

mms

ns.publish
Our Certificates



Unsere Zertifikate / Our Certificates

Document Version 2.4

August 2026

mms solutions ag
Dorfstrasse 29
CH-8037 Zurich
T +41 44 446 83 30

mms solutions gmbh
TechQuartier, Platz der Einheit 2
DE-60327 Frankfurt a. M.
T +49 69 247 43 62 00

Office an register court
Frankfurt a. M.
HRB 107996
Managing director: Rolf Traber

A member of
Neidhart + Schön Group
mmssolutions.io



Übersicht / Overview

1	IQ NET ISMS Certificate for mms solutions AG	5
2	SQS ISO 27001 Certificate for mms solutions AG	6
3	Statement of Applicability (SoA) to the above SQS Certificate	8
4	Swiss Safety Center ISO 27001 Certificate for publiccloud ag	19
5	Statement of Applicability (SoA) to the above Swiss Safety Center Certificate	20
6	SV ISO 27001 Certificate for Green Datacenter AG	30
8	Bureau Veritas Certification ISO 27001 Certificate for AE Corp NL B.V.	31

Only applies to publicly accessible online reports, hosted by mms:

10	EY ISO 27001 Certificate for Amazon Web Services, Inc.	34
11	Statement of Applicability (SoA) to the above bsi Certificate	41

Erläuterung zur selbständigen Prüfung der Gültigkeit der aufgelisteten Zertifikate

Die ISO-27001-Norm schreibt vor, dass zur Aufrechterhaltung des Zertifikats ein jährlicher Audit durch die Zertifizierungsstelle bestanden werden muss. Wird dieser Audit nicht bestanden, zieht die Zertifizierungsstelle das Zertifikat zurück: es wird ungültig. Und jeder Aussteller solcher ISO-Zertifikate muss ein öffentliches Register mit den aktuell gültigen Zertifikaten führen, damit deren Gültigkeit jederzeit überprüft werden kann.

Statement for independent verification of the validity of the listed certificates

The ISO 27001 standard requires that an annual audit by the certification authority must be passed in order to maintain the certificate. If this audit is not passed, the certification authority withdraws the certificate: it becomes invalid. And every issuer of such ISO certificates must keep a public register of currently valid certificates so that their validity can be checked at any time.

Certificate

SQS has issued an IQNET recognized certificate that the organization:

mms solutions ag

Dorfstrasse 29
8037 Zurich
Switzerland

has implemented and maintains a
Information Security Management System

for the following scope:

The certification of the information security management system for the development, provision and operation of intelligent reporting solutions and the provision of IT services for the companies of the Neidhart + Schön Group.

which fulfils the requirements of the following standard:

ISO/IEC 27001:2022

Issued on: **08.01.2024**

Expires on: **07.01.2027**

Registration Number: **CH-H44239**



Alex Stoichitoiu
President of IQNET



F. Müller
CEO SQS



This attestation is directly linked to the IQNET Member's original certificate and shall not be used as a stand-alone document

IQNET Members*:

AENOR Spain **AFNOR Certification** France **APCER** Portugal **CCC** Cyprus **CISQ** Italy **CQC** China **CQM** China **CQS** Czech Republic
Cro Cert Croatia **DQS Holding GmbH** Germany **EAGLE Certification Group** USA **FCAV** Brazil **FONDONORMA** Venezuela **ICONTEC**
Colombia **ICS** Bosnia and Herzegovina **INTECO** Costa Rica **IRAM** Argentina **JQA** Japan **KFQ** Korea **LSQA** Uruguay **MIRTEC** Greece
MSZT Hungary **Nemko AS** Norway **NSAI** Ireland **NYCE** México **PCBC** Poland **Quality Austria** Austria **SII** Israel **SIQ** Slovenia **SIRIM**
QAS International Malaysia **SQS** Switzerland **SRAC** Romania **TSE** Turkey **YUQS** Serbia

* The list of IQNET Members is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com



Certificate

The SQS herewith attests that the organisation named below has a management system that meets the requirements of the normative basis mentioned.



mms solutions ag
Dorfstrasse 29
8037 Zurich
Switzerland

Further sites according to appendix

Scope

The certification of the information security management system for the development, provision and operation of intelligent reporting solutions and the provision of IT services for the companies of the Neidhart + Schön Group.

Normative basis

ISO/IEC 27001:2022 Information Security Management System

Statement of applicability / Version 13.11.2023

Reg. no. H44239
Page 1 of 2

Validity 08.01.2024–07.01.2027
Issue 08.01.2024



sqs.ch



A. Grisard
A. Grisard, President SQS

F. Müller
F. Müller, CEO SQS

Swiss Association for Quality and Management Systems (SQS)
Bernstrasse 103, 3052 Zollikofen, Switzerland



Member of





Appendix

Appendix of main certificate H44239

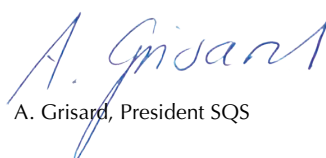


mms solutions ag
Dorfstrasse 29
8037 Zurich
Switzerland

Central Function	Scope	Norm / Revision	Reg. no.	Validity
mms solutions ag Dorfstrasse 29 8037 Zurich Switzerland	The certification of the information security management system for the development, provision and operation of intelligent reporting solutions and the provision of IT services for the companies of the Neidhart + Schön Group.	ISO/IEC 27001:2022	H44239	08.01.2024 07.01.2027
Locations	Scope	Norm / Revision	Reg. no.	Validity
mms solutions gmbh TechQuartier Platz der Einheit 2 60327 Frankfurt am Main Germany	Sales of the services provided by mms solutions ag, based in Zurich, for Germany and the EU.	ISO/IEC 27001:2022	H44239	08.01.2024 07.01.2027
Neidhart + Schön Group AG Dorfstrasse 29 8037 Zurich Switzerland	Investments in specialised companies in the communications industry. Central services.	ISO/IEC 27001:2022	H44239	08.01.2024 07.01.2027

Reg. no. H44239
Page 2 of 2

Validity 08.01.2024–07.01.2027
Issue 08.01.2024


A. Grisard, President SQS


F. Müller, CEO SQS



sqs.ch



Swiss Association for Quality and Management Systems (SQS)
Bernstrasse 103, 3052 Zollikofen, Switzerland



Statement of Applicability

based on ISO/IEC 27001:2022

Version 13.11.2023

5 Organizational controls

Control	Applicability	Justification
<u>5.1</u> Policies for information security Information security policy and topic-specific policies should 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.	✓	Die IS-Politik ist zusammen mit den IS-Zielsetzungen und der Management Reviews als Leitlinie für unser Handeln zu verstehen. Dort finden sich weitere grundlegende Aussagen darüber, welches Sicherheitsniveau erreicht werden soll und wie das nachgewiesen wird. Die IS-Richtlinien werden mindestens jährlich durch die Geschäftsleitung der MMS auf Eignung und Wirksamkeit geprüft.
<u>5.2</u> Information security roles and responsibilities Information security roles and responsibilities shall be defined and allocated according to the organization needs.	✓	Hauptverantwortlich für die Managementsysteme ist der CTO, welcher vom CISO massgeblich unterstützt wird. Er stellt die Ressourcen bereit und sorgt dafür, dass das System aufgebaut, unterhalten und weiterentwickelt wird.
<u>5.3</u> Segregation of duties Conflicting duties and conflicting areas of responsibility shall be segregated.	✓	Der CISO wurde extern beauftragt. Damit kann eine effektive Rollentrennung sichergestellt werden.
<u>5.4</u> 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.	✓	Die Mitarbeitenden sind sich der Informationssicherheitsproblematik und ihrer Aufgaben sowie Verantwortlichkeiten bewusst. Die dafür notwendigen Informationen werden regelmässig vermittelt und aktualisiert. Die Mitarbeitenden werden im Rahmen des jährlichen Mitarbeitergesprächs über diese informiert. Der jeweilige Vorgesetzte ist hierfür verantwortlich.
<u>5.5</u> Contact with authorities The organization shall establish and maintain contact with relevant authorities.	✓	Wo notwendig und sinnvoll, hat die MMS Kontakt zu Behörden. Dies gilt vor allem für die Polizei und Feuerwehr.
<u>5.6</u> Contact with special interest groups The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	✓	Die MMS hat Kontakt zu entsprechenden Fachverbänden. Der Bereich Informationssicherheit wird durch den CISO sichergestellt, welcher gut vernetzt ist.
<u>5.7</u> Threat intelligence Information relating to information security threats shall be collected and analysed to produce threat intelligence.	✓	Um die Systemumgebung jederzeit gegen mögliche Bedrohungen schützen zu können, werden verschiedenste Daten gesammelt, ausgewertet und durch geeignete Massnahmen kontinuierlich umgesetzt.
<u>5.8</u> Information security in project management Information security shall be integrated into project management.	✓	In jedem Projekt wird die Informationssicherheit berücksichtigt. Bei Softwareprojekten dürfen nur die Punkte aus der Anforderungsliste umgesetzt werden.

