MTS STATEMENT OF APPLICABILITY (SOA)

Version 2.3

JANUARY 2026

MTS

Since October 2020 MTS S.p.A. is ISO 27001:2022 certified.

This certificate is valid for the following scope:

The conception, design, software development and application management and customer support of the following MTS electronic market platforms: Cash Market Facility (CMF); BondVision (BV); Money Market Repo (MMF); Primary Auction (PAF).

The conception, design, clients' support and monitoring of regulated markets and MTF organized and managed by MTS Spa and its subsidiaries (EuroMTS Ltd and MTS France SAS).

The conception, design, software development, application management and clients' support of ancillary services which are the following: MTS Datafeed; Upstream data contributors; Management Information System; Regulatory data flows; End of day data flows.

In accordance with the Statement of Applicability version 2 of 16 september 2024.

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
5.1	ORGANIZATIONAL	Policies for information security	To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.	YES	YES
5.2	ORGANIZATIONAL	information security roles and responsibilities	To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.	YES	YES
5.3	ORGANIZATIONAL	Segregation of duties	To reduce the risk of fraud, error and bypassing of information security controls.	YES	YES
5.4	ORGANIZATIONAL	Management responsibilities	To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.	YES	YES
5.5	ORGANIZATIONAL	Contact with autorities	To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.	YES	YES
5.6	ORGANIZATIONAL	Contact with special interest groups	To ensure appropriate flow of information takes place with respect to information security	YES	YES
5.7	ORGANIZATIONAL	Threat intelligence	To provide awareness of the organization’s threat environment so that the appropriate mitigation actions can be taken.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
5.8	ORGANIZATIONAL	Information security in project management	To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.	YES	YES
5.9	ORGANIZATIONAL	Inventory of information and other associated assets	To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.	YES	YES
5.10	ORGANIZATIONAL	Acceptable use of information and other associated assets	To ensure information and other associated assets are appropriately protected, used and handled.	YES	YES
5.11	ORGANIZATIONAL	Return of assets	To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.	YES	YES
5.12	ORGANIZATIONAL	Classification of information	To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.	YES	YES
5.13	ORGANIZATIONAL	Labelling of information	To facilitate the communication of classification of information and support automation of information processing and management.	YES	YES
5.14	ORGANIZATIONAL	Information transfer	To maintain the security of information transferred within an organization and with any external interested party.	YES	YES
5.15	ORGANIZATIONAL	Access control	To ensure authorized access and to prevent unauthorized access to information and other associated assets.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
5.16	ORGANIZATIONAL	Identity management	To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.	YES	YES
5.17	ORGANIZATIONAL	Authentication information	To ensure proper entity authentication and prevent failures of authentication processes.	YES	YES
5.18	ORGANIZATIONAL	Access rights	To ensure access to information and other associated assets is defined and authorized according to the business requirements.	YES	YES
5.19	ORGANIZATIONAL	Information security in supplier relationships	To maintain an agreed level of information security in supplier relationships.	YES	YES
5.20	ORGANIZATIONAL	Addressing information security within supplier agreements	To maintain an agreed level of information security in supplier relationships.	YES	YES
5.21	ORGANIZATIONAL	Managing information security in the ICT supply	To maintain an agreed level of information security in supplier relationships.	YES	YES
5.22	ORGANIZATIONAL	Monitoring, review and change management of supplier	To maintain an agreed level of information security and service delivery in line with supplier agreements.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
5.23	ORGANIZATIONAL	Information security for use of cloud services	To specify and manage information security for the use of cloud services.	YES	YES
5.24	ORGANIZATIONAL	Information security incident management planning and	To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.	YES	YES
5.25	ORGANIZATIONAL	Assessment and decision on information security events	To ensure effective categorization and prioritization of information security events.	YES	YES
5.26	ORGANIZATIONAL	Response to information security incidents	To ensure efficient and effective response to information security incidents.	YES	YES
