

	Standard Security Requirements for Cloud Services and on-premises Systems	Document Identifier	559-487964975	Rev	1
		Effective Date	30 March 2024		
		Review Date	31 March 2027		

Notes:

- 1) Cloud Services include Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Function as a Service (FaaS), Data as a Service (DaaS), Integration Platform as a Service (iPaaS) and Security as a Service (SECaaS).
- 2) On-premises Systems include all systems that are placed and hosted on the Eskom corporate local area network (LAN) or business information network (BIN), and this does not include systems that are placed and hosted on the operational technology (OT) or process control network (PCN).
- 3) Service Organisation Control (SOC) attestation reports are only applicable to Cloud Services such as SaaS, PaaS, IaaS, iPaaS, and SECaaS, not systems hosted on Eskom's Azure tenant/virtual private cloud (VPC) and on-premises on the Eskom corporate local area network (LAN) or business information network (BIN).
- 4) SOC 1 Type II and SOC 2 Type II is an attestation standard put forth by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) that addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide cloud services to user entities.
- 5) SOC 1 Type II is a mandatory requirement for all Cloud Services that store and process financial information.
- 6) SOC 2 Type II is a mandatory requirement for all Cloud Services that store and process personal identification information (PII) and intellectual property (IP) information.
- 7) The SOC reports must be for the Service Provider that submits the technical proposal as part of the RFP for the Cloud Service offered and not for the Service Provider or sub-organisation (such as Microsoft Azure, AWS and GCP) where the Cloud Service is hosted.

Controlled Disclosure

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

	Standard Security Requirements for Cloud Services and on-premises Systems	Document Identifier	559-487964975	Rev	1
		Effective Date	30 March 2024		
		Review Date	31 March 2027		

Security Control	Mandatory/ Optional/ Preferred
1. External Third-Party Attestation Reports The Cloud Service Provider (CSP) shall: a) For all cloud services that store and process financial information and personal identifiable information (PII) including intellectual property (IP), the CSP shall have a valid Service Organisation Control (SOC) 1 and SOC 2 Type II reports, such attestation reports shall be submitted to Eskom for review. b) Up to once per period of twelve (12) months, the CSP will provide comprehensive summaries of its latest SOC 2 report at no cost upon Eskom's written request. c) if the SOC Reports indicate any deficiencies or matters requiring attention, the CSP shall use commercially reasonable efforts to address all such items without any costs to the Eskom. d) Subject to Section 1.b, if vendor's reporting cycle is not aligned with the financial year, and/or the SOC report is older than six (6) months, the CSP shall submit a bridge letter to the Eskom at no cost, and such bridging letter shall not cover a period exceeding three (3) months.	Mandatory for all cloud services that store and process PII, intellectual property (IP) and financial information.
2. The cloud service shall be able to integrate with existing Eskom's identity provider (IdP) and Multi Factor Authentication (MFA) to enable Single sign-on (SSO).	Mandatory for all cloud services and on-prem systems
3. Role base access control (RBAC) shall be employed.	Mandatory for all cloud services and on-prem systems
4. Data at rest (using at minimal AES-256) and in transit or in motion (using at minimum TLS 1.2, or later version) shall be encrypted.	Mandatory for all cloud services and on-prem systems
5. Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.	Mandatory for all cloud services and on-prem systems
6. Sensitive information such as personal identifiable information (PII) data in Sandbox/development (DEV) environment shall be masked.	Mandatory for all cloud services and on-prem systems
7. Incremental daily back-ups shall be done, encrypted, and securely kept offsite.	Mandatory for all systems classified a mission critical
8. Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site, located in different region shall be employed.	Mandatory for all systems classified a mission critical

Controlled Disclosure

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

	Standard Security Requirements for Cloud Services and on-premises Systems	Document Identifier	559-487964975	Rev	1
		Effective Date	30 March 2024		
		Review Date	31 March 2027		