Control	Applicability	Justification
<u>5.9</u> Inventory of information and other associated assets An inventory of information and other associated assets, including owners, shall be developed and maintained.	✓	Die organisationseigenen Werte und Zuständigkeiten sind im Werteinventar dokumentiert.
<u>5.10</u> 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.	✓	Die Nutzung der IT ist in verschiedenen Nutzungsreglementen IT geregelt, welche die Mitarbeiter bei der Einstellung erhalten und deren Kenntnis sie mit Unterschrift bestätigen. Alle Personen mit Zugang zu klassifizierter Information müssen die definierten Regeln befolgen. Der CTO muss disziplinarische Massnahmen einleiten, falls die Regeln nicht befolgt werden oder die Information an nicht berechnigte Personen kommuniziert wird.
<u>5.11</u> 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.	✓	Die Rückgabe der Werte des austretenden Mitarbeiter wird durch eine HR Checkliste sichergestellt. Unabhängig davon werden sämtliche Zugriffsrechte entfernt und entsprechende Zugänge gelöscht.
<u>5.12</u> 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.	✓	Die MMS ist sich der Bedeutung des Schutzes von Informationen bewusst, da deren Missbrauch zu grossen materiellen und immateriellen Schäden führen kann. Die Klassifizierung und angemessenen Handhabung von Informationen ist ein wichtiger Baustein zur Vermeidung solcher Schäden. Deshalb schützen wir unsere Informationen (Daten und Dokumente) vor Verlust, Fälschung und unautorisiertem Zugriff.
<u>5.13</u> 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.	✓	Die Kennzeichnung von Dokumenten jeglicher Art ist geregelt.
<u>5.14</u> 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.	✓	Regeln für den transfer von Informationen sind definiert. Wo immer möglich werden verschlüsselte Verbindungen genutzt.
<u>5.15</u> 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.	✓	Das Grundprinzip besteht darin, dass der Zugang zu allen Systemen, Netzwerken, Diensten und Informationen verboten ist, solange er nicht einzelnen Benutzern oder Benutzergruppen ausdrücklich erlaubt wird. Es gibt ein entsprechendes Verfahren für die Verwaltung von Benutzern für System, Netzwerke und Dienste.
<u>5.16</u> Identity management The full life cycle of identities shall be managed.	✓	Die Ordner innerhalb der einzelnen Laufwerke sind durch individuelle Zugriffsrechte geschützt.

Control	Applicability	Justification
<u>5.17</u> Authentication information Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	✓	Der Zugriff auf ns-Produkte erfolgt über einen Webbrowser, in dem sich die Benutzer über ein zweistufiges Login (Benutzername und Passwort, SecureID-Token) authentifizieren müssen. Sämtliche Applikationen sind erst nach dieser Anmeldung abrufbar. Den Nutzern ist bewusst, dass die Authentifizierungsdaten persönlich sind und vertraulich behandelt werden müssen. Sie dürfen nicht notiert, nicht gespeichert oder gar anderen Personen mitgeteilt werden. Auch die verantwortlichen Systemadministratoren können das Passwort im Notfall nur neu setzen, aber nicht auslesen. Nicht personenbezogene Logindaten, z.B. für Serviceaccounts, werden in einem sicheren Passwortsafe dokumentiert und gespeichert. Der Zugang ist nur berechtigten Personen möglich.
<u>5.18</u> 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.	✓	Änderungen der Zugriffsrechte werden über den Servicedesk von Scheuss & Partner abgewickelt. Vor Durchführung einer Änderung muss die Einwilligung des Eigentümers eines Ordners, beziehungsweise der Geschäftsleitung eingeholt werden. Die entsprechenden Rechte sind von der entsprechenden Stelle zu autorisieren. Die Benutzerberechtigungen werden mindestens einmal jährlich überprüft. Beim Austritt werden die entsprechenden Berechtigungen gelöscht.
<u>5.19</u> 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.	✓	Anforderungen an die Lieferanten sind in der entsprechenden Richtlinie definiert. Neue Lieferanten durchlaufen ein initiales IS Assessment. Grundsätzlich, jedoch kontextabhängig, werden Lieferanten mit einer ISO/IEC 27001 Zertifizierung (oder ähnlichen Frameworks) bevorzugt.
<u>5.20</u> Addressing information security within supplier Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	✓	Die durch die Lieferanten aufgesetzten Verträge werden vor der Unterzeichnung gemeinsam an die jeweiligen Erfordernisse angepasst und es wird sichergestellt, dass die IS-Anforderungen an den Lieferanten berücksichtigt werden.
<u>5.21</u> 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 products and services supply chain.	✓	Die in den Verträgen ausgemachten IS Anforderungen gelten grundsätzlich für die gesamte Lieferkette.
<u>5.22</u> Monitoring, review and change management agreements of supplier services The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	✓	Sämtliche Lieferanten werden regelmässig überprüft. Der CTO überprüft die Kernlieferanten mindestens jährlich. Je nach Kritikalität können zusätzlich Lieferantenaudits durchgeführt werden. Die Verträge werden regelmässig durch die Geschäftsleitung überprüft.
<u>5.23</u> 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.	✓	Die IS Anforderungen an Cloud respektive SaaS Dienstleister sind bestimmt und werden im Rahmen des Lieferantenmanagements berücksichtigt.

Control	Applicability	Justification
<u>5.24</u> 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.	✓	Die Informationssicherheit soll möglichst umfassend gewährleistet werden. Dazu ist es nötig, mögliche Schwachstellen und Vorfälle frühzeitig zu erkennen und definierte Prozesse zu deren Behebung und entsprechender (Kunden-) Kommunikation einzuhalten und zu dokumentieren.
<u>5.25</u> 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.	✓	Jeder Informationssicherheitsvorfall wird durch den Head of IT und seinem Team bewertet. Je nach Ereignis wird auch der CTO oder der CISO eingeschaltet, welcher beim Assessment hilft.
<u>5.26</u> Response to information security incidents Information security incidents shall be responded to in accordance with the documented procedures.	✓	Der Head of IT und seinem Team sind für die Erarbeitung und Umsetzung der nötigen Massnahmen verantwortlich. Bei schwerwiegenden Informationssicherheitsvorfällen oder Datenschutzverletzungen muss der CTO, CISO und gegebenenfalls der Datenschutzverantwortliche beigezogen werden.
<u>5.27</u> Learning from information security incidents Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	✓	Der Head of IT prüft sämtliche Vorfälle, insbesondere jene, welche sich wiederholen (oder solche, die sich bei der nächsten Wiederholung zu einem erheblichen oder gar kritischen Vorfall steigern könnten). Zudem muss er alle Vorfälle analysieren (Feststellung des Typs, der Herkunft und der Kosten eines Vorfalls) und gegebenenfalls Vorbeugungs- oder Korrekturmassnahmen vorschlagen. Die Erkenntnisse werden zur Sensibilisierung relevanter Parteien über Managementbewertung und Mitarbeiterschulungen weitergegeben.
<u>5.28</u> Collection of evidence The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	✓	Grundsätzlich ist der Head of IT und sein Team für das identifizieren, sammeln und speichern von Beweismaterial zuständig. Bei erheblichen oder kritischen IS Vorfällen, sowie bei Datenschutzverletzungen kann respektive muss der CTO, sowie gegebenenfalls weitere Personen (z.B. CISO, Datenschutzverantwortlicher, etc.) miteinbezogen werden.
<u>5.29</u> Information security during disruption The organization shall plan how to maintain information security at an appropriate level during disruption.	✓	Bei den ns-Systemen wird in allen Bereichen auf eine hohe Verfügbarkeit geachtet. Um dies sicherzustellen, wurde ein Notfallbetriebskonzept erarbeitet, das den Eintritt eines Totalausfalls eines Standorts berücksichtigt.
<u>5.30</u> ICT readiness for business continuity ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	✓	Für die im BCM identifizierten kritischen Systeme wurden entsprechende Notfallszenarien definiert, welche regelmässig überprüft und getestet werden.
<u>5.31</u> 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.	✓	Der CISO stellt sicher, dass bei jeder wesentlichen Gesetzes- oder Vertragsänderung überprüft wird, ob das interne Vorgehen dieser entspricht. Bei einer Gesetzes- oder Vertragsänderung wird vom CISO und, wenn notwendig, von einem internen oder externen Experten die Relevanz geprüft.
<u>5.32</u> Intellectual property rights The organization shall implement appropriate procedures to protect intellectual property rights.	✓	Um einen transparenten Umgang mit den eigenen geistigen Eigentumsrechten und denen anderer zu gewährleisten, wurde eine entsprechende Richtlinie erstellt.

