures protect against obsolescence and deterioration of storage media within the period of time that records are required to be retained.

7.4. Access control

The QTSP ensures that QTSP system access is limited to properly authorized individuals. In particular:

a) A firewall is implemented to protect the QTSP's internal network domains from unauthorized access, including access by subscribers and third parties. The firewall is configured to prevent all protocols and accesses not required for the operation of the QTSP. Technical solution is provided in System Architecture and Management document.

b) The QTSP ensures effective administration of user access required for the work of operators, administrators, and auditors. The principle of "least privileges" is applied when configuring user access privileges.

c) QTSP reviews access rights to administrator, operator and auditor accounts regularly or upon termination of employment, change of function or

organisational changes. The necessary changes of access rights and assignment of trusted roles are documented. In this way, the system security, including MitSoft QTSP user account management, auditing, and timely modification or removal of access, is maintained.

d) Access to information and application system functions is restricted in accordance with the access control policy, and the QTSP system provides sufficient computer security controls for the separation of trusted roles identified in the information security policy, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled.

e) The QTSP sets up specific administrator accounts for installation, configuration, management and maintenance of its systems. The MitSoft QTSP personnel uses administrator accounts only to perform specific system maintenance activity.

f) QTSP personnel are properly identified and authenticated before using critical applications related to the qualified trust services. Strong identification, authentication and authorisation procedures are implemented for accounts used to perform system administration and maintenance activities.

g) QTSP personnel are accountable for their activities; to this end, event logs are retained (see the section 7.10. Collection of evidence).

h) Sensitive data is protected against being revealed through re-used storage objects or storage media being accessible to unauthorized user (see 7.3.3. Storage media handling).

i) The local network components (e.g., routers) are kept in a physically secure environment, and their configurations are periodically audited for compliance with the requirements specified by the QTSP.

j) Continuous monitoring and alarm facilities are provided to enable the QTSP to detect, register, and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

7.5. Cryptographic controls

Appropriate security controls are in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

7.6. Physical and environmental security

The QTSP ensures that physical access to critical services is controlled and physical risks to its assets is minimized. In particular:

- Physical access to facilities concerned with qualified trust services is limited to properly authorized individuals.
- Non-authorised person is accompanied by authorized person in the security area.
- Controls are implemented to avoid loss, damage or compromise of assets, theft or leak of information, interruption to business activities.
- Controls are implemented to avoid compromise or theft of information and information processing facilities.
- The qualified trust services facilities are operated in an environment that physically protects the service from compromise through unauthorized access to systems or data.
- Physical protection is achieved through the creation of a clearly defined security perimeter around the qualified trust services. Inside this perimeter, there are no parts of the premises shared with other organizations.

- Physical and environmental security controls are implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The QTSP's physical and environmental security policy for systems concerned with qualified trust services addresses the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g., power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.
- Controls are implemented to protect against equipment, information, media and software relating to the trust services being taken off-site without authorization.

QTSP's qualified trust services equipment operates in the DELSKA data centre (DC). The boundaries within DC, at the same time, define the security perimeter, unauthorized access to the inside area of which is not possible. The building of the Data centre is protected by the watchers and security service. Every entry to the physically secure area and exit from it is logged. In this way, the assets (including media) are protected against being taken off-site without authorization or compromise.

Data centre operates a modern air conditioning system, which is maintaining the air temperature necessary and cleaning the air of the dust. If the power supply fails, UPS and the diesel electric power generator maintain normal operation of the system for 4 hours.

To prevent compromise and theft of information, the following measures are taken: in the QTSP's equipment, internet connection is limited – only the connections necessary for the provision of qualified trust services are allowed. Firewalls and intrusion protection systems are implemented.

7.7. Operation security

For critical services, as identified by the risk analysis, the QTSP uses trustworthy systems and products that are protected against modification. The QTSP ensures that the QTSP system components are secure and correctly operated, with minimal risk of failure.

In particular:

a) An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by the QTSP or on behalf of the QTSP to ensure that security is built into IT systems.

b) Change control procedures are applied for releases, modifications, and emergency software fixes of any operational software and changes to the configuration which applies the QTSP's security policy. These procedures include documentation of the changes. The maximum interval between two checks does not exceed 12 months.

c) The integrity of QTSP system components and information is protected against viruses, malicious and unauthorized software by antivirus software installation.

d) Media used within the QTSP trustworthy systems are securely handled to protect media from damage, theft, unauthorized access, and obsolescence.

e) Media management procedures are employed to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

f) Procedures are established and implemented for all trusted and administrative roles that have impact on the provision of qualified trust services.

g) Security patches management procedures are employed to ensure that:
   - security patches are applied within a reasonable time after they come available;
   - security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
   - the reasons for not applying any security patches are documented.

h) Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available;

i) The QTSP establishes, documents, implements, monitors, and reviews configurations, including security configurations, of hardware, software, services and networks;

j) The QTSP monitors configurations with a comprehensive set of system management tools, as defined in the document System Architecture and Management;

k) The QTSP reviews configurations during system audits to verify configuration settings, evaluate password strengths and assess activities performed.

