




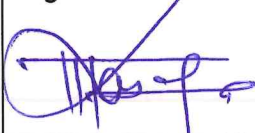
SIEM Audit Form			
Information Security Risk Assessment Tool			
			Page 1 of 9
Document No:011	Version:1.0	Effective	Relevant area: IBA department

Author:

Written/Revised by: (Name, Position) Mwema Mwamasimbi	Signature: 	Date: 19.1.2024
--	--	--------------------


Approval cycle:

Reviewed by: (Name, Position)	Signature:	Date:
Alfred Kilamile		19/1/2024


Authorized by: (Name, Position) Paul Kasanga (IBA Head)	Signature:	Date:
IBA Head		18/01/2024

Document Change Control


Version	Changes	Name	effective date
1.0	New SOP	Alfred Kilamile	2024
1.1	Revised SOP		
1.2	Revised SOP		

SIEM Audit Form			
Information Security Risk Assessment Tool			
Document No:011	Version:1.0	Effective	Page 3 of 9
			Relevant area: IBA department


8	<u>Vulnerability Scanning</u> – A regular occurring (e.g., bi-annual, quarterly, monthly) process using specialized scanning tools and techniques that evaluates the configuration, patches, and services for known vulnerabilities is employed.		
B Personnel Practices			
1	<u>Security Awareness</u> – Training is provided to all employees and contractors on an annual basis that addresses acceptable use and good computing practices for systems they are authorized to access. Content of training is based on CCBRT policies addressing issues, such as, privacy requirements, virus protection, incident reporting, Internet use, notification to staff about monitoring activities, password requirements, and consequences of legal and policy violations.		
2	<u>Human Resources Security</u> – Policies and procedures that address purpose, scope, roles, responsibilities, and compliance to support personnel security requirements, such as access rights, disciplinary process, etc. are in place.		
3	<u>Position Categorization</u> – Procedures for identifying system access needs by job function and screening criteria for individuals performing those functions are in place.		
4	<u>Personnel Separation</u> – A process to terminate information system and physical access and ensure the return of all CCBRT-related property (keys, id badges, etc.) when an individual changes assignment or separates from the agency is developed and implemented.		
5	<u>Third Party or Contractor Security</u> – Personnel security requirements for third-party providers and procedures to monitor compliance are in place. Requirements are included in acquisition-related documents, such as service-level agreements, contracts, and memorandums of understanding.		
6	<u>Personnel Screening</u> – Employee history and/or a background check is performed on employees who work with or have access to confidential or sensitive information or critical systems.		
C Physical Security Practices			
1	<u>Physical and Environmental Program</u> – Policy and procedures that address the purpose, scope, roles, responsibilities, and compliance for physical and		

SIEM Audit Form			
Information Security Risk Assessment Tool			
Document No:011	Version:1.0	Effective	Page 5 of 9
			Relevant area: IBA department

2	<u>Information Back-up</u> – Backup copies of information and software are completed on a routine schedule, tested regularly, and stored off-site.		
3	<u>Monitoring</u> – System logging, and routine procedures to audit logs, security events, system use, systems alerts or failures, etc. are implemented and log information is in place where it cannot be manipulated or altered.		
4	<u>Data Classification</u> – Policies and processes to classify information in terms of its value, legal requirements, sensitivity, and criticality to the organization are in place.		
5	<u>Access Controls</u> – Policies and procedures are in place for appropriate levels of access to computer assets. Access controls include, but are not limited to:		
	<ul style="list-style-type: none"> Wireless access restrictions, appropriate configuration of wireless devices and policy procedures are in place 		
	<ul style="list-style-type: none"> Training for technical staff and users are in place. 		
	<ul style="list-style-type: none"> Secure remote access procedures and policies are in place, and are known and followed by users. 		
	<ul style="list-style-type: none"> Mobile and portable systems and their data are protected through adequate security measures, such as encryption and secure passwords, and physical security, such as storing devices in a secure location and using cable locking devices. 		
	<ul style="list-style-type: none"> The tracking of access and authorities, including periodic audits of controls and privileges is in place. 		
6	<u>Least Privilege</u> – Configuration to the lowest privilege level necessary to execute legitimate and authorized business applications is implemented.		
7	<u>Data Storage and Portable Media Protection</u> – Policies and procedures to protect data on electronic storage media, including CDs, USB drives, and tapes are in place. Procedures include labels on media to show sensitivity levels and handling requirements, rotation, retention and archival schedules, and appropriate destruction/disposal of media and data.		
E	Information Integrity Practices		

SIEM Audit Form			
Information Security Risk Assessment Tool			
			Page 7 of 9
Document No:011	Version:1.0	Effective	Relevant area: IBA department

	place to address roles and responsibilities, and processes for compliance checking.		
2	<u>Software Integrity Practices</u> – Policies and procedures associated with system and services acquisition and product acceptance are in place.		
	<ul style="list-style-type: none"> Acquisitions – Security requirements and/or security specifications, either explicitly or by reference, are included in all information system acquisition contracts based on an assessment of risk. 		
	<ul style="list-style-type: none"> Software Usage Restrictions – Controls or validation measures to comply with software usage restrictions in accordance with contract agreements and copyright laws are in place. 		
	<ul style="list-style-type: none"> User Installed Software – An explicit policy governing the downloading and installation of software by users is in place. 		
	<ul style="list-style-type: none"> Outsourced Information System Services – Controls or validation measures to ensure that third-party providers of information system services employ adequate security controls in accordance with applicable laws, policies and established service level agreements are in place. 		
	<ul style="list-style-type: none"> Developer Security Testing – A security test and evaluation plan is in place, implemented, and documents the results. Security test results may be used in support of the security certification process for the delivered information system. 		
G	Personal Computer Security Practices – Personal computing devices include desktops, laptops, notebooks, tablets, Personal Device Assistants (PDA), and other mobile devices.		
1	<u>Device Hardening</u> – Operating system and application-level updates, patches, and hot fixes are applied as soon as they become available and are fully tested. Services on the computing devices are only enabled where there is a demonstrated business need and only after a risk assessment.		
2	<u>Lock-Out for Inactive Computing Devices</u> – The automatic locking of the computing device after a period of inactivity is enforced.		
3	<u>Data Storage</u> – Data that needs additional protection is stored on pre-defined servers, rather than on		

SIEM Audit Form			
Information Security Risk Assessment Tool			
			Page 9 of 9
Document No:011	Version:1.0	Effective	Relevant area: IBA department

Information Security (IS) Officer:

Name.....

Date:

Signature:

Head IBA:

Name:

Date:

Signature.....