Control	Applicability	Justification
<u>5.33</u> Protection of records Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	✓	Um eine möglichst durchgängige Dokumentation all unserer Aktivitäten zu gewährleisten, schützen wir unsere Informationen vor Verlust, Fälschung und vor unautorisiertem Zugriff.
<u>5.34</u> Privacy and protection of PII 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.	✓	Die Privatsphäre und der Schutz von personenbezogener Information sind, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt und in den entsprechenden Richtlinien dokumentiert.
<u>5.35</u> 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.	✓	Das Managementsystem wird mindestens jährlich durch verschiedene interne und externe Experten überprüft. Nur so kann die Implementierung und Anwendung entsprechend den vorgegebenen Prozessen und Richtlinien wirkungsvoll kontrolliert werden.
<u>5.36</u> 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.	✓	Es werden regelmässig Schulungen und Kontrollen, sowie mindestens jährlich ein internes Audit nach ISO/IEC 27001 durchgeführt. Um die Sicherheit, Resilienz und Zuverlässigkeit unserer Systeme durch Angriffe aus dem Internet zu testen, werden jährliche Penetration Tests durch einen externen Dienstleister durchgeführt. Darüber hinaus finden jährlich mehrere Audits durch Kunden oder von Kunden beauftragten Drittparteien statt.
<u>5.37</u> Documented operating procedures Operating procedures for information processing facilities should be documented and made available to personnel who need them.	✓	Die Betriebsabläufe, insbesondere in der IT, sind umfassend dokumentiert.

6 People controls

Control	Applicability	Justification
6.1 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.	✓	Bereits vor einer Anstellung von Mitarbeitenden findet eine angemessene Überprüfung des neuen Personals statt. Potenzielle Kandidaten, die sich um eine Beschäftigung bewerben, werden einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.
6.2 Terms and conditions of employment The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	✓	Die Geschäftsleitung ist für die Einstellung eines neuen Mitarbeitenden verantwortlich. Die Stellenbeschreibung ist Bestandteil der Stellenausschreibung. Der Anstellungsvertrag mit der entsprechenden Funktion wird durch die Personaladministration erstellt.

Control	Applicability	Justification
6.3 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.	✓	Wir stellen sicher, dass alle Mitarbeitenden, die Informationssicherheitsbedrohungen und -bedenken sowie ihre Verantwortlichkeiten und Pflichten kennen, diese Kenntnisse regelmässig auffrischen, und dass sie entsprechend ausgestattet sind, um die organisationseigenen IS-Richtlinien bei ihrer normalen Arbeit zu befolgen, und das Risiko von menschlichen Fehlern zu reduzieren.
6.4 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.	✓	Jeder Mitarbeiter, der gegen die Regeln verstösst (sei es gegen den NSG-Kodex, den Arbeitsvertrag, firmeninterne Richtlinien, die Weisungen von Vorgesetzten oder externe Gesetze, Vorschriften und Regelungen), muss mit Konsequenzen rechnen. Die rechtlichen Grundlagen in der Schweiz sind das Obligationenrecht und das Arbeitsgesetz (ArG).
6.5 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.	✓	Ein Mitglied der Geschäftsleitung und der direkte Vorgesetzte führen zusammen mit dem austretenden Mitarbeiter und dem HR ein Austrittsgespräch. Dabei wird allfälliges Verbesserungspotenzial ermittelt sowie die Modalitäten (Rückgabe von Material und Dokumentationen, Sperrung von Zugangs- und Zugriffsrechten, Hinweis auf Schutz von Betriebsdaten etc.) geregelt. Es kann ein Kurzprotokoll über das Gespräch erstellt und im Mitarbeiterdossier abgelegt werden.
6.6 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.	✓	Anforderungen an die Vertraulichkeit sind sowohl für Mitarbeiter, wie auch für externe Parteien definiert.
6.7 Remote working Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	✓	Telearbeit wird auf Anfrage durch den CTO genehmigt. Dazu wird dem Mitarbeitenden der Zugriff via Citrix ermöglicht.
6.8 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.	✓	Jeder Mitarbeiter, Lieferant oder andere Dritte, welche in Kontakt zu Informationen oder Systemen der Organisation steht, muss jegliche Systemschwachstellen, Vorfälle oder Ereignisse, die zu einem möglichen Sicherheitsvorfall führen könnten, umgehend melden.

7 Physical controls

Control	Applicability	Justification
<u>7.1</u> Physical security perimeters Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	✓	Die Vorgaben zum Schutz der physischen Sicherheit sind dokumentiert. Das Schutzzonenkonzept definiert drei Schutzzonen.

Control	Applicability	Justification
<u>7.2</u> Physical entry Secure areas shall be protected by appropriate entry controls and access points.	✓	Die Räumlichkeiten der MMS sind entsprechend dem Schutzzonenkonzept mit verschiedenen Massnahmen gesichert. Die Besucherregelung stellt sicher, dass externe Parteien mit der nötigen Sorgfalt betreut werden, so dass keine Sicherheitsvorfälle entstehen.
<u>7.3</u> Securing offices, rooms and facilities Physical security for offices, rooms and facilities shall be designed and implemented.	✓	Die Räumlichkeiten der MMS sind für die Mitarbeiter mit eigenem Schlüssel zugänglich. Der Zutritt zu Sicherheitsbereichen, in denen sich besonders betriebswichtige Informationen befinden, ist eingeschränkt.
<u>7.4</u> Physical security monitoring Premises shall be continuously monitored for unauthorized physical access.	✓	Die Büroräumlichkeiten sind mit einer Alarmanlage gesichert. Wird ein Alarm ausgelöst, wird dieser durch einen externen Anbieter direkt an die Geschäftsleitung eskaliert.
<u>7.5</u> 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.	✓	Die externen und umweltbedingten Bedrohungen sind erfahrungsgemäss sehr gering. Nichtsdestotrotz wurde die grundlegende Notfallvorsorge und entsprechende Verantwortungen in einem Notfallkonzept definiert.
<u>7.6</u> Working in secure areas Security measures for working in secure areas shall be designed and implemented.	✓	Regeln für die Arbeit in Sicherheitszonen sind definiert.
<u>7.7</u> 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.	✓	Falls die berechnigte Person nicht an ihrem Arbeitsplatz ist, dürfen keine sensiblen Informationen auf dem Bildschirm angezeigt werden und der Zugang zu allen Systemen, zu denen die Person Zugangsberechtigung hat, muss gesperrt sein.
<u>7.8</u> Equipment siting and protection Equipment shall be sited securely and protected.	✓	Geräte werden nur in den Räumlichkeiten der MMS genutzt. Für mobile Geräte gelten spezielle Regeln.
<u>7.9</u> Security of assets off-premises Off-site assets shall be protected.	✓	Die Nutzung der IT ist in verschiedenen Nutzungsreglementen IT geregelt, welche die Mitarbeiter bei der Einstellung erhalten und deren Kenntnis sie mit Unterschrift bestätigen.
<u>7.10</u> 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.	✓	Die Verwendung von Wechselmedien oder persönliche Cloud-Anwendungen ist für einen reibungslosen und flexiblen Ablauf unserer Tätigkeiten unerlässlich. Aus diesem Grund ist der Zugriff auf die eigenen beziehungsweise organisationseigenen Daten im Nutzungsreglement IT geregelt. Zur Datensicherheit gehört auch die sichere Entsorgung beziehungsweise Lagerung nicht mehr benötigter Datenträger und von Rechnern, Notebooks etc. Diese werden zentral über die IT entsorgt. Ausdrucke mit vertraulichen Massnahmen werden geschreddert. Diese Regeln gelten sowohl für die Verwendung als auch den Transport vertraulicher Daten auf Speichermedien und persönlichen Clouds.
<u>7.11</u> Supporting utilities Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	✓	Bei einem Ausfall des Standorts können die Mitarbeiter, über ihre Laptops standortunabhängig (mit kleineren Einschränkungen) auf die Server-Infrastruktur (ns-Systeme) zugreifen. Der E-Mail-Verkehr ist über Office 365 gelöst und somit auch bei einem Ausfall des Standorts funktionstüchtig.

Control	Applicability	Justification
<u>7.12</u> Cabling security Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	✓	Die Kabel sind nur innerhalb des Gebäudes.
<u>7.13</u> Equipment maintenance Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	✓	Der Support der Geräte erfolgt über die Scheuss & Partner.
<u>7.14</u> 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.	✓	Zur Datensicherheit gehört auch die sichere Entsorgung beziehungsweise Lagerung nicht mehr benötigter Datenträger von Rechnern, Notebooks etc. Diese werden zentral über die IT entsorgt. Ausdrucke mit vertraulichen Informationen werden geschreddert.