Security Control		Mandatory/ Optional/ Preferred
9.	Disaster Recovery Plan (DRP) shall be defined, annually tested and such DRP test results shall be shared with Eskom Cybersecurity team.	Mandatory for all systems classified a mission critical
10.	Back up Restore Plan and Procedure shall be defined, annually tested and such test results shall be shared with Eskom Cyber Security team.	Mandatory for all cloud services and on-prem systems
11.	Patch Management Process shall be defined. The software updates and patches shall be tested on Sandbox or development (DEV) environment before being deployed into production (PROD) environment.	Mandatory for all cloud services and on-prem systems
12.	The static application security test (SAST) and dynamic application security test (DAST) and penetration test shall be conducted prior deploying the cloud system and on-prem systems to PROD, all critical, high, and medium vulnerabilities shall be addressed prior deploying PROD, and the summary of the test results shall be submitted to the Eskom Cybersecurity team for review and acceptance.	Mandatory for all cloud services and on-prem systems
13.	The CSP shall comply with applicable privacy and protection of personal information Acts such as GDPR in European Union (EU) and POPIA in South Africa (SA) where the cloud service is hosted, and the region where the data subjects are physically located and where the data is collected.	Mandatory for all cloud services that store and process PII
14.	The CSP shall notify Eskom immediately or within 24 hours when any cyber security breach has occurred. Although the GDPR and the South African Cybercrimes Act 19 of 2020 states that the notification shall be sent within 72 hours, Eskom shall be notified sooner to allow Eskom to notify the information regulator and take necessary actions to minimize the impact on Eskom.	Mandatory for all cloud systems that store and process PII
15.	The CSP shall notify Eskom within one (1) month if there are any significant changes to the business, platform and hosting service provider or any change that could have an impact the security assessment conducted and the auditor's opinion on the SOC audit.	Mandatory for all cloud services
16.	The database shall be placed within Eskom corporate LAN/BIN network (if hosted on premise) and partner private network (If hosted in the cloud) behind the perimeter firewall.	Mandatory for all cloud services and on-prem systems
17.	Database Security tools shall be employed to provide regulatory compliance, encryption, key management, granular access controls, flexible data masking, comprehensive activity monitoring, and sophisticated auditing capabilities.	Mandatory for all cloud services and on-prem systems
18.	Distributed denial of service (DDoS) protection mechanism shall be employed for all could services.	Mandatory for all cloud services

Controlled Disclosure

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

	Standard Security Requirements for Cloud Services and on-premises Systems	Document Identifier	559-487964975	Rev	1
		Effective Date	30 March 2024		
		Review Date	31 March 2027		

Security Control		Mandatory/ Optional/ Preferred
19.	Web Application Firewall (WAF) for all internet facing applications and/or web-based applications shall be employed.	Mandatory for all cloud services and on-prem systems
20.	The Cloud Service shall support the prevailing enterprise services bus (ESB), application programmable interfaces (API's) and Integration Platform as a Service (iPaaS) platforms for security, logging and monitoring for both on-prem, hybrid-cloud and multi-cloud environments such as IBM App Connect, TIBCO Cloud Integration (including Business Works and Scribe), WSO2 Carbon, Software AG web Methods, Neuron ESB, Apache Camel, WebSphere Message Broker, RSSBus Connect, Azure Service Bus and Oracle Service Bus, Salesforce Mulesoft, IBM DataPower, Oracle API Platform, Cyclr, DreamFactory JDBC, Microsoft SQL Server Integration Services (SSIS), SAS Data Integration Studio, Integration Adaptor DirXML, Oracle X AI Services, SAP Business Process Automation, SAP NetWeaver, Oracle Fusion Middleware, Connect Direct, HP Data Protector, WINSCP, FreeFileSync, SAP PI/PO, SAP CPI, HP SOA Systinet, JCAPS, Cloud Pak for Data, K2, Microsoft Power Automate and Zapier but not limited to these listed.	Mandatory for all cloud services and on-prem systems
21.	The Cloud Service shall provide e-Discovery capability to identify, collect and produce electronically stored information (ESI) in response to a request for production in a lawsuit or investigation as part of the cloud services offered.	Mandatory for all cloud services

Controlled Disclosure

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30