Annex Y to SLA 1023_001: Information System Security Services

Document No:	1023_001_Y
Version:	1.0
Author:	Ronald Mamdoo
Effective Date:	1 April 2025
Electronic File:	1023_Annex 001_Y_Information System Security_01 Apr 25_31 Mar 28

DLH

BN

Annex Y: Information System Security Services

Y1. Service Classification

This Service is classified as value added services in terms of the SITA Services Catalogue and as a mandatory service in terms of the SITA Act.

Y2. Reference(s)

SITA ISS Maturity Assessment Report KZN EDTEA

Y3. Benefit Statement

The value contribution of Information Security-as-a-Service to the customer as it addresses the business challenges.

#	Aspect of business challenge	Value statement	
		Area	Statement
1	Interruption of business process	Service Continuity	Effectively recover business process after a disaster
2	Business Continuity	Service Continuity	Business continues with little disruption
3	Disaster Recovery	Service Continuity	Little or no duplication of work that has already been done
4	Security and Vulnerability Assessment	Service Delivery	Ensure execution of Department mandate.
5	Cyber Security Awareness	Service Delivery	Provide training to users as per Department mandate.
6	Information Security Policy	Service Delivery	Provide review of Information System Security Policy and Processes

Y4. Information System Security Services

Y4.1. Service Metric: Business Continuity Management Services

The purpose of this service is to address findings in discipline 18 and 19 of the ISF Cyber Security Assessment. The goal is to provide the organisation will an established method to deal with major incidents and to provide resilience against disruption and minimise the impact of disruption to the organisation. The following are the deliverables aligned to the KZN Provincial Treasury templates:

a) Emergency Response Plan (ERP) -Year 1
b) Crisis Management Plan (CMP)- Year 1
c) Media/Communication Plan – Year 1
d) Disaster Recovery Plan (DRP)-Year 1
e) Business Continuity Plan (BCP)- Year 1
f) BCM Simulation and Testing (1/3 Years)
g) DRP Simulation and Testing (1/3 Years)
h) Presentation to Client / Post Meeting- Year 1

Y4.2. Service Metric: Vulnerability Management Services

This service is to address system and software vulnerabilities quickly and effectively to reduce the likelihood of vulnerabilities being exploited and serious business impact arising. SITA will conduct technical vulnerability assessment on servers and workstations using a market leading vulnerability assessment tool. The assessment will comprise of the following for 3 years:

a) Conduct Technical Vulnerability Assessment for Critical Department Subnets (Sites to be identified by the Department) per 6 months.
b) Provide Remediation Plan.
c) Provide support.

Y4.3. Service Metric: Cyber Security Awareness Services

The purpose of this service is to address findings in discipline 20 of the ISF Cyber Security Assessment. The goal is to embed a positive security culture where all relevant individuals make effective risk-based decisions and protect critical and sensitive information from being compromised. SITA

a) Planning: Presentation of Awareness – Year 1
b) 1 Virtual Quarter Session (2 Hours) Interactive- Year 1,2,3
c) Monthly Newsletter – Year 1, 12; Year 2, 2 and Year 3, 2
d) Email Campaign (online)- Year 1, 2 and 3: 12
e) Adhoc Campaign and Awareness Services

Y4.4. Service Metric: Information Services

The purpose of this service is to address findings in discipline 20 of the ISF Cyber Security Assessment. The goal is to embed a positive security culture where all relevant individuals make effective risk-based decisions and protect critical and sensitive information from being compromised. SITA

a) Planning
b) Review and identify gaps in policy and procedures.
c) Close the gaps identified in the policy and procedures.
d) Provide training on the policy and procedures.

Y5. Service Category: Information system Security Services

Y5.1. Service Metric

	Service Offering	Service Description	Configured Service		Workload		Service Components	Measurement		
			Basic features	Additional features required	Contracted	Cap		Metric	Unit of measure	
Security Management	Business Continuity Management Services	The purpose of this service is to address findings in discipline 18 and 19 of the ISF Cyber Security Assessment. The goal is to provide the organisation will an established method to deal with major incidents and to provide resilience against disruption and minimise the impact of disruption to the organisation.	a) Risk Identification Review b) Business Impact Analysis Review c) Business Continuity management documentation Review d) Testing		228 Hours	Budget and Time	a) Emergency Response Plan (ERP) b) Crisis Management Plan (CMP) c)Media/Communication Plan d) Disaster Recovery Plan (DRP) e) Business Continuity Plan (BCP) f) BCM Simulation and Testing (3 Years) g) DRP Simulation and Testing h) Presentation to Client / Post Meeting	Year 1. 100% activities completed Year 2: Test and Review Year 3: Test and Review	1. % delivery per project plan	Service Management