8 Technological controls

Control	Applicability	Justification
<u>8.1</u> User endpoint devices Information stored on, processed by or accessible via user end point devices shall be protected.	✓	Die Nutzung der IT ist in verschiedenen Nutzungsreglementen geregelt, welche die Mitarbeiter bei der Einstellung erhalten und deren Kenntnis sie mit Unterschrift bestätigen.
<u>8.2</u> Privileged access rights The allocation and use of privileged access rights shall be restricted and managed.	✓	Administrativen Usern ist es nicht möglich sich direkt am System anzumelden. Vorgängig ist die Anmeldung mittels des regulären, persönlichen, nicht privilegierten Users des einzelnen Administrators nötig. Erst nach erfolgreicher Authentifikation steht dem berechtigten User die Möglichkeit offen, sich via RDP für administrative Tätigkeiten auf den ns-Systemen anzumelden.
<u>8.3</u> Information access restriction Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	✓	Die Ordner innerhalb der einzelnen Laufwerke sind durch individuelle Zugriffsrechte geschützt.
<u>8.4</u> Access to source code Read and write access to source code, development tools and software libraries shall be appropriately managed.	✓	Der Zugriff auf den Software-Quellcode wird streng kontrolliert, um das Hinzufügen nicht autorisierter Funktionen zu verhindern und unbeabsichtigte Änderungen zu vermeiden, sowie um die Vertraulichkeit des wertvollen geistigen Eigentums zu gewährleisten.
<u>8.5</u> Secure authentication Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	✓	Zugriffe sind immer nur mittels Benutzername und Passwort möglich. Von aussen muss ein weiteres Element benutzt werden (2FA).
<u>8.6</u> Capacity management The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	✓	Die entsprechenden Systeme werden überwacht und es erfolgt eine frühzeitige Anpassung der Systeme.
<u>8.7</u> Protection against malware Protection against malware shall be implemented and supported by appropriate user awareness.	✓	Auf den relevanten Systemen der ns-Systeme wird eine in den Hypervisor integrierte Antivirenlösung eingesetzt. Auf allen internen Clients, sowie auf den Windowsservern ist eine marktübliche Antivirenlösung installiert.

Control	Applicability	Justification
<u>8.8</u> 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.	✓	Informationen über technische Schwachstellen werden regelmässig eingeholt, daraus folgernd Ziele definiert und geeignete Massnahmen festgelegt. Um die Sicherheit, Resilienz und Zuverlässigkeit unserer Systeme durch Angriffe aus dem Internet zu testen, werden jährliche Penetration Tests durch einen externen Dienstleister durchgeführt. Darüber hinaus finden jährlich mehrere Audits durch Kunden oder von Kunden beauftragten Drittparteien statt.
<u>8.9</u> Configuration management Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	✓	IS Anforderungen an das Konfigurationsmanagement, zum Sicherstellen von korrekten und autorisierten Änderungen, sind in der entsprechenden Richtlinie definiert.
<u>8.10</u> Information deletion Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	✓	Das aktive und zeitnahe Löschen von Informationen bei der Verarbeitung und Speicherung auf Informationssystemen, insbesondere das Einhalten der Löschfristen bei persönlich identifizierbaren Informationen (PII), muss den Anforderungen der relevanten Gesetze und Vorschriften genügen.
<u>8.11</u> 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.	✓	Bei der systematischen und ausgedehnten Verarbeitung von persönlich identifizierbaren Informationen (PII), sollen diese Daten entsprechend maskiert werden. Eine solche Verarbeitung, sowie die Umsetzung der Datenmaskierung, muss jeweils vom CTO schriftlich freigegeben werden.
<u>8.12</u> Data leakage prevention Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	✓	Um Datenlecks frühzeitig zu identifizieren und zu verhindern, kommen verschiedene Massnahmen zum Einsatz. Die Mitarbeiter kontinuierlich im Umgang von klassifizierter Information geschult. Ausserdem sorgen die vielfältigen Überwachungstätigkeiten und der effiziente IS Incident Management Prozess für eine effektive Data Leakage Prevention.
<u>8.13</u> 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.	✓	Für die Gewährleistung der Betriebssicherheit werden unter Befolgung der Datensicherungsrichtlinie regelmässige Backups angelegt.
<u>8.14</u> Redundancy of information processing facilities Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	✓	Bei den ns-Systemen wird in allen Bereichen auf eine hohe Verfügbarkeit geachtet. Um dies sicherzustellen, wurden die relevanten Bereiche identifiziert und entsprechend redundant aufgebaut.
<u>8.15</u> Logging Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	✓	Es werden Ereignisprotokolle geführt, welche im Bedarfsfall ausgewertet werden. Die Logdaten sind auf dem zentralen Auswertungsserver vor Manipulationen geschützt.
<u>8.16</u> Monitoring activities Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	✓	Es findet eine umfassende Überwachung der Netzwerke, Systeme und Applikationen durch verschiedene Massnahmen statt.

Control	Applicability	Justification
<u>8.17</u> Clock synchronization The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	✓	Alle System laufen mit der gleichen Uhrzeit. Dies ist insbesondere relevant für die Auswertung bei Vorfällen.
<u>8.18</u> 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.	✓	Es dürfen nur die für die Durchführung der beruflichen Tätigkeiten notwendigen Programme genutzt werden. Die zur Verfügung stehenden Programme funktionieren einwandfrei und ermöglichen die vertragsmässige Servicebereitstellung.
<u>8.19</u> Installation of software on operational systems Procedures and measures shall be implemented to securely manage software installation on operational systems.	✓	Es dürfen nur die für die Durchführung der beruflichen Tätigkeiten notwendigen Programme installiert sein und genutzt werden. Nur Administratoren können Software installieren. Dies erfolgt jeweils über die Scheuss & Partner.
<u>8.20</u> Networks security Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	✓	Der Aufbau des Netzwerks und die Implementation entsprechender Firewallregeln zwischen den einzelnen Netzwerkzonen verhindert den Zugriff auf nicht zum Zugriff vorgesehene Ressourcen.
<u>8.21</u> Security of network services Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	✓	Wo immer möglich werden verschlüsselte Verbindungen genutzt. Zugänge werden geschützt und die Dienstleistungserbringung durch entsprechende SLAs abgesichert.
<u>8.22</u> Segregation of networks Groups of information services, users and information systems shall be segregated in the organization's networks.	✓	Die Netzwerke sind segmentiert und die Firewallregeln stellen sicher, dass kein unautorisierter Zugriff auf Netzwerksegmente stattfindet.
<u>8.23</u> Web filtering Access to external websites shall be managed to reduce exposure to malicious content.	✓	Die Firewall stellt eine eigene Web Filtering Lösung bereit, welche durch Filter-Kategorien und individuell angepasster Sperrlisten sämtliche dahinterliegenden Netzwerke und Geräte schützt.
<u>8.24</u> Use of cryptography Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	✓	Der Zugang zu den ns-Systemen ist ausschliesslich über verschlüsselte Verbindungen möglich. Die genutzten Verschlüsselungsverfahren entsprechen dem aktuellen Stand der Technik. Der Head of IT ist für die Vorgabe zur Schlüsselverwaltung verantwortlich.
<u>8.25</u> Secure development life cycle Rules for the secure development of software and systems shall be established and applied.	✓	Über den gesamten Software-Entwicklungszyklus ist ein angemessener Schutz des jeweiligen Entwicklungsstandes sichergestellt.
<u>8.26</u> Application security requirements Information security requirements shall be identified, specified and approved when developing or acquiring applications.	✓	Die Schutzanforderungen für Anwendungsdienste und deren Umgang mit Informationen sind definiert. Es sollen möglichst wenig Transaktionen eingesetzt werden. Die Auftragsverarbeitung soll wenn möglich wiederholbar mit dem gleichen Auftrag sein. Das bedeutet, dass bei einem Fehler der Auftrag nochmals ausgeführt wird und die vorherigen Veränderungen überschrieben werden.
<u>8.27</u> Secure system architecture and engineering principles Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	✓	Die Entwicklung wird von einem verteilten Team verantwortet. Das Team arbeitet nach der agilen Vorgehensmethodik Scrum.
<u>8.28</u> Secure coding Secure coding principles shall be applied to software development.	✓	Das Entwicklerteam verfolgt einen strikten Security by Design Ansatz, welcher ausführlich im Produktentwicklungsprozess dokumentiert ist.

