ISO/IEC 27001:2022, ISO/IEC 27017:2015, AND ISO/IEC 27018:2019 RECERTIFICATION AUDIT REPORT

Versa Networks

June 19, 2025

Prepared by
Sensiba LLP

Contents

Confidentiality Statement

This document presents Versa Networks the results of this ISO/IEC 27001:2022, ISO/IEC 27017:2015, and ISO/IEC 27018:2019 Recertification audit report (Report). Versa may distribute this Report to its clients, provided that each recipient agrees not to use or distribute the information contained herein or any other information regarding Versa for any purpose other than those stated. This Report and any other Versa related information provided shall remain the sole property of Versa and may not be copied, reproduced, or distributed without prior written consent of Versa.

Applicability

The audit approach taken was based on a sampling process of the available information provided by Versa to meet the audit objectives. As such, Versa acknowledges that there is a risk of sampling error. The accuracy of the Report and its conclusions are dependent upon the complete and accurate disclosure of information by Versa.

Disclosure of Independence

Sensiba LLP (Sensiba) assessed the Information Security Management System (ISMS) for Versa without holding any investment or control over the company. At no point during the assessment did Sensiba willfully or unnecessarily market services to help Versa achieve conformance to ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018. No services were recommended by Sensiba during the engagement.

Certification Body and Audit Parameters

Sensiba is accredited by ANAB as a certification body for ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018. Sensiba received an application for certification from Versa Networks (Versa or the Company) and has conducted a Recertification audit based on the following criteria:

- Standard(s): ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018
- Control Objectives: ISO 27001 Annex A, ISO 27017 Annex A, and ISO 27018 Annex A
- Scope: The Information Security Management System (ISMS) of Versa Networks supports the development, operation, and maintenance of its Cybersecure Information Security Program, including associated information systems, infrastructure, personnel, and processes used to deliver secure services and manage both company and client information assets. This ISMS is applied across all relevant business functions and technical environments, in accordance with the Statement of Applicability (SoA), and is aligned with the requirements of ISO/IEC 27001:2022.

Audit Team Recommendations

Based on the results of the recertification audit, including the absence of nonconformities, the demonstrated maturity of the ISMS, and a strong culture of continual improvement, the audit team recommends continued certification of Versa Networks to ISO/IEC 27001:2022.

It is the audit team's recommendation that Versa be issued an ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 Certificate of Registration based on their Statement of Applicability version 4 dated 2/17/2025.

During the audit process, the following nonconformities were identified:

Finding Ref	NC Type	Domain	Status	Finding Justification
No nonconformities were identified during this audit cycle				

During the audit process, the following opportunities for improvement (OFIs) were identified:

Finding Ref	Domain	Finding Justification
No opportunities for improvement were identified this audit cycle		

During the audit process, Sensiba determined that the scope of the ISMS was appropriate for Versa.

All audit objectives were met.

Audit Detail

Versa Networks
Sunil Ravi
Chief Security Architect
2550 Great America Way 350, 3rd floor,
Santa Clara, CA 95054

June 19, 2025

Company Background

Versa Networks (“Versa” or the “Company”) offers cutting-edge networking and security solutions, including Secure Access Service Edge (SASE) technology, to securely connect enterprise branches, teleworkers, and end users to applications in the cloud or data centers globally.

Overview

To demonstrate its commitment to information security, Versa has implemented an ISMS that meets the requirements of ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018. Developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 is a standard that outlines the process for establishing, implementing, operating, monitoring, reviewing, and maintaining an ISMS. To validate conformity and certify the Company's ISMS. against the ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 standard(s), Versa engaged Sensiba LLP (Sensiba) to perform a Recertification audit.

The Recertification audit is conducted as a point-in-time audit and is conducted to review the documented Recertification information, acquire the necessary information regarding the scope of the Recertification and assess its ongoing effectiveness.

The Recertification audit was conducted to assess the success and efficiency of the company's Information Security Management System (ISMS). The audit took place between 05/29/2025 and 06/13/2025.

Audit Criteria

Sensiba conducted a Recertification audit to determine if the company's ISMS conformed to the requirements of the ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 and the processes and procedures defined by Versa. The Statement of Applicability version 4, dated 2/17/25, was used as the basis for the audit, which derived the controls and control objectives from ISO 27001 Annex A, ISO 27017 Annex A, and ISO 27018 Annex A, as a cloud service provider.