Security Management	Service Offering	Service Description	Configured Service		Workload		Service Components	Measurement		Service Management
			Basic features	Additional features required	Contracted	Cap		Metric	Unit of measure	
	Vulnerability Management Services	(a) Security Risk management service enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. (b) Risk Assessment: Activities that are used to gather some information about the department. (c) Risk Control – Implementation of measure to mitigate the Risk	a) Risk Identification b) Risk Analysis c) Risk Evaluation d) Risk Reporting e) Risk Monitoring	Assessment to be conducted on site. All nodes must be connected on a network.	100 Hours per quarter	Budget and Time	(a) Gather Information (b) Identification of information and Information Systems © Analyse the identified information (d) Assess threats and vulnerabilities e) Compile security risks and vulnerability assessment f) Attend quarterly meetings g) Once vulnerabilities are identified, recommendations for remediation will be passed to relevant lines of business for implementation	Year 1: Conduct 2 vulnerability assessments per cycle Year 2: Conduct 2 vulnerability assessments per cycle Year 3: Conduct 2 vulnerability assessments per cycle	1. % delivery per project plan	

	Service Offering	Service Description	Configured Service		Workload		Service Components	Measurement		
			Basic features	Additional features required	Contracted	Cap		Metric	Unit of measure	
Security Management	Cyber Security Awareness services	The purpose of this service is to address findings in discipline 20 of the ISF Cyber Security Assessment. The goal is to embed a positive security culture where all relevant individuals make effective risk-based decisions and protect critical and sensitive information from being compromised.	Cyber Security Awareness		112Hours	Budget and Time	a) Planning & Presentation of Awareness b) 1 Virtual Quarter Session (2 Hours) Interactive c) Monthly Newsletter d) Email Campaign (online) e) Adhoc Campaign and Awareness Services	Year 1. 50% activities completed Year 2: 25 % activities completed Year 3: 25% of activities completed	1. % delivery per project plan	Service Management
Security Management	Information Security Policy and Procedure Review	The purpose of the service is to review the department's current Information Security Policy and the procedures. To identify analyse and identify gaps.	Information Security Policy		260 Hours	Budget and Time	a) Planning of the review period. b) Review and identify gaps in policy and procedures. c) Close the gaps identified in the policy and procedures. d) Provide training on the policy and procedures.	Year 1. 40% activities completed Year 2: 30% activities completed Year 3: 30% of activities completed	1. % delivery per project plan	

Y6. Roles and responsibilities

The client is responsible for

a) providing requested information by SITA in an appropriate timeframe,
b) scheduling internal meetings for engagement,
c) having the appropriate personnel available from the department
d) ensuring VPNra access to the department
e) ensure effective and efficient document review and
f) managing their service providers.

SITA is responsible for

a) Ensure availability of knowledgeable resources,
b) Ensure service delivery as agreed in the annexure,
c) Providing feedback and
d) The client relationship manager is responsible for the recommendations of payment of invoices after sign-off of the rendered services.

Y7. Pricing

Y7.1 Annual Recurrent Cost

No.	Service/Application	Year 1	Year 2	Year 3
1	Business Continuity Management Services	R240,511.21	R252,536.77	R265,163.61
2	Vulnerability Management Services	R79,729.64	R83,716.12	R87,901.93
3	Cyber Awareness Campaign	R277,240.76	R34,052.88	R37,458.16
4	Information Security Policy Services	R157,165.01	R172,881.51	R190,169.66
	Total (VAT excl.)	R754,646.62	R543,187.28	R580,693.36
	Monthly Total (VAT excl)	R62,887.22	R45,265.61	R48,391.11
	Annual Total (VAT Incl.)	R867,843.61	R624,665.37	R667,797.36
	Grand Total (VAT Incl.)	R2,160,306.34		

NOTE:

1) The addition of any specific new service to this SLA shall necessitate adjustment of the price

Y8. Penalties

If SITA fails to achieve the service levels that are stipulated above and provided that such a failure is not caused by a failure of the Client to comply with its obligations and duties in terms of this SLA, SITA shall compensate the Client by raising a credit note of 2.5% on the relevant invoice. Credit notes will not be processed for such penalties in the event of the Client's Account being in the arrears.

Y9. Dependencies and constraints

Y9.1Dependencies:

1. Availability of client for assessment
2. Access to the client environment

Y9.2Constraints:

1. Budget and Time.

SP

Y10. Certification:

We hereby certify that this Annex covers the full extent of the Information System Security as required. We further accept the service and the price accordingly.

This Annex shall be effective from 1 April 2025 until 31 March 2028.

Thus, done and signed at Pietermaritzburg on this 10 day of March 20 25

Signed by:Brightboy Nhlakanipho Nkont
Signed at:2025-03-10 13:04:54 +02:00
Reason:I approve this document

Full names: Brightboy Nhlakanipho Nkontwana
On behalf of KwaZulu Natal Department of Economic Development,Tourism & Environmental Affairs
And duly authorised thereto

Thus, done and signed at Durban on this 11th day of February 2025

Full names: Pamella Gqabaza – KZN Provincial Manager (Acting)
On behalf of State Information Technology Agency SOC Ltd
And duly authorised thereto

Signed by:VANESSA MACLOU
Signed at:2025-03-11 08:35:30 +02:00
Reason:I approve this document