Control	Applicability	Justification
<u>8.29</u> Security testing in development and acceptance Security testing processes shall be defined and implemented in the development life cycle.	✓	Es werden bei jeder neuen Entwicklung automatisierte Test für das neue Feature erstellt. Zusätzlich werden die einzelnen Codeteile mit Tests sowohl automatisiert als auch manuell getestet. Systemabnahmetests und deren Umfang werden vom Head of Software Development und vom Product Owner festgelegt. Dies geschieht anhand der vorgenommenen Änderungen am System, durch die die abzuarbeitenden Punkte bestimmt werden.
<u>8.30</u> Outsourced development The organization shall direct, monitor and review the activities related to outsourced system development.	✓	Allfällige externen Entwickler werden vollständig in das Team integriert und nehmen auch am Workshop für sicheres Entwickeln teil. Alle externen Entwickler arbeiten direkt in unserem Code-Repository.
<u>8.31</u> Separation of development, test and production environments Development, testing and production environments shall be separated and secured.	✓	Die Entwicklungsumgebung ist bei jedem Entwickler lokal auf seinem Rechner. Es wird dort direkt aus dem Entwicklungstool auf die Datenbank zugegriffen. Die Test- und Liveumgebungen sind geschützt und nur autorisierte Benutzer können darauf zugreifen.
<u>8.32</u> Change management Changes to information processing facilities and information systems shall be subject to change management procedures.	✓	Jede Änderung an einem betrieblichen oder Produktiv-System muss gemäss dem Change Prozess durchgeführt werden. Es dürfen nur berechnete User Änderungen übermitteln. Bei der Abnahme eines neuen Release, welcher auf die Liveumgebung ausgerollt werden soll, wird kontrolliert, ob die Systemabnahme ordnungsgemäss durchgeführt wurde. Anhand definierter Aufgaben wird überprüft, ob mit den neuen Versionen die nötigen Anforderungen für die Sicherheit des System eingehalten wurden.
<u>8.33</u> Test information Test information shall be appropriately selected, protected and managed.	✓	Sämtliche Tests erfolgen in einer möglichst praxisnahen, geschützten und von der Live-Umgebung getrennten Umgebung. Die Testdaten werden nach der Kontrolle wieder gelöscht.
<u>8.34</u> 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.	✓	Es ist wichtig, die Systeme regelmässig zu überprüfen. Nur so kann die Implementierung und Anwendung entsprechend den vorgegebenen Prozessen und IS-Richtlinien wirkungsvoll kontrolliert werden. Entsprechende Planungen werden gemäss den Vorgaben vorgenommen.

Zertifikat



Die Zertifizierungsstelle von Swiss Safety Center AG
bescheinigt, dass die Firma

publiccloud ag
Saatlenstrasse 13
CH-8051 Zürich



für den Geltungsbereich

**Betrieb von Cloud-Rechenzentren, Verwaltung von Multi-
Cloud Lösungen und Erbringung von gemanagten IT-Services**

ein **Informationssicherheitsmanagementsystem (ISMS)**
erfolgreich anwendet nach

ISO/IEC 27001:2022

Erklärung zur Anwendbarkeit:	02.05.2024
Registriernummer:	15-145-903
Erstzertifizierung:	29.07.2015
Rezertifizierung:	04.07.2024
Gültig ab:	29.07.2024
Gültig bis:	28.07.2027



Heinrich A. Bieler
Leiter der Zertifizierungsstelle

Wallisellen, 04.07.2024

Swiss Safety Center AG, Certifications
Richtstrasse 15, CH-8304 Wallisellen

Ein Unternehmen der SVTI-Gruppe, Mitglied des TÜV-Verbands.



Control	Thema	Massnahme	Anwendbar	Begründung
A.5.01	Informationssicherheitsrichtlinien	Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.	JA	
A.5.02	Informationssicherheitsrollen und -verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.	JA	
A.5.03	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.	JA	
A.5.04	Verantwortlichkeiten der Leitung	Die Leitung muss von dem gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.	JA	
A.5.05	Kontakt mit Behörden	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.	JA	
A.5.06	Kontakt mit speziellen Interessensgruppen	Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.	JA	
A.5.07 (neu)	Bedrohungsintelligenz	Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.	JA	
A.5.08	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss in das Projektmanagement integriert werden.	JA	
A.5.09	Inventar der Informationen und anderen damit verbundenen Werten	Ein Inventar der Informationen und anderen damit verbundenen Werten, einschliesslich der Eigentümer, muss erstellt und gepflegt	JA	
A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten müssen aufgestellt, dokumentiert und angewendet werden.	JA	

A.5.11	Rückgabe von Werten	Das Personal und gegebenenfalls andere interessierte Parteien müssen alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.	JA
A.5.12	Klassifizierung von Information	Informationen müssen entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.	JA
A.5.13	Kennzeichnung von Information	Ein angemessener Satz von Verfahren zur Kennzeichnung von Information muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und	JA
A.5.14	Informationsübertragung	Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.	JA
A.5.15	Zugangssteuerung	Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Werte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.	JA
A.5.16	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.	JA
A.5.17	Informationen zur Authentifizierung	Die Zuweisung und Verwaltung von Authentifizierungsinformationen muss durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.	JA
A.5.18	Zugangsrechte	Zugangsrechte zu Informationen und anderen zugehörigen Werten müssen in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.	JA
A.5.19	Informationssicherheit in Lieferantenbeziehungen	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu	JA

A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Je nach Art der Lieferantenbeziehung müssen die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.	JA
A.5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.	JA
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Die Organisation muss regelmässig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und	JA
A.5.23 (neu)	Informationssicherheit für die Nutzung von Cloud-Diensten	Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt	JA
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Die Organisation muss die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.	JA
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Die Organisation muss Ereignisse im Bereich der Informationssicherheit beurteilen und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden müssen.	JA
A.5.26	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.	JA
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse müssen zur Verstärkung und Verbesserung der Informationssicherheitsmassnahmen genutzt werden.	JA
A.5.28	Sammeln von Beweismaterial	Die Organisation muss Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismaterial im Zusammenhang mit Informationssicherheitsvorfällen einführen und	JA
A.5.29	Informationssicherheit bei Störungen	Die Organisation muss planen, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau gehalten werden kann.	JA

A.5.30 (neu)	IKT-Bereitschaft für Business Continuity	Die IKT-Bereitschaft muss auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.	JA
A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen müssen ermittelt, dokumentiert und auf dem neuesten Stand gehalten	JA
A.5.32	Geistige Eigentumsrechte	Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.	JA
A.5.33	Schutz von Aufzeichnungen	Aufzeichnungen müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.	JA
A.5.34	Datenschutz und Schutz personenbezogener Daten (pbD)	Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.	JA
A.5.35	Unabhängige Überprüfung der Informationssicherheit	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschliesslich der Mitarbeiter, Prozesse und Technologien, müssen auf unabhängige Weise in planmässigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.	JA
A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen muss regelmässig überprüft werden.	JA
A.5.37	Dokumentierte Betriebsabläufe	Die Betriebsverfahren für Informationsverarbeitungsanlagen müssen dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.	JA

A.6.01	Sicherheitsüberprüfung	Alle Personen, die in die Belegschaft aufgenommen werden, müssen vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und diese Überprüfung muss in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken stehen.	JA
A.6.02	Beschäftigungs- und Vertragsbedingungen	In den arbeitsvertraglichen Vereinbarungen müssen die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.	JA
A.6.03	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Das Personal der Organisation und relevante interessierte Parteien müssen ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmässige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet	JA
A.6.04	Massregelungsprozess	Ein Massregelungsprozess muss formalisiert und kommuniziert werden, um Massnahmen gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoss gegen die Informationssicherheitspolitik begangen haben.	JA
A.6.05	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, müssen festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien	JA
A.6.06	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, müssen identifiziert, dokumentiert, regelmässig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.	JA

A.6.07	Telearbeit	Es müssen Sicherheitsmassnahmen ergriffen werden, wenn Mitarbeiter extern arbeiten, um Informationen zu schützen, die ausserhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.	JA
A.6.08	Meldung von Informationssicherheitsereignissen	Die Organisation muss einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig	JA
A.7.01	Physische Sicherheitsperimeter	Zum Schutz von Bereichen, in denen sich andere zugehörige Werte befinden, müssen Sicherheitsperimeter festgelegt und verwendet	JA
A.7.02	Physischer Zutritt	Sicherheitsbereiche müssen durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.	JA
A.7.03	Sichern von Büros, Räumen und Einrichtungen	Die physische Sicherheit für Büros, Räume und Einrichtungen muss konzipiert und umgesetzt werden.	JA
A.7.04 (neu)	Physische Sicherheitsüberwachung	Die Räumlichkeiten müssen ständig auf unbefugten physischen Zugang überwacht werden.	JA
A.7.05	Schutz vor physischen und umweltbedingten Bedrohungen	Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur muss konzipiert und umgesetzt werden.	JA
A.7.06	Arbeiten in Sicherheitsbereichen	Es müssen Sicherheitsmassnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.	JA
A.7.07	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Es müssen klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.	JA
A.7.08	Platzierung und Schutz von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen sicher und geschützt aufgestellt werden.	JA
A.7.09	Sicherheit von Werten ausserhalb der Räumlichkeiten	Werte ausserhalb des Standorts müssen geschützt werden.	JA