7.8. Network security

The QTSP maintains and protects QTSP system hosted by DELSKA data centre in a secure internal network, accessible by the personnel in trusted roles only. The same security controls are applied to all system's components co-located in the secure internal network:

a) The QTSP segments trust services system's network based on information security policy requirements according to functional, logical, and physical relationship between components as provided in the document System Architecture and Management.

b) The QTSP restricts access and communications between these zones to those necessary for the operation of the QTSP.

c) The configuration of QTSP systems is hardened so that only the necessary accounts, applications, services, protocols, and ports are used. The firewall is configured to prevent all protocols and accesses not required for the operation of the QTSP.

d) The information security policy of the QTSP identifies the trusted roles and assigns the corresponding responsibilities in order to implement network security practices. The QTSP reviews the established rules set on a regular basis.

e) The QTSP keeps all subsystems that are critical to the QTSP's operation in secured zones as indicated in the document System Architecture and Management.

f) Administration systems and networks are logically separated from other information systems and networks, including QTSP's operational network.

g) The QTSP separates the production system for the QTSP's services from systems used in development and testing. Development and test systems are hosted in a separate location outside of the QTSP network.

h) According to the document System Architecture and Management the QTSP establishes communication between distinct subsystems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

i) The QTSP protects its network and information systems against malicious and unauthorized software by means of malware detection and removal software. Definitions of malware are updated several times per day.

j) The QTSP performs the vulnerability scan on public and private IP addresses identified by the QTSP at least once per quarter.

k) The QTSP performs a penetration test on the QTSP's systems at set up and after infrastructure or application upgrades or modifications that the QTSP determines are significant at least once per year.

l) The QTSP provides evidence that each vulnerability scan and penetration test are performed by persons with the skills, tools, proficiency, and independence necessary to provide a reliable report.

7.9. Vulnerabilities and Incident management

The QTSP is constantly monitoring system activities concerning access to and use of the QTSP's systems:

a) Monitoring activities analyse system status and collect a technical information that is restricted according to the MitSoft QTSP information classification scheme and accessible only to persons in trusted role with security obligations.

b) Abnormal system activities that indicate potential security violations, including possible intrusions, are detected and reported as alarms based on monitoring functionality and obligations of system administrators and system operator.

c) The monitoring includes the start-up and shutdown of the logging functions and the availability and utilization of needed services with the QTSP's network.

d) The QTSP acts in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security as described in Incident management procedure.

e) The QTSP appoints in job descriptions system administrator trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the QTSP's procedures.

f) The QTSP establishes procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

g) The QTSP notifies the natural or legal person on the breach of security or loss of integrity without undue delay when the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided according to Incident management procedure.

h) The QTSP's systems are monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity. The QTSP implements automatic mechanisms to process the audit logs and alert personnel of possible critical security events. System auditor acts according to the System audit procedure.

i) The QTSP addresses any new critical vulnerability within a period of 48 hours after its discovery.

j) For any vulnerability, the QTSP determines the cost of the potential impact and based on it creates and implements the vulnerability's mitigation plan or documents the factual basis for the QTSP's determination that the vulnerability does not require remediation.

k) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

7.10. Collection of evidence

The QTSP ensures that all relevant information concerning the operation of qualified trust services is recorded and stored for an appropriate period of time, for the purpose of providing evidence for the purposes of legal proceedings. In particular:

a) The specific events and data to be logged are documented in the QTSP's information security policy, including clients calls to API operations, services operations, and interactive actions of users.

b) The confidentiality and integrity of current and archived records concerning operation of qualified trust services is maintained.

c) Records concerning the operation of qualified trust services are completely and confidentially archived in accordance with disclosed QTSP practices.

d) Records concerning the operation of qualified trust services are made available if required for the purposes of providing evidence of the correct operation of the qualified trust services for the purpose of legal proceedings.

e) The precise time of clock adjustments of over 1 second is recorded. The time used to record events in the audit log is synchronized with UTC at least once a day.

f) The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

g) Any information recorded about subscribers are kept confidential except as where agreement is obtained from the subscriber for its wider publication.

7.11. Business continuity management

The QTSP has an up-to-date continuity plan to enact in case of a disaster. In the event of a disaster operations are restored within the delay established in the continuity plan, addressing any cause of the disaster which may recur (e.g., a security vulnerability) with appropriate remediation measures.

The QTSP ensure that in the case of events which affect the security of the QTSP's services, relevant information is made available to subscribers and relying parties.