Audit Objectives

The Stage 2 audit was performed by Sensiba to accomplish the following:

- Assess the alignment of the company's ISMS, or elements of it, with the audit standards.
- Assess the adequacy of the company's ISMS to satisfy applicable legal, regulatory, and contractual obligations.

- Assess the performance of the company's ISMS in meeting its stated goals
- Discover ways to enhance the company's Information Security Management System (ISMS), when applicable.

All audit objectives were completed as planned.

Audit Scope

The scope of certification has been defined as “The Information Security Management System (ISMS) of Versa Networks supports the development, operation, and maintenance of its Cybersecure Information Security Program, including associated information systems, infrastructure, personnel, and processes used to deliver secure services and manage both company and client information assets. This ISMS is applied across all relevant business functions and technical environments, in accordance with the Statement of Applicability (SoA), and is aligned with the requirements of ISO/IEC 27001:2022.”

Audit Locations

Location	Registered Activity
HQ: 2550 Great America Way, Suite 350 Santa Clara, CA 95054	Headquarters, ISMS Management, Engineering, Sales & Marketing, Administration
India (Remote)	Technical Support, Managed Services, Systems Engineering

Audit Time

The following table represents the amount of auditor time required at each stage of the audit program lifecycle. These values are based on ISO 27006-1:2024 Table C.1, and adjustments in Annex C.3.5

Audit Cycle	Year	# of EEs	Required Audit Days	Actual Audit Days
Recertification	2025	734	12	12
1st Surveillance	2026	734	6	6
2nd Surveillance	2027	734	6	6
Recertification	2028	734	12	12

1 Legend: Rows in light green are future years

Remote Auditing

Remote auditing techniques were used to conduct this ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 audit with Versa. Any in-scope locations were visited via remote auditing techniques per ISO/IEC 27006-1:2024 C.3.2.

Risks

There is a risk that remote auditing procedures could limit the level of interaction with the audit team, including the connectivity with the client, lack of documentation to support our conclusions, and a lack of audit time. To mitigate this, the audit team scheduled Zoom meetings in advance to ensure that sufficient time was allocated with the client's control owners and management to ensure an effective review.

Mitigation Strategy

To further mitigate the risks of applying a remote audit approach, Sensiba set up Zoom meetings to ensure that teams could connect for the interviews and meetings. Zoom is hosted by an external cloud service provider, meaning that the risk of them not being available was low. Additionally, Sensiba teams routinely work remotely and have sufficient connectivity to support working from home, and they also implemented additional measures to ensure the remote audit process was secure and that all data was protected.

Mitigation to lack of availability: Sensiba team members, working remotely, remained committed to the project and client for the days specified in the audit plan. With a remote working team, both the client and Sensiba team members were able to minimize any disruption that could potentially hinder the audit (e.g., government-mandated working from home if the audit was taking place at a physical office). Moreover, it was communicated to the client that they must be available during the remote audit, as per the times stated in the audit plan and the criteria to be audited, for Sensiba to conduct an effective audit, regardless of whether all persons were on-site or remote.

Mitigation to a lack of documentation: Sensiba provided an Information Request List (IRL) prior to the audit fieldwork. The client, who has access to the IRL, was required to provide the necessary documentation prior to and during the audit. Despite the remote approach to the audit, documents were still requested and were required to be provided to ensure the accuracy and completeness of the audit process.

Mitigation to a lack of audit time to perform an effective audit: As noted, the approach to the audit did not change. It remained the same planned audit time and days as if it were conducted on-site. Meetings were performed via remote means, with the review of supporting evidence conducted during the meetings. Any testing that would be impacted from a remote approach (ie,. on-site physical security walk throughs) were revised to occur in the subsequent surveillance review. In order to maximize the effectiveness of the audit, additional time was allocated to review and analyze the evidence to ensure all risks and exposures were identified and discussed.

** See ISO 27006-1:2024, C.3.2 for reference

If remote auditing methods such as interactive web-based collaboration, web meetings, teleconferences and/or electronic verification of the organization’s processes are utilized to interface with the organization, these activities should be identified in the audit plan (see 9.2.3) and may be considered as partially contributing to the total “on-site audit time”.

NOTE On-site audit time refers to the on-site audit time allocated for individual sites. Electronic audits of remote sites are considered to be remote audits, even if the electronic audits are physically carried out on the organization's premises.