A.7.10	Speichermedien	Speichermedien müssen während ihres gesamten Lebenszyklus - Erwerb, Verwendung, Transport und Entsorgung - in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.	JA	
A.7.11	Versorgungseinrichtungen	Informationsverarbeitungseinrichtungen müssen vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.	JA	
A.7.12	Sicherheit der Verkabelung	Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Unterbrechung, Störung oder Beschädigung geschützt werden.	JA	
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.	JA	
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.	JA	
A.8.01	Endpunktgeräte des Benutzers	Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.	JA	
A.8.02	Privilegierte Zugangsrechte	Zuteilung und Gebrauch von privilegierten Zugangsrechten müssen eingeschränkt und verwaltet werden.	JA	
A.8.03	Informationszugangsbeschränkung	Der Zugang zu Informationen und anderen zugehörigen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.	JA	
A.8.04	Zugriff auf den Quellcode	Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken müssen angemessen verwaltet werden.	NEIN	kommt nicht vor
A.8.05	Sichere Authentifizierung	Sichere Authentifizierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert	JA	

A.8.06	Kapazitätssteuerung	Die Nutzung von Ressourcen muss überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.	JA	
A.8.07	Schutz gegen Schadsoftware	Schutz gegen Schadsoftware muss umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.	JA	
A.8.08	Handhabung von technischen Schwachstellen	Es müssen Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.	JA	
A.8.09 (neu)	Konfigurationsmanagement	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.	JA	
A.8.10 (neu)	Löschung von Informationen	Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, müssen gelöscht werden, wenn sie nicht mehr benötigt werden.	JA	
A.8.11 (neu)	Datenmaskierung	Die Datenmaskierung muss in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden	NEIN	kommt nicht vor
A.8.12 (neu)	Verhinderung von Datenlecks	Massnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.	JA	
A.8.13	Sicherung von Information	Sicherungskopien von Informationen, Software und Systemen müssen in Übereinstimmung mit den vereinbarten themenspezifischen Richtlinien für Datensicherungen aufbewahrt und regelmässig geprüft	JA	
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert werden.	JA	
A.8.15	Protokollierung	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.	JA	

A.8.16 (neu)	Überwachung von Aktivitäten	Netzwerke, Systeme und Anwendungen müssen auf unübliches Verhalten überwacht und geeignete Massnahmen müssen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.	JA
A.8.17	Uhrensynchronisation	Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit zugelassenen Zeitquellen synchronisiert werden.	JA
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmassnahmen zu umgehen, muss eingeschränkt und streng überwacht werden.	JA
A.8.19	Installation von Software auf Systemen im Betrieb	Es müssen Verfahren und Massnahmen umgesetzt werden, um die Installation von Software auf Betriebssystemen sicher zu verwalten.	JA
A.8.20	Netzwerksicherheit	Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen	JA
A.8.21	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste müssen ermittelt, umgesetzt und überwacht werden.	JA
A.8.22	Trennung von Netzwerken	Informationsdienste, Benutzer und Informationssysteme müssen in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.	JA
A.8.23 (neu)	Webfilterung	Der Zugang zu externen Websites muss verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.	JA
A.8.24	Verwendung von Kryptographie	Es müssen Regeln für den wirksamen Einsatz von Kryptographie, einschliesslich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.	JA
A.8.25	Lebenszyklus einer sicheren Entwicklung	Regeln für die sichere Entwicklung von Software und Systemen müssen festgelegt und angewendet werden.	JA
A.8.26	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit müssen bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.	JA
A.8.27	Sichere Systemarchitektur und technische Grundsätze	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme müssen festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet	JA

A.8.28 (neu)	Sicheres Coding	Bei der Softwareentwicklung müssen die Grundsätze der sicheren Kodierung angewandt werden.	NEIN	kommt nicht vor
A.8.29	Sicherheitsprüfung in Entwicklung und Abnahme	Sicherheitsprüfverfahren müssen definiert und in den Entwicklungslebenszyklus integriert werden.	JA	
A.8.30	Ausgegliederte Entwicklung	Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgegliederten Systementwicklung leiten, überwachen und	NEIN	kommt nicht vor
A.8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	Entwicklungs-, Prüf- und Produktionsumgebungen müssen getrennt und gesichert werden.	JA	
A.8.32	Änderungssteuerung	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.	JA	
A.8.33	Prüfinformationen	Die Prüfinformationen müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.	NEIN	kommt nicht vor
A.8.34	Schutz der Informationssysteme während der Überwachungsprüfung	Auditprüfungen und andere Sicherheitstätigkeiten, die eine Beurteilung der betrieblichen Systeme beinhalten, müssen zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.	JA	

CERTIFICATE

No. 040-ISMS-24

Hereby we certify that the Management System of

GREEN DATACENTER AG

Industriestrasse 33 - 5242 - Lupfig (Switzerland)

Operating Offices:

Unterrohrstrasse 4 - 8952 - Schlieren (Zürich, Switzerland)

Cherstrasse 4 - 8152 - Glattbrugg (Switzerland)

Niederhaslistrasse 6 - 8157 - Dielsdorf (Switzerland)

Is according to: Information security, cybersecurity and privacy protection —
Information security management systems

ISO/IEC 27001:2022

for the following scope:

Datacenter Services

SOA Version	First Issue Date	Date of modification	Certificate expiration date
Version 9 vom 17.01.2024	15/07/2015	03/06/2024	15/07/2027



For the Certification Body
SV Certification Sro



(Gaetano Spera CEO SV CERT.)

The validity of the certificate is subject to periodic annual surveillance and a complete review of the System every three years. The use and validity of this certificate are subject to compliance with the Certification Regulations of SV Certification..



BUREAU
VERITAS

AE Corp NL B.V.

Van der Madeweg 12-14A, Postbus 94018, 1090 GA Amsterdam, 1114 AM, Amsterdam, The Netherlands

Bureau Veritas Certification certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

STANDARD

ISO/IEC 27001:2022

SCOPE

Operational management processes and procedures of the organisation, employees and the physical locations included in the certified list

Statement of Applicability: Version 4 (Approved 08.04.2025)

Subject to the continued satisfactory operation of the organisation's Management System, this certificate is valid until: 20-07-2028

Certification / Recertification cycle start date: 12-08-2025

Original cycle start date: 21-07-2022

Expiry date of previous cycle: -

Certification / Recertification audit date: -

Certificate Number: FIHSK27133

Version 1, Revision date: 12-08-2025

**Salla Punkari, Certification Manager,
Bureau Veritas Certification Finland**



The SoA (statement of applicability) as a source of control set that are determined in accordance with ISO/IEC 27001:2022, section 6.1.3. d)
The SoA itself is not certified

Bureau Veritas Branch office for Finland, Sörnäisten rantatie 29, FI-00500 Helsinki, Finland

Further clarifications regarding the scope of this certificate and the applicability of the Management System requirements may be obtained by consulting the organisation. To check the validity of this certificate please call, tel. +358 10 830 8630.



BUREAU
VERITAS

AE Corp NL B.V.

STANDARD

ISO/IEC 27001:2022

SCOPE

Site	Address	Scope
Head Office	AE Corp NL B.V. Van Der Madeweg 12-14a, 1090 GA Amsterdam 1114 AM-Amsterdam Netherlands	Operational management processes and procedures of the organisation, employees and the physical locations included in the certified list
Site 1	AE Corp NL B.V. Wiebestr. 46-49, 10553 Berlin Germany	Local Management, operations
Site 2	AE Corp NL B.V. Mercuriusstraat 30, Zaventem, Brussels 1930 Belgium	
Site 3	AE Corp NL B.V. Badenerstrasse 820, 8048 Zurich Switzerland	
Site 4	AE Corp NL B.V. & RS Colocation Services Germany GmbH Obenhauptstr 1. C, 22335 Hamburg	
Site 5	UK London - Manning House 161 Hammersmith Road, London, W6 8BS	
Site 6	RS Colocation Services Germany GmbH, Obenhauptstr 1. C, 22335 Hambu	
Site 7	Calle Acero N. 5-9, 08038 Barcelona (Zona Franca)	

Certificate Number: FIHSK27133

Version 1, Revision date: 12-08-2025

Salla Punkari, Certification Manager,
Bureau Veritas Certification Finland



Bureau Veritas Branch office for Finland, Sörnäisten rantatie 29, FI-00500 Helsinki, Finland

Further clarifications regarding the scope of this certificate and the applicability of the Management System requirements may be obtained by consulting the organisation. To check the validity of this certificate please call, tel. +358 10 830 8630.



BUREAU
VERITAS

AE Corp NL B.V.