5.27	ORGANIZATIONAL	Learning from information security incidents	To reduce the likelihood or consequences of future incidents.	YES	YES
5.28	ORGANIZATIONAL	Collection of evidence	To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.	YES	YES
5.29	ORGANIZATIONAL	Information security during disruption	To protect information and other associated assets during disruption.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
5.30	ORGANIZATIONAL	ICT readiness for business continuity	To ensure the availability of the organization's information and other associated assets during disruption.	YES	YES
5.31	ORGANIZATIONAL	Legal, statutory, regulatory and contractual requirements	To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.	YES	YES
5.32	ORGANIZATIONAL	Intellectual property rights	To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.	YES	YES
5.33	ORGANIZATIONAL	Protection of records	To ensure compliance with legal, statutory, regulatory and contractual requirements requirements, as well as community or societal expectations related to the protection and availability of records.	YES	YES
5.34	ORGANIZATIONAL	Privacy and protection of PII	To ensure compliance with legal, statutory, regulatory and contractual requirements to the information security aspects of the protection of PII.	YES	YES
5.35	ORGANIZATIONAL	Independent review of information security	To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.	YES	YES
5.36	ORGANIZATIONAL	Compliance with policies, rules and standards for information security	To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
5.37	ORGANIZATIONAL	Documented operating procedures	To ensure the correct and secure operation of information processing facilities.	YES	YES
6.1	PEOPLE	Screening	To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.	YES	YES
6.2	PEOPLE	Terms and conditions of employment	To ensure personnel understand their information security responsibilities for the roles for which they are considered.	YES	YES
6.3	PEOPLE	Information security awareness, education and training	To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.	YES	YES
6.4	PEOPLE	Disciplinary process	To ensure personnel and relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.	YES	YES
6.5	PEOPLE	Responsibilities after termination or change of employment	To protect the organization’s interests as part of the process of changing or terminating employment or contracts.	YES	YES
6.6	PEOPLE	Confidentiality or non-disclosure agreements	To maintain confidentiality of information accessible by personnel or external parties.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
6.7	PEOPLE	Remote working	To ensure the security of information when personnel are working remotely.	YES	YES
6.8	PEOPLE	Information security event reporting	To support timely, consistent and effective reporting of information security events that can be identified by personnel.	YES	YES
7.1	PHYSICAL	Physical security perimeters	To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.	YES	YES
7.2	PHYSICAL	Physical entry	To ensure only authorized physical access to the organization's information and other associated assets occurs.	YES	YES
7.3	PHYSICAL	Securing offices, rooms and facilities	To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.	YES	YES
7.4	PHYSICAL	Physical security monitoring	To detect and deter unauthorized physical access.	YES	YES
7.5	PHYSICAL	Protecting against physical and environmental threats	To prevent or reduce the consequences of events originating from physical and environmental threats.	YES	YES
7.6	PHYSICAL	Working in secure areas	To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
7.7	PHYSICAL	Clear desk and clear screen	To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.	YES	YES
7.8	PHYSICAL	Equipment siting and protection	To reduce the risks from physical and environmental threats, and from unauthorized access and damage.	YES	YES
7.9	PHYSICAL	Security of assets off-premises	To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.	YES	YES
7.10	PHYSICAL	Storage media	To ensure only authorized disclosure, modification, removal or destruction of information on storage media.	YES	YES
7.11	PHYSICAL	Supporting utilities	To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.	YES	YES
7.12	PHYSICAL	Cabling security	To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations related to power and communications cabling.	YES	YES
7.13	PHYSICAL	Equipment maintenance	To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations caused by lack of maintenance.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
7.14	PHYSICAL	Secure disposal or re-use of equipment	To prevent leakage of information from equipment to be disposed or re-used.	YES	YES