Audit Process

An opening meeting was held on 05/29/2025 at 9:00 AM PT. In attendance were Vasu Kommidi (Technical Program Manager, Versa), Vengal Darapaneni (Head of Program Management Customer Success, Versa), Sunil Ravi (Chief Security Architect, Versa), Jason Clark (Consultant, Comply Federal), and Eric Bruning (Lead Auditor, Sensiba). During the meeting, the agenda and the detailed audit plan for the Recertification of the project were presented and discussed. All parties left the meeting with a clear understanding of their respective roles and responsibilities.

The audit was performed over 12 days, between 05/29/2025 and 06/13/2025, which included 12 days of remote auditing. Screen sharing technology tools (Zoom) were used to facilitate the audit. No major issues were identified that would impact the audit program.

At the conclusion of the audit activities, a closing meeting was held at 4:30 PM PT on 06/13/2025. Present at the meeting were Vasu Kommidi (Technical Program Manager, Versa), Vengal Darapaneni (Head of Program Management Customer Success, Versa), Sunil Ravi (Chief Security Architect, Versa), Jason Clark (Consultant, Comply Federal), and Eric Bruning (Lead Auditor, Sensiba), and the agenda provided was in accordance with version 1 of the Recertification audit plan. All audit objectives were successfully completed as outlined in the audit plan.

Interviews

Interviews were conducted with Versa personnel, as well as subject matter experts (SMEs), key vendors, and sub-service providers as necessary.

Internal Audit

Sensiba reviewed the audit program for the objectives, scope, and criteria of internal audits. Internal audits were to be conducted annually. The most recent internal audit was conducted in March 2025 by Independent Third-Party and identified no nonconformities. The results of this internal audit, including any nonconformities and corrective action(s), were reviewed and approved by the Compliance Team in March 2025, and documented in the meeting minutes.

Sensiba determined that the internal audit objectives, scope, and criteria were suitable, and the internal audit could guarantee that the Information Security Management System (ISMS) had been properly implemented and managed, based on the audit evidence collected.

Sensiba determined that the Client would maintain their Internal Audit cadence with the next Internal Audit scheduled for March 2026.

Management Reviews

Management reviews were held regularly at intervals of annually by the Compliance Team. This body was composed of:

- Chief Development Officer
- Chief Security Architect
- Management board
- Consultant

Sensiba reviewed the management review results, risk assessment and risk treatment plan approvals, monitoring and measurement results, internal audit findings, nonconformities, and corrective actions discussed in the Compliance Team meeting minutes. The audit team ensured that all necessary steps were taken to ensure the effectiveness of the Information Security Management System.

Sensiba determined management had the necessary capabilities to ensure the ongoing suitability, adequacy, and effectiveness of the ISMS, based on the audit evidence collected. Additionally, Sensiba has determined that the Client's Management Review cadence will be maintained based on their next Management Review scheduled for March 2026.

Audit Method

During the audit, Sensiba obtained the necessary information to meet the audit objectives, scope, and criteria. This included, but was not limited to, interviews, observation of processes and activities, and reviews of documentation and records. Sampling procedures were used to ensure the accuracy of the audit results. However, sampling does not provide absolute assurance that the controls are functioning correctly across the entire population. Sensiba took all necessary steps to ensure the audit was conducted in a thorough and accurate manner.

Audit methods applied by Sensiba:

- Review the structure, policies, processes, procedures, records, and related documents of the client to ensure compliance with the Information Security Management System (ISMS).
- Verify that all the requirements relevant to the intended scope of certification have been met.
- Verify that the processes and procedures put in place for the Company's ISMS have been effectively established, implemented, and maintained.
- Inform the client of any discrepancies between the Company's policy, objectives, and goals that may require their action.

During the Recertification audit, evidence that was examined or observed included, but was not limited to:

Document	Artifact Reference	Version/Date
Scope of the ISMS	Cybersecure Manual	1.2 - 04/11/2025
Leadership and commitment	Cybersecure Manual	1.2 - 04/11/2025
Information Security Policy	Cybersecure Manual Versa Networks Information Security Policy	Various
Organizational roles, responsibilities and authorities	Cybersecure Manual Roles & Responsibilities	1.2 - 04/11/2025
Information security risk assessment	Cybersecure Manual Risk Register	1.2 - 04/11/2025
Information security risk treatment	Cybersecure Manual Risk Register	1.2 - 04/11/2025
Statement of Applicability	SoA	4 – 2/17/2025
Information security objectives and planning to achieve them	Cybersecure Manual	1.2 - 04/11/2025
Evidence of Competence	Cybersecure Manual	1.2 - 04/11/2025
Documented Information Determined by the Organization as being Necessary for the Effectiveness of the ISMS	Cybersecure Manual	1.2 - 04/11/2025
Operations planning and control	Cybersecure Manual	1.2 - 04/11/2025
Information security risk assessment	Risk Register	03/01/2025
Information security risk treatment	Risk Register	03/01/2025
	Internal Audit Report	1 - 03/27/2025
Internal audit program and report	Internal Audit Report	1 - 03/27/2025
	Management Review	1 - 03/27/2025
Evidence of the Results of any Corrective Action	NC & OFI Log - 2025	06/11/2025
Access control	Access to source code.png	Various
Information security in supplier relationships	Supplier Management Policy	1.6 – 1/15/2025