STANDARD

ISO/IEC 27001:2022

SCOPE

Site	Address	Scope
Site 8	AMS002- Luchtvaartstraat, Unit 1C and Unit 1B, Luchtvaartstraat, 1059 CA Amsterdam	Local Management, operations
Site 9	AMS Boeing Avenue 53, Schiphol-Rijk, 1119 PE	
Site 10	LIN001 Milan, Viale Lancetti, 23, 20158 Milan	
Site 11	BRU001 Brussels Mercuriusstraat 30, Zaventem, Brussels 1930	

Certificate Number: FIHSK27133

Version 1, Revision date: 12-08-2025

Salla Punkari, Certification Manager,
Bureau Veritas Certification Finland



Bureau Veritas Branch office for Finland, Sörnäisten rantatie 29, FI-00500 Helsinki, Finland

Further clarifications regarding the scope of this certificate and the applicability of the Management System requirements may be obtained by consulting the organisation. To check the validity of this certificate please call, tel. +358 10 830 8630.



Certificate



Certificate number: 2013-009

Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006-1:2024, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27001:2022

Issue date of certificate: November 25, 2025

Re-issue date of certificate: August 24, 2026

Expiration date of certificate: November 30, 2028

Last certification cycle expiration date: November 30, 2025

EY CertifyPoint will, according to the certification agreement dated July 16, 2024, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2025.01 dated August 29, 2025, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

DocuSigned by:

Jatin Sehgal

3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certification examination was conducted by Ernst & Young CertifyPoint B.V., an independent entity from Ernst & Young LLP that performed a separate System and Organization Controls 3 (SOC 3) Report issued semiannually in accordance with the AICPA Attestation Standards on the same subject matter included in the scoping section of this ISO Certification. That report may be found on the AWS Compliance Programs website.

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V., located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Amazon Web Services, Inc.

Scope for certificate 2013-009

The scope of this ISO/IEC 27001:2022 certification is bounded by the Information Security Management System (ISMS) that applies to specified services of Amazon Web Services, Inc. and specified facilities as listed below. The ISMS is centrally managed out of Amazon Web Services, Inc. headquarter in Seattle, Washington, United States of America.

The in-scope applications, systems, people, and processes are globally implemented and operated by teams out of an explicit set of facilities that comprise Amazon Web Services, Inc. and are specifically defined in the scope and bounds.

The Amazon Web Services, Inc. ISMS scope includes the services as mentioned on <https://aws.amazon.com/compliance/iso-certified/>, the locations and Supporting Resources are stated in the following section of this certificate.

The Information Security Management System mentioned in the above scope is restricted as defined in "AWS Integrated Information Management System (IIMS) Manual" version 2026.06, dated July 13, 2026.

This scope is only valid in connection with certificate 2013-009.

Amazon Web Services, Inc.

Scope for certificate 2013-009

Locations in scope:

AWS Services are offered and available across multiple geographic regions around the world. The scope of AWS infrastructure includes corporate headquarters, data center facilities, network and server hardware, and resources which support the datacenter operations. AWS data centers house the hardware supporting the AWS Services listed above.

AWS Data center locations in:

- ▶ Australia: Asia Pacific (Sydney) (ap-southeast-2) (12 sites), Asia Pacific (Melbourne) (ap-southeast-4) (5 sites)
- ▶ Bahrain: Middle East (Bahrain) (me-south-1) (3 sites)
- ▶ Brazil: South America (São Paulo) (sa-east-1) (12 sites)
- ▶ Canada: Canada (Central) (ca-central-1) (8 sites), Canada West (Calgary) (ca-west-1) (3 sites)
- ▶ England: Europe (London) (eu-west-2) (18 sites)
- ▶ EU: AWS European Sovereign Cloud (Germany) (eusc-de-east-1) (5 sites)
- ▶ France: Europe (Paris) (eu-west-3) (14 sites)
- ▶ Germany: Europe (Frankfurt) (eu-central-1) (27 sites)
- ▶ Hong Kong: Asia Pacific (ap-east-1) (8 sites)
- ▶ India: Asia Pacific (Mumbai) (ap-south-1) (22 sites), Asia Pacific (Hyderabad) (ap-south-2) (6 sites)
- ▶ Indonesia: Asia Pacific (Jakarta) (ap-southeast-3) (6 sites)
- ▶ Ireland: Europe (Ireland) (eu-west-1) (30 sites)
- ▶ Israel: Israel (Tel Aviv) (il-central-1) (4 sites)
- ▶ Italy: Europe (Milan) (eu-south-1) (11 sites)
- ▶ Japan: Asia Pacific (Tokyo) (ap-northeast-1) (21 sites), Asia Pacific (Osaka) (ap-northeast-3) (6 sites)
- ▶ Malaysia: Asia Pacific (Malaysia) (ap-southeast-5) (8 sites)
- ▶ Mexico: Mexico (Central) (mx-central-1) (3 sites)
- ▶ New Zealand: Asia Pacific (New Zealand) (ap-southeast-6) (4 sites)
- ▶ Singapore: Asia Pacific (Singapore) (ap-southeast-1) (20 sites)
- ▶ South Africa: Africa (Cape Town) (af-south-1) (3 sites)
- ▶ South Korea: Asia Pacific (Seoul) (ap-northeast-2) (13 sites)
- ▶ Spain: Europe (Spain) (eu-south-2) (6 sites)
- ▶ Sweden: Europe (Stockholm) (eu-north-1) (6 sites)
- ▶ Switzerland: Europe (Zurich) (eu-central-2) (4 sites)
- ▶ Taiwan: Asia Pacific (Taipei) (ap-east-2) (6 sites)
- ▶ Thailand: Asia Pacific (Thailand) (ap-southeast-7) (3 sites)
- ▶ United Arab Emirates: Middle East (UAE) (me-central-1) (3 sites)

This scope is only valid in connection with certificate 2013-009.

Amazon Web Services, Inc.

Scope for certificate 2013-009

- ▶ United States: US East (Northern Virginia) (us-east-1) (136 sites), US East (Ohio) (us-east-2) (48 sites), US West (Oregon) (us-west-2) (88 sites), US West (Northern California) (us-west-1) (8 sites), AWS GovCloud (US-East) (us-gov-east-1) (18 sites), AWS GovCloud (US-West) (us-gov-west-1) (24 sites)

AWS Edge locations in:

- | | |
|-------------------------------------|--|
| ▶ Amsterdam, Netherlands (3 sites) | ▶ Dubai, United Arab Emirates (2 sites) |
| ▶ Anyang-si, South Korea | ▶ Dublin, Ireland (3 sites) |
| ▶ Ashburn, United States (3 sites) | ▶ Dusseldorf, Germany |
| ▶ Atlanta, United States (4 sites) | ▶ El Segundo, United States (2 sites) |
| ▶ Auckland, New Zealand (2 sites) | ▶ Elk Grove Village, United States |
| ▶ Aurora, United States | ▶ Espoo, Finland |
| ▶ Ballerup, Denmark | ▶ Fortaleza, Brazil |
| ▶ Bang Chalong, Thailand | ▶ Frankfurt, Germany (2 sites) |
| ▶ Bangalore, India | ▶ Franklin, United States |
| ▶ Bangkok, Thailand | ▶ Fujairah, United Arab Emirates (2 sites) |
| ▶ Barcelona, Spain | ▶ General Pacheco, Argentina |
| ▶ Barka, Oman | ▶ Greenwood Village, United States (2 sites) |
| ▶ Berlin, Germany (2 sites) | ▶ Haifa, Israel |
| ▶ Bluffdale, United States | ▶ Hamburg, Germany (2 sites) |
| ▶ Bogotá, Colombia (2 sites) | ▶ Hanoi, Vietnam (2 sites) |
| ▶ Boston, United States | ▶ Helsinki, Finland |
| ▶ Brisbane, Australia | ▶ Hillsboro, United States (2 sites) |
| ▶ Brussels, Belgium | ▶ Ho Chi Minh, Vietnam |
| ▶ Bucharest, Romania | ▶ Houston, United States |
| ▶ Budapest, Hungary | ▶ Huechuraba, Chile |
| ▶ Caba, Argentina | ▶ Inzai, Japan |
| ▶ Cairo, Egypt | ▶ Irvine, United States |
| ▶ Canberra, Australia (2 sites) | ▶ Istanbul, Turkey (2 sites) |
| ▶ Cape Town, South Africa (3 sites) | ▶ Jakarta, Indonesia (3 sites) |
| ▶ Chandler, United States | ▶ Jeddah, Saudi Arabia |
| ▶ Chennai, India (2 sites) | ▶ Johannesburg, South Africa (2 sites) |
| ▶ Chicago, United States (4 sites) | ▶ Kansas City, United States |
| ▶ Clonshaugh, Ireland | ▶ Kolkata, India |
| ▶ Columbus, United States | ▶ Koropi, Greece (2 sites) |
| ▶ Dallas, United States (3 sites) | |
| ▶ Denver, United States | |
| ▶ Diemen, Netherlands | |
| ▶ Doha, Qatar | |

This scope is only valid in connection with certificate 2013-009.