7.12. QTSP termination and termination plans

The QTSP ensures that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the QTSP's qualified trust services. The QTSP's termination plans comply with the requirements set out in the Commission implementing Regulation (EU) 2025/2530 of 16 December, that is, an implementing act adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014. The QTSP takes the following measures to maintain its termination plans:

a) The QTSP sets up controls and procedures to ensure the availability for internal use of documented policies, practices, procedures, and third-party arrangements to ensure the effectiveness of the termination plan.

b) The QTSP ensures that termination plan and any document associated with it are up to date.

c) The QTSP reviews the termination plan and any associated documents at least every two years and as part of the implementation of any changes to the qualified trust service provider or to the qualified trust services it provides and update the termination plan accordingly.

d) The QTSP manages the risks that are specific to the termination of the provision of qualified trust services as part of the risk management framework.

e) The QTSP ensures maintenance of sufficient financial resources to cover the costs required to effectively execute the termination plan, including in case of unanticipated termination.

f) The QTSP ensures that the termination plan specifies appropriate procedures and arrangements.

g) The QTSP termination plan references:
   - Qualified Long-term Preservation service activity termination plan;
   - Qualified Time-stamping service activity termination plan.

7.13. Compliance

QTSP confirms that the MitSoft qualified trust services conform to the Policies and the Practice Statements. In this way, QTSP undertakes all the obligations defined in the Policies and fulfils all the defined requirements for its activities.

The compliance of the QTSP 's activities with the Policies and Practice Statements is verified as defined by this QTS PS, at least every two years.

The QTSP ensures compliance with legal requirements. In particular:

a) Compliance with the requirements of the Regulation (EU) No 910/2014 [eIDAS] is confirmed at least every 24 months by an audit performed by an accredited conformity assessment body.

b) The QTSP has no specific requirements for use of the services which could prevent access for persons with disabilities. Trust services client software will provide user interface. Trust services itself provide limited user interface for administration purpose.

c) The QTSP ensures that the requirements of the European Data Protection Directive 95/46/EC, as it is implemented through Lithuanian legislation, are met:
   - The QTSP processes the data together with the communication level attributes as necessary to provide the trust services and to fulfil the requirements of the applicable standards, including monitoring for security, accounting and capacity planning.
   - No other data, including personal data, is collected or processed during the provision of the services.
   - Appropriate technical and organizational measures are taken against unauthorized or unlawful processing, disclosure, accidental loss or destruction of, or damage to, the data received.
   - MitSoft UAB has policy for personal data processing, employees involved have signed confidentiality agreements.

d) MitSoft QTSP operational software has no user interface, it provides API that should be used from client system.

e) Activity Termination Plans are to be approved by Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers.

7.14. Supply chain

QTSP supply chain consists of suppliers that are qualified trust service providers or ISO 27001 and TIER 3 certified Infrastructure as a Service providers. These providers, being qualified trust service providers, satisfy all supply chain requirements of the standard ETSI EN 319 401.

All ICT products that make up the QTSP system are developed by QTSP employees according to the secure development principles. When QTSP uses open source from other

parties, including trust service component providers, it maintains overall responsibility for compliance with the supply chain policy, information security policy, and the requirements defined in the trust service policy.

Infrastructure as a Service providers ensure all utilities needed for physical and environmental security, including internet communication.

According to the supply chain security policy, QTSP identifies his role in the supply chain and communicates it to related parties. QTSP has defined and implemented processes and procedures to manage information security risks, associated with service supply chain and ICT products.

7.14.1. Supply chain policy

QTSP has established, implemented and applies a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems.

The supply chain policy defines criteria for selecting and contracting suppliers or service providers:

a) requirements regarding awareness, skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees;
b) requirements regarding the verification of the background of the suppliers' and service providers' employees;
c) an obligation on suppliers and service providers to notify, without undue delay, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;
d) the right to audit or right to receive audit reports;
e) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of MitSoft;
f) requirements regarding subcontracting and, where MitSoft allows subcontracting, cybersecurity requirements for subcontractors;
g) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.

7.14.2. Supply chain procedures and processes

QTSP has defined and implemented processes and procedures to manage information security risks associated with the trust services supply chain.

QTSP regularly monitors, reviews, evaluates, and manages change in supplier information security practices and service delivery to keep early indications on supplier status.

QTSP establishes permanent communication channels with suppliers, including sensor-based signals.

QTSP creates a current knowledge exchange network with suppliers on new requirements and actualities of trust services.

7.14.3. Responsibility, third-party agreements and SLA

QTSP has two kinds of relationship with third-parties: contractual and non-contractual. The contractual relationship foresees full substitution of service provision in the case of service abandon of the main service provider according to requirements of qualified trust service provider level.

Non-contractual relationship with third-parties takes place in the case when free service provision is mandatory for qualified service providers as part of qualified service provision, like response to qualified certificate status request.