NIST 800-171 Compliance Data Sheet

maytech
A Kiteworks Company

Maytech Information Security Management System Conformance with NIST 800-171

Maytech's information security management system (ISMS) is compliant with NIST 800-171 and is certified with the international standard ISO 27001:2013 for which we are audited twice a year by Lloyd's Register Quality Assurance, one of the leading business assurance providers globally.

Appendix D of the NIST 800-171 (Revision1) publication maps each requirement statement against the equivalent control in ISO 27001:2013, the implication being that conformance with the ISO 27001 control signifies conformance with the respective NIST 800-171 requirement.

However, some of the NIST 800-171 requirements have no direct mapping, or the equivalent ISO 27001 control has an asterisk against it, indicating that the ISO control "does not fully satisfy the intent of the NIST control". The requirements in these two categories are itemised in the table below.

The first three columns are reproduced from Appendix D of NIST 800-171. The fourth column shows how Maytech's ISMS and/or product conforms with the specified requirement - thereby demonstrating that Maytech conforms to NIST 800-171.

NIST 800-171 requirement	NIST SP 800-53 relevant security controls		Maytech compliance status
3.1.5	AC-6(1)	Least Privilege *Authorize Access to Security Functions*	Privileged access (security-related functions) is available only to system administrators
	AC-6(5)	Least Privilege *Privileged Accounts*	
3.1.6	AC-6(2)	Least Privilege *Non-Privileged Access for Non-security Functions*	Non-privileged access is granted, in accordance with Maytech's access control processes, based on job requirements and managed by system administrators
3.1.7	AC-6(9)	Least Privilege *Auditing Use of Privileged Functions*	Standard operating system facilities are used to audit use of privileged accounts e.g. log-in times
	AC-6(10)	Least Privilege *Prohibit Non-Privileged Users from Executing Privileged Functions*	Privileged functions are available only to privileged users

3.1.10	AC-11(1)	Session Lock *Pattern-Hiding Displays*	Users are required to lock their screens when unattended. Systems are configured so that screens lock after a specified period of inactivity
3.1.11	AC-12	Session Termination	Similarly, sessions are set to terminate after 15 minutes of inactivity
3.1.12	AC-17(1)	Remote Access *Automated Monitoring / Control*	Remote access is possible only via VPN, thereby controlling which users are able to access from remote locations
3.1.13	AC-17(2)	Remote Access *Protection of Confidentiality / Integrity Using Encryption*	VPN ensures encryption
3.1.14	AC-17(3)	Remote Access *Managed Access Control Points*	VPN provides management of access control points
3.1.15	AC-17(4)	Remote Access *Privileged Commands / Access*	See 3.1.12-14 above. See also 3.1.5 about the restrictions relating to privileged access.
3.1.17	AC-18(1)	Wireless Access *Authentication and Encryption*	WP22 Enterprise (dot1x) is used for secure authentication . It's based on the client certificates and require one-time authentication.
3.1.19	AC-19(5)	Access Control for Mobile Devices *Full Device / Container-Based Encryption*	Laptop hard drives are encrypted. No CUI is stored on phones
3.1.20	AC-20(1)	Use of External Systems *Limits on Authorized Use*	External systems are used only with CTO authorization
3.1.21	AC-20(2)	Use of External Systems *Portable Storage Devices*	Portable Storage Devices are not used
3.1.22	AC-22	Publicly Accessible Content	This requirement is covered by a Maytech security policy
3.2.1 - 3.2.2	AT-3	Role-Based Security	All staff are trained so that they have the skills needed for their respective jobs
3.2.3	AT-2(2)	Security Awareness Training *Insider Threat*	Regular Security Awareness Training is provided

3.3.1 - 3.3.2	AU-2	Audit events	Records are generated by operating systems and other system software and retained for twelve months
	AU-3	Content of Audit Records	Records enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity
	AU-3(1)	Content of Audit Records *Additional Audit Information*	Confirmed; see above
3.3.3	AU-2(3)	Audit Events *Reviews and Updates*	Confirmed; see above
3.3.4	AU-5	Response to Audit *Processing Failures*	An alert is generated if an audit tool (e.g. IDS) fails
3.3.5	AU-6(3)	Audit Review, Analysis, and Reporting *Correlate Audit Repositories*	This is addressed by Maytech's Incident Management process
3.3.6	AU-7	Audit Reduction and Report Generation	This is conducted dependent on the incident and circumstances
3.3.7	AU-8(1)	Time Stamps *Synchronization with Authoritative Time Source*	Systems are automatically synchronised to an authoritative time source via industry standard features in the respective operating systems
3.3.9	AU-9(4)	Protection of Audit Information *Access by Subset of Privileged Users*	Audit information is available only to the system administrators. See 3.1.5.
3.4.1 - 3.4.2	CM-2	Baseline Configuration	This is part of Maytech's system development process
	CM-6	Configuration Settings	
	CM-8(1)	System Component Inventory *Updates During Installations / Removals*	Inventories of assets are maintained