Document	Artifact Reference	Version/Date
Information security during disruption	Business Continuity Test	1.6 – 11/15/2024
Legal, statutory, regulatory and contractual requirements	Legal, Regulatory and Contractual Requirements Management	1 - 03/11/2025
Documented operating procedures	Various operating procedures available	Various
Terms and conditions of Employment	Observed various employees' terms and conditions	Various
Logging	Various Logs	Various
Secure system architecture and engineering principles	Secure Development Life Cycle Policy	1.9 - 01/15/2024
ISO 27001:2022 Transition GAP	Versa Gap Assessment	1 – 1/7/2025

Audit Findings

No nonconformities were identified.

Audit Conclusions

At the conclusion of the audit, Sensiba determined that Versa had met the requirements of ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 and issued a Certificate of Registration. This certificate confirms that Versa has established, implemented, and maintained an ISMS that meets the requirements of the ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 standard. Versa is committed to maintaining a secure environment for its customers and employees. The successful completion of the ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 audit demonstrates the Company's dedication to information security and its commitment to protecting the privacy and security of its customers and employees.

Distribution List

This report has been distributed to the following:

- Sunil Ravi, Chief Security Architect, Versa
- Jeffery Stark, Partner in Charge, Risk Assurance Services, Sensiba
- Brian Beal, Partner, Risk Assurance Services, Sensiba
- Scott Dritz, Senior Manager, Risk Assurance Services, Sensiba
- Eric Bruning, Lead Auditor, Sensiba

Conformance Testing

Nonconformity Grading

This report provides management with an identification of the documentation efforts, review, and testing of the maintenance, monitoring, and operating effectiveness of the ISMS in relation to the ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 standard requirements (Clauses and the control activities identified in the Annex(s)). The documentation requirements and the maintenance, monitoring, and operating effectiveness of the ISMS have been classified according to their importance in achieving compliance with the standard.

ISO 17021-1 defines nonconformities as follows:

> **3.11 - nonconformity** - non-fulfilment of a requirement
>
> **3.12 - major nonconformity** - nonconformity (3.11) that affects the capability of the management system to achieve the intended results
>
> > **Note 1 to entry:** Nonconformities could be classified as major in the following circumstances:
> >
> > - if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
> > - a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.
>
> **3.13 - minor nonconformity** - nonconformity (3.11) that does not affect the capability of the management system to achieve the intended results

The classifications in this report are defined as follows:

Conforms - Based on observations, discussions with personnel, and inspection testing, it has been determined that the documentation requirements and/or controls are effectively in place and functioning

Major Nonconformity - nonconformity that affects the capability of the management system to achieve the intended results

Minor Nonconformity - nonconformity that does not affect the capability of the management system to achieve the intended results

Opportunity for Improvement (OFI) - identifies areas for improvement in an organization in order to enhance performance, efficiency, and effectiveness and thereby increase overall success

Not Applicable - Annex control was excluded by the Company's Statement of Applicability

Not Selected - Annex Control not selected during a Surveillance Audit

Status Classifications documented are defined as follows:

Open - When a nonconformity is assigned a status of "open," it means that the corresponding corrective action plan and evidence of correction have not been reviewed or are unacceptable. The nonconformity will remain open until an acceptable corrective action plan and evidence of correction are reviewed and deemed acceptable by the audit team. Additionally, the nonconformity will remain open even if an acceptable corrective

action plan and evidence of correction are on file, but there is no evidence of remediation (e.g., the full implementation of the corrective action plan that addresses the root cause related to the nonconformance). In such cases, the report will document that the nonconformity has an acceptable corrective action plan and evidence of correction on file.

Closed - A nonconformity is assigned a status of "closed" when the corresponding corrective action plan, evidence of correction, and evidence of remediation have been reviewed and accepted by the audit team, thus verifying that the nonconformity has been adequately addressed.