Amazon Web Services, Inc.

Scope for certificate 2013-009

- ▶ Kuala Lumpur, Malaysia
- ▶ Lagos, Nigeria
- ▶ Las Vegas, United States (2 sites)
- ▶ Lisbon, Portugal
- ▶ London, United Kingdom (5 sites)
- ▶ Los Angeles, United States (3 sites)
- ▶ Lynnwood, United States
- ▶ Madrid, Spain (5 sites)
- ▶ Manchester, United Kingdom (2 sites)
- ▶ Manila, Philippines (2 sites)
- ▶ Marseille, France (3 sites)
- ▶ Melbourne, Australia (2 sites)
- ▶ Miami, United States
- ▶ Milan, Italy (3 sites)
- ▶ Milpitas, United States
- ▶ Minneapolis, United States
- ▶ Munich, Germany
- ▶ Nairobi, Kenya
- ▶ New Delhi, India
- ▶ New Taipei City, Taiwan
- ▶ New York City, United States (2 sites)
- ▶ Newark, United States
- ▶ Noida, India
- ▶ North Las Vegas, United States
- ▶ Osaka, Japan (3 sites)
- ▶ Oslo, Norway (2 sites)
- ▶ Perth, Australia
- ▶ Philadelphia, United States (2 sites)
- ▶ Phoenix, United States
- ▶ Piscataway, United States
- ▶ Pittsburgh, United States
- ▶ Portland, United States
- ▶ Prague, Czech Republic
- ▶ Pune, India
- ▶ Quezon, Philippines
- ▶ Reston, United States (2 sites)
- ▶ Richardson, United States
- ▶ Rio de Janeiro, Brazil (2 sites)
- ▶ Riyadh, Saudi Arabia
- ▶ Rome, Italy
- ▶ Rosedale, New Zealand
- ▶ Santiago de Querétaro, Mexico (4 sites)
- ▶ Santiago de Surco, Peru
- ▶ Santiago, Chile
- ▶ Scarborough, Canada
- ▶ Schiphol-Rijk, Netherlands
- ▶ Seattle, United States (3 sites)
- ▶ Secaucus, United States (2 sites)
- ▶ Seoul, South Korea (4 sites)
- ▶ Singapore, Singapore (2 sites)
- ▶ Sofia, Bulgaria
- ▶ Stockholm, Sweden (4 sites)
- ▶ Tokyo, Japan (4 sites)
- ▶ Taipei, Taiwan (2 sites)
- ▶ Tallinn, Estonia
- ▶ Tampa, United States (2 sites)
- ▶ Tempe, United States
- ▶ Toronto, Canada (2 sites)
- ▶ Vancouver, Canada (2 sites)
- ▶ Vienna, Austria (2 sites)
- ▶ Wall, United States
- ▶ Warsaw, Poland (2 sites)
- ▶ West Valley City, United States
- ▶ Zagreb, Croatia
- ▶ Zurich, Switzerland (3 sites)

This scope is only valid in connection with certificate 2013-009.

Amazon Web Services, Inc.

Scope for certificate 2013-009

Wavelength locations in:

- ▶ Alpharetta, United States
- ▶ Annapolis Junction, United States
- ▶ Aurora, United States
- ▶ Azusa, United States
- ▶ Berlin, Germany
- ▶ Charlotte, United States
- ▶ Daejeon, South Korea
- ▶ Dortmund, Germany
- ▶ Eufless, United States
- ▶ Houston, United States
- ▶ Knoxville, United States
- ▶ Las Vegas, United States
- ▶ Lenexa, United States
- ▶ London, United Kingdom
- ▶ Minneapolis, United States
- ▶ Munich, Germany
- ▶ New Berlin, United States
- ▶ Osaka, Japan
- ▶ Pembroke Pines, United States
- ▶ Plant City, United States
- ▶ Redmond, United States
- ▶ Rufisque, Senegal
- ▶ Rocklin, United States
- ▶ Salford, United Kingdom (2 sites)
- ▶ Seoul, South Korea
- ▶ Southfield, United States
- ▶ Tama, Japan
- ▶ Tempe, United States
- ▶ Toronto, Canada
- ▶ Wall Township, United States
- ▶ Westborough, United States

Local zone locations in:

- ▶ Atlanta, United States (4 sites)
- ▶ Ballerup, Denmark
- ▶ Bang Chalong, Thailand
- ▶ Barka, Oman
- ▶ Boston, United States
- ▶ Caba, Argentina
- ▶ Chicago, United States (2 sites)
- ▶ Doral, United States
- ▶ El Segundo, United States
- ▶ Espoo, Finland
- ▶ Garland, United States (3 sites)
- ▶ Greenwood Village, United States
- ▶ Hamburg, Germany
- ▶ Hillsboro, United States
- ▶ Houston, United States (2 sites)
- ▶ Irvine, United States
- ▶ Itasca, United States
- ▶ Kansas City, United States (2 sites)
- ▶ Kapolei, United States
- ▶ Kolkata, India (2 sites)
- ▶ Lagos, Nigeria
- ▶ Las Vegas, United States
- ▶ Lee's Summit, United States*
- ▶ Lithia Springs, United States (2 sites)
- ▶ Manila, Philippines
- ▶ Mesa, United States (3 sites)
- ▶ Miami, United States
- ▶ Minneapolis, United States
- ▶ New Carlisle, United States (4 sites)
- ▶ New Delhi, India
- ▶ New Taipei City, Taiwan
- ▶ Noida, India*
- ▶ North Las Vegas, United States
- ▶ Nouaceur, Morocco
- ▶ Perth, Australia
- ▶ Philadelphia, United States
- ▶ Phoenix, United States
- ▶ Piscataway, United States (2 sites)

This scope is only valid in connection with certificate 2013-009.

Amazon Web Services, Inc.

Scope for certificate 2013-009

- ▶ Richardson, United States
- ▶ Rosedale, New Zealand
- ▶ Santiago de Querétaro, Mexico
- ▶ Santiago de Surco, Peru
- ▶ Santiago, Chile
- ▶ Seattle, United States
- ▶ Singapore, Singapore* (4 sites)
- ▶ Warsaw, Poland

* This local zone is a dedicated local zone and may not be available to all customers.

Note: For locations where the number of sites is not explicitly specified, it is interpreted as one (1) site.



This scope is only valid in connection with certificate 2013-009.

ISO/IEC 27001:2022 Statement of Applicability, Version 2025.01

Amazon Web Services (AWS)

August 29, 2025

Control #	Applicable (Y/N)	Control #	Applicable (Y/N)	Control #	Applicable (Y/N)
A.5.1	Y	A.5.32	Y	A.8.4	Y
A.5.2	Y	A.5.33	Y	A.8.5	Y
A.5.3	Y	A.5.34	Y	A.8.6	Y
A.5.4	Y	A.5.35	Y	A.8.7	Y
A.5.5	Y	A.5.36	Y	A.8.8	Y
A.5.6	Y	A.5.37	Y	A.8.9	Y
A.5.7	Y	A.6.1	Y	A.8.10	Y
A.5.8	Y	A.6.2	Y	A.8.11	Y
A.5.9	Y	A.6.3	Y	A.8.12	Y
A.5.10	Y	A.6.4	Y	A.8.13	Y
A.5.11	Y	A.6.5	Y	A.8.14	Y
A.5.12	Y	A.6.6	Y	A.8.15	Y
A.5.13	Y	A.6.7	Y	A.8.16	Y
A.5.14	Y	A.6.8	Y	A.8.17	Y
A.5.15	Y	A.7.1	Y	A.8.18	Y
A.5.16	Y	A.7.2	Y	A.8.19	Y
A.5.17	Y	A.7.3	Y	A.8.20	Y
A.5.18	Y	A.7.4	Y	A.8.21	Y
A.5.19	Y	A.7.5	Y	A.8.22	Y
A.5.20	Y	A.7.6	Y	A.8.23	Y
A.5.21	Y	A.7.7	Y	A.8.24	Y
A.5.22	Y	A.7.8	Y	A.8.25	Y
A.5.23	N	A.7.9	Y	A.8.26	Y
A.5.24	Y	A.7.10	Y	A.8.27	Y
A.5.25	Y	A.7.11	Y	A.8.28	Y
A.5.26	Y	A.7.12	Y	A.8.29	Y
A.5.27	Y	A.7.13	Y	A.8.30	N
A.5.28	Y	A.7.14	Y	A.8.31	Y
A.5.29	Y	A.8.1	Y	A.8.32	Y
A.5.30	Y	A.8.2	Y	A.8.33	Y
A.5.31	Y	A.8.3	Y	A.8.34	Y

NOTE: All marked applicable controls are implemented.