3.4.6	CM-7	Least Functionality	This is part of standard working practice
3.4.7	CM-7(1)	Least Functionality *Periodic Review*	
	CM-7(2)	Least Functionality *Prevent program execution*	
	CM-7(4)	Least Functionality *Unauthorized Software/ Blacklisting*	The access/privilege control arrangements described at 3.5.1 prevent unauthorised software from being used
	CM-7(5)	Least Functionality *Authorized Software/ Whitelisting*	Similarly, the arrangements control the authorisation of trusted software
3.5.1 - 3.5.2	IA-3	Device Identification and Authentication	This is implemented as part of the access control arrangements referred to in 3.1.5 and 3.1.6
3.5.3	IA-2(1)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts*	Two-factor authentication is in place to control access for system administrators and for user access to critical business systems
	IA-2(2)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts*	See 3.1.6
	IA-2(3)	Identification and Authentication (Organizational Users) *Local Access to Privileged Accounts*	See 3.1.5 and 3.1.6. Note that access to privileged accounts is restricted to system administrators
	IA-2(8)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts-Replay Resistant*	Industry-standard systems are in use which prevent the use of replay facilities
		Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts-Replay Resistant*	
3.5.7- 3.5.10	IA-5(1)	Authenticator Management *Password-Based Authentication*	A system-enforced password policy is in place

3.6.1	IR-2	Incident Response Training	Staff familiarity with incident response processes is included in general ISMS awareness training
3.6.1 - 3.6.2	IR-5	Incident Monitoring	An incident management procedure defines the process for incident monitoring and response
	IR-7	Incident Response Assistance	
3.6.3	IR-3	Incident Response Testing	The Business Continuity Plan is tested annually
	MA-2	Controlled Maintenance	Any need for equipment maintenance or consequent removal of assets is controlled in accordance with the ISMS
3.7.1 - 3.7.2	MA-3	Maintenance Tools	Industry standard products are in use. Maintenance tools are not required or used.
	MA-3(1)	Maintenance Tools *Inspect Tools*	
	MA-3(2)	Maintenance Tools *Inspect media*	
3.7.3	MA-2	Controlled Maintenance	Any equipment removed for off-site maintenance is sanitized of any CUI, in accordance with equipment disposal procedures
3.7.4	MA-3(2)	Maintenance Tools	Not applicable
3.7.5	MA-4	Non-local Maintenance	No non-local maintenance is required or applied
3.7.6	MA-5	Maintenance Personnel	If maintenance personnel were needed they would be treated as visitors and under the supervision of their hosts
3.8.6	MP-5(4)	Media Transport *Cryptographic Protection*	Not applicable (no media transport)
3.8.8	MP-7(1)	Media Use *Prohibit Use Without Owner*	Not applicable. No business requirement.

3.10.1	PE-2	Physical Access Authorizations	Physical access to organizational systems, equipment, and the respective operating environments, either on Maytech premises or data centres, is limited to authorized individuals
3.10.1 - 3.10.2	PE-6	Monitoring Physical Access	This is covered by the respective service agreement with providers
3.11.1		Risk Assessment	The risk to organizational operations, as documented in the risk assessment, is reviewed regularly - particularly at ISMS management review meetings
3.11.2 - 3.11.3	RA-5	Vulnerability Scanning	Daily vulnerability scanning with Vuls (https://vuls.io/) and weekly vulnerability scanning with McAfee Secure. Remediation applied in accordance with the corrective action and continual improvement processes.
3.11.2	RA-5(5)	Vulnerability Scanning *Privileged Access*	Scanning is undertaken only conducted by system administrators
3.12	CA-5	Plan of Action and Milestones	Addressed by incident management and improvement processes
	CA-7	Continuous Monitoring	
3.13.3	SC-2	Application Partitioning	Confirmed i.e. user functionality is separated from system management functionality
3.13.4	SC-4	Information in Shared Resources	Access and network controls are in place, as confirmed above
3.13.6	SC-7(5)	Boundary Protection *Deny by Default / Allow by Exception*	Implemented via firewalls
3.13.7	SC-7(7)	Boundary Protection *Prevent Split Tunneling for Remote Devices*	

	SC-8(1)	Transmission Confidentiality and Integrity *Cryptographic or Alternate Physical Protection*	All transmission is encrypted
3.13.12	SC-15	Collaborative Computing Devices	These are not generally used but any that are would be industry-standard and not subject to remote activation
3.13.13	SC-18	Mobile Code	User consent is required before the code is loaded or changed
3.13.14	SC-19	Voice over Internet Protocol	Used only with CTO approval
3.13.15	SC-23	Session Authenticity	See controls above. Note that only industry standard communications products are used.
3.13.16	SC-28	Protection of Information at Rest	Client-owned information is encrypted at rest with AES-256 algorithm
3.14.3	SI-5	Security Alerts, Advisories, and Directives	System administrators receive alerts (e.g. on vulnerabilities) from suppliers and independent news sources
3.14.6	SI-4	System Monitoring	IDS is in place
	SI-4(4)	System Monitoring *Inbound and Outbound Communications Traffic*	
3.14.7	SI-4	System Monitoring	Any unauthorized use of organizational systems is evident from IDS and system access logs

Maytech is a security specialist and works hard to maintain a very secure file sharing platform for our customers. If you have any questions on compliance or our services, please contact us to discuss the specific requirements for your organization.