ISO 27001:2022 Clauses

Clause Reference	Clause Requirement	Conformity Level
4	**Context of the organization**	
4.1	Understanding the organization and its context	Conforms
4.2	Understanding the needs and expectations of interested parties	Conforms
4.3	Determining the scope of the information security management system	Conforms
4.4	Information security management system	Conforms
5	**Leadership**	
5.1	Leadership and commitment	Conforms
5.2	Policy	Conforms
5.3	Organizational roles, responsibilities and authorities	Conforms
6	**Planning**	
6.1.1	Actions to address risks and opportunities - General	Conforms
6.1.2	Information security risk assessment	Conforms
6.1.3	Information security risk treatment	Conforms
6.1.3.d	Statement of Applicability	Conforms
6.2	Information security objectives and planning to achieve them	Conforms
6.3	Planning of changes	Conforms
7	**Support**	
7.1	Resources	Conforms
7.2	Competence	Conforms
7.3	Awareness	Conforms
7.4	Communication	Conforms
7.5.1	Documented information - General	Conforms
7.5.2	Creating and updating	Conforms
7.5.3	Control of documented information	Conforms
8	**Operation**	
8.1	Operational planning and control	Conforms
8.2	Information security risk assessment	Conforms
8.3	Information security risk treatment	Conforms
9	**Performance evaluation**	
9.1	Monitoring, measurement, analysis and evaluation	Conforms

Clause Reference	Clause Requirement	Conformity Level
9.2.1	Internal audit - General	Conforms
9.2.2	Internal audit programme	Conforms
9.3	Management review	Conforms
9.3.3	Management review results	Conforms
10	**Improvement**	
10.1	Continual improvement	Conforms
10.2	Nonconformity and corrective action	Conforms

ISO 27001:2022 Annex A

Annex Control	Control Name	Conformity Level
A.5	**Organizational controls**	
A.5.1	Policies for information security	Conforms
A.5.2	Information security roles and responsibilities	Conforms
A.5.3	Segregation of duties	Conforms
A.5.4	Management responsibilities	Conforms
A.5.5	Contact with authorities	Conforms
A.5.6	Contact with special interest groups	Conforms
A.5.7	Threat intelligence	Conforms
A.5.8	Information security in project management	Conforms
A.5.9	Inventory of information and other associated assets	Conforms
A.5.10	Acceptable use of information and other associated assets	Conforms
A.5.11	Return of assets	Conforms
A.5.12	Classification of information	Conforms
A.5.13	Labelling of information	Conforms
A.5.14	Information transfer	Conforms
A.5.15	Access control	Conforms
A.5.16	Identity management	Conforms
A.5.17	Authentication information	Conforms
A.5.18	Access rights	Conforms
A.5.19	Information security in supplier relationships	Conforms
A.5.20	Addressing information security within supplier agreements	Conforms
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Conforms
A.5.22	Monitoring, review and change management of supplier services	Conforms
A.5.23	Information security for use of cloud services	Conforms
A.5.24	Information security incident management planning and preparation	Conforms
A.5.25	Assessment and decision on information security events	Conforms
A.5.26	Response to information security incidents	Conforms
A.5.27	Learning from information security incidents	Conforms
A.5.28	Collection of evidence	Conforms
A.5.29	Information security during disruption	Conforms
A.5.30	ICT readiness for business continuity	Conforms
A.5.31	Legal, statutory, regulatory and contractual requirements	Conforms
A.5.32	Intellectual property rights	Conforms
A.5.33	Protection of records	Conforms