8.1	TECHNOLOGICAL	User endpoint devices	To protect information against the risks introduced by using user endpoint devices.	YES	YES
8.2	TECHNOLOGICAL	Privileged access rights	To ensure only authorized users, software components and services are provided with privileged access rights.	YES	YES
8.3	TECHNOLOGICAL	Information access restriction	To ensure only authorized users and to prevent unauthorized access to information and other associated assets.	YES	YES
8.4	TECHNOLOGICAL	Access to source code	To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.	YES	YES
8.5	TECHNOLOGICAL	Secure authentication	To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.	YES	YES
8.6	TECHNOLOGICAL	Capacity management	To ensure the required capacity of information processing facilities, human resources, offices and other facilities.	YES	YES
8.7	TECHNOLOGICAL	Protection against malware	To ensure information and other associated assets are protected against malware.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
8.8	TECHNOLOGICAL	Management of technical vulnerabilties	To prevent exploitation of technical vulnerabilities.	YES	YES
8.9	TECHNOLOGICAL	Configuration management	To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.	YES	YES
8.10	TECHNOLOGICAL	Information deletion	To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.	YES	YES
8.11	TECHNOLOGICAL	Data masking	To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.	YES	Partially
8.12	TECHNOLOGICAL	Data leakage prevention	To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.	YES	YES
8.13	TECHNOLOGICAL	Information backup	To enable recovery from loss of data or systems.	YES	YES
8.14	TECHNOLOGICAL	Redundancy of information processing facilities	To ensure the continuous operation of information processing facilities.	YES	YES
8.15	TECHNOLOGICAL	Logging	To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
8.16	TECHNOLOGICAL	Monitoring activities	To detect anomalous behaviour and potential information security incidents.	YES	YES
8.17	TECHNOLOGICAL	Clock synchronization	To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.	YES	YES
8.18	TECHNOLOGICAL	Use of privileged utility programs	To ensure the use of utility programs does not harm system and application controls for information security.	YES	YES
8.19	TECHNOLOGICAL	Installation of software on operational systems	To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.	YES	YES
8.20	TECHNOLOGICAL	Network security	To protect information in networks and its supporting information processing facilities from compromise via the network.	YES	YES
8.21	TECHNOLOGICAL	Security of network services	To ensure security in the use of network services.	YES	YES
8.22	TECHNOLOGICAL	Segregation of networks	To split the network in security boundaries and to control traffic between them based on business needs.	YES	YES
8.23	TECHNOLOGICAL	Web filtering	To protect systems from being compromised by malware and to prevent access to unauthorized web resources.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
8.24	TECHNOLOGICAL	Use of cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.	YES	YES
8.25	TECHNOLOGICAL	Secure development life cycle	To ensure information security is designed and implemented within the secure development life cycle of software and systems.	YES	YES
8.26	TECHNOLOGICAL	Application security requirements	To ensure all information security requirements are identified and addressed when developing or acquiring applications.	YES	YES
8.27	TECHNOLOGICAL	Secure system architecture and engineering principles	To ensure information systems are securely designed, implemented and operated within the development life cycle.	YES	YES
8.28	TECHNOLOGICAL	Secure coding	To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.	YES	YES
8.29	TECHNOLOGICAL	Security testing in development and acceptance	To validate if information security requirements are met when applications or code are deployed to the production environment.	YES	YES
8.30	TECHNOLOGICAL	Outsourced development	To information security measures required by the organization are implemented in outsourced system development.	YES	YES

CONTROL ID	CONTROL TYPE	CONTROL NAME	CONTROL PURPOSE	APPLICABLE	APPLIED
8.31	TECHNOLOGICAL	Separation of development, test and production environments	To protect the production environment and data from compromise by development and test activities.	YES	YES
8.32	TECHNOLOGICAL	Change management	To preserve information security when executing changes.	YES	YES
8.33	TECHNOLOGICAL	Test information	To ensure relevance of testing and protection of operational information used for testing.	YES	YES
8.34	TECHNOLOGICAL	Protection of information systems during audit testing	To minimize the impact of audit and other assurance activities on operational systems and business processes.	YES	YES

www.mtsmarkets.com