Annex Control	Control Name	Conformity Level
A.5.34	Privacy and protection of personal identifiable information (PII)	Conforms
A.5.35	Independent review of information security	Conforms
A.5.36	Compliance with policies, rules and standards for information security	Conforms
A.5.37	Documented operating procedures	Conforms
A.6	**People controls**	
A.6.1	Screening	Conforms
A.6.2	Terms and conditions of employment	Conforms
A.6.3	Information security awareness, education and training	Conforms
A.6.4	Disciplinary process	Conforms
A.6.5	Responsibilities after termination or change of employment	Conforms
A.6.6	Confidentiality or non-disclosure agreements	Conforms
A.6.7	Remote working	Conforms
A.6.8	Information security event reporting	Conforms
A.7	**Physical controls**	
A.7.1	Physical security perimeters	Conforms
A.7.2	Physical entry	Conforms
A.7.3	Securing offices, rooms and facilities	Conforms
A.7.4	Physical security monitoring	Conforms
A.7.5	Protecting against physical and environmental threats	Conforms
A.7.6	Working in secure areas	Conforms
A.7.7	Clear desk and clear screen	Conforms
A.7.8	Equipment siting and protection	Conforms
A.7.9	Security of assets off-premises	Conforms
A.7.10	Storage media	Conforms
A.7.11	Supporting utilities	Conforms
A.7.12	Cabling security	Conforms
A.7.13	Equipment maintenance	Conforms
A.7.14	Secure disposal or re-use of equipment	Conforms
A.8	**Technological controls**	
A.8.1	User end point devices	Conforms
A.8.2	Privileged access rights	Conforms
A.8.3	Information access restriction	Conforms
A.8.4	Access to source code	Conforms
A.8.5	Secure authentication	Conforms
A.8.6	Capacity management	Conforms
A.8.7	Protection against malware	Conforms
A.8.8	Management of technical vulnerabilities	Conforms
A.8.9	Configuration management	Conforms
A.8.10	Information deletion	Conforms

Annex Control	Control Name	Conformity Level
A.8.11	Data masking	Conforms
A.8.12	Data leakage prevention	Conforms
A.8.13	Information backup	Conforms
A.8.14	Redundancy of information processing facilities	Conforms
A.8.15	Logging	Conforms
A.8.16	Monitoring activities	Conforms
A.8.17	Clock synchronization	Conforms
A.8.18	Use of privileged utility programs	Conforms
A.8.19	Installation of software on operational systems	Conforms
A.8.20	Networks security	Conforms
A.8.21	Security of network services	Conforms
A.8.22	Segregation of networks	Conforms
A.8.23	Web filtering	Conforms
A.8.24	Use of cryptography	Conforms
A.8.25	Secure development life cycle	Conforms
A.8.26	Application security requirements	Conforms
A.8.27	Secure system architecture and engineering principles	Conforms
A.8.28	Secure coding	Conforms
A.8.29	Security testing in development and acceptance	Conforms
A.8.30	Outsourced development	Conforms
A.8.31	Separation of development, test and production environments	Conforms
A.8.32	Change management	Conforms
A.8.33	Test information	Conforms
A.8.34	Protection of information systems during audit testing	Conforms

ISO 27017:2015 Annex A

Annex Control	Control Name	Conformity Level
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Conforms
CLD.8.1.5	Removal of cloud service customer assets	Conforms
CLD.9.5.1	Segregation in virtual computing environments	Conforms
CLD.9.5.2	Virtual Machine Hardening	Conforms
CLD.12.1.5	Administrator's operational security	Conforms
CLD.12.4.5	Monitoring of Cloud Services	Conforms
CLD.13.1.4	Alignment of security management for virtual and physical networks	Conforms

ISO 27018:2019 Annex A

Annex Control	Control Name	Conformity Level
A.2.1	Obligation to co-operate regarding PII principals' rights	Conforms
A.3.1	Public cloud PII processor's purpose	Conforms
A.3.2	Public cloud PII processor's commercial use	Conforms
A.5.1	Secure erasure of temporary files	Conforms
A.6.1	PII Disclosure Notification	Conforms
A.6.2	Recording of PII disclosures	Conforms
A.8.1	Disclosure of sub-contracted PII processing	Conforms
A.10.1	Notification of a data breach involving PII	Conforms
A.10.2	Retention period for administrative security policies and guidelines	Conforms
A.10.3	PII return, transfer and disposal	Conforms
A.11.1	Confidentiality or non-disclosure agreements	Conforms
A.11.2	Restriction of the creation of hardcopy material	Conforms
A.11.3	Control and logging of data restoration	Conforms
A.11.4	Protecting data on storage media leaving the premises	Conforms
A.11.5	Use of unencrypted portable storage media and devices	Conforms
A.11.6	Public cloud PII protection implementation guidance	Conforms
A.11.7	Secure Disposal of Material	Conforms
A.11.8	Unique use of user IDs	Conforms
A.11.9	Records of authorized users	Conforms
A.11.10	User ID management	Conforms
A.11.11	Contract Measures	Conforms
A.11.12	Sub-contracted PII processing	Conforms
A.11.13	Access to data on pre-used data storage space	Conforms
A.12.1	Geographical location of PII	Conforms
A.12.2	Intended destination of PII	Conforms

Nonconformity Details

Nonconformities from the current certification cycle, including the current year, if any, are listed below.

	Noted	Control	Justification	NC Type / Status
No findings have been identified during the current audit cycle.				