Policy: Information Security Incident and Vulnerability Management Policy

Reference Number: 8/7/2/1/6/9 Incident and Vulnerability Management

Version: 3.0
Date:15/12/2021

Contents

1 Document Version Control

Changes:

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
19/12/2018	Louis van Dyk	1.0	First Draft
04/04/2019	Louis van Dyk	1.1	Change applicability section 3 to include external service providers and consultants
23/04/2019	Louis van Dyk	1.2	Add responsible office section 4
25/05/2019	Grant Donald	1.3	Overall format change
21/08/2019	Louis van Dyk	2.0	Change version for sign off
15/02/2021	Michael Stadler	2.1	Update policy details
16/02/2022	Louis van Dyk	3.0	Added intended audience section & Change version for sign off

Reviews:

DATE	AUTHOR	VERSION NUMBER	REVIEW DETAILS
21/08/2019	Michael Stadler	2.0	Reviewed
28/03/2022	Deidre Marais	3.0	Reviewed
28/03/2022	Deidre Marais	3.0	Reviewed

Sign offs:

DATE	AUTHOR	DESIGNATION	SIGNATURE
	Andrew Coleman	Director: DSCS	Andrew Coleman Digitally signed by Andrew Coleman Date: 2022.03.29 07:53:31 +02'00'
	Augi de Freitas	CD: GMS	A De Freitas 2022.03.28 22:09:21 +02'00'
	Hilton Arendse	DDG: Be-I	Hilton Arendse 2022.03.30 19:54:54 +02'00'

2 Policy Overview

The purpose of this policy is to ensure a consistent and effective approach to the management of information security incidents and vulnerabilities. It defines the requirements for managing the security incident lifecycle, managing vulnerabilities and performing patch management. This policy serves to complement other IT policies and processes which would address the broader areas of incident management and disaster recovery. It also aims to establish a process for the reporting on security incidents and vulnerabilities together with the escalation and sign-off on risks not mitigated.

3 Applicability

This policy applies to all individuals that provide and manage IT resources and services under the custodianship of the WCG or sourced from 3rd party services. This includes all WCG employees, third parties, temporary staff, contractors, external service providers and consultants.

3.1 Intended Audience

This policy is intended for review by all **IT operational Teams**.

The following are the key expectations of users:

- To familiarise themselves with this policy and all other related policies, standards and guidelines (where applicable).
- Take responsibility for all activity related to IT accounts they have been allocated and any information they access.
- Report any accidental breach of policy or suspected misuse of WCG IT resources or fraudulent activity to their line manager.

4 Responsible Office

The WCG Be-I information Security Sub-directorate owns and maintains this policy and can be contacted with the following email address ictpolicies@westerncape.gov.za

5 Policy Statement

The policy addresses information security incidents which are events that may indicate that the WCG's systems or data have been compromised or that measures put in place to protect them have failed. Security incidents include the violation of an explicit or implicit security policy or breach of legislation. It also addresses the requirements for identifying both infrastructure and application vulnerabilities with remediation through patch management and system development processes. While this policy addresses the specific requirements of this security area, there are other related information security policies, IT policies and standards that need to be considered.

The coverage and mandate of this policy will be limited to the scope of the Be-I managed IT environment within the WCG. These IT and information security services are focused on the Corporate VPN (Virtual Private Network) used by multiple provincial departments in the Western Cape. Other IT areas may make use of this policy but enforcement is limited to the scope of IT governance and security controls.

6 Related Policy Detail

Policy Section	6.1 Information Security Incident Response Planning
Rationale	An information security incident response planning mechanism must be in place to ensure that information security breaches or incidents are resolved within the minimum possible time and the least impact to the IT environment of the WCG.
Policy Statements	6.1.1 An information security incident and problem response process must be documented and implemented in accordance with this policy and related standards. 6.1.2 Forms, processes, procedures and support tools for the detection and reporting of assessment and response to information security incidents are to be recorded in a response planning document, including details of the incident's severity scale. 6.1.3 A Cyber Security Incident Response Team (CSIRT) must be established with defined roles and responsibilities allocated to personnel who are available to adequately respond to all known types of information security incidents. 6.1.4 In the event of the CSIRT being activated, the related personnel will be responsible for prioritising and coordinating a resolution as directed by the CSIRT officer. 6.1.5 Security Incident response plans and related playbooks must be documented and indicate roles, responsibilities (RACI) and handling procedures before and after an incident. 6.1.6 Response plans must cater to both IT systems and business functions in accordance with IT DR and BC Plans. 6.1.7 Planning must include all business and IT functions that are both critical and non-critical yet necessary support functions. 6.1.8 Crisis Management plans must be defined to deal with critical incidents that may impact the WCG's reputation in accordance with the Business Continuity Management Policy.
Related Policies and Procedures	Enterprise Risk Management Framework WCG ICT Backup and Recovery Policy

Policy Section	6.2 Identification and Investigation
Rationale	A security-related event is any observable occurrence that is relevant to information security. This can include attempted attacks or weaknesses that expose security vulnerabilities. A security incident however is a specific security event or a number of security events that result in damage or risk to the WCG assets and operations.
Policy Statements	6.2.1 Establish relevant security event categories for all physical access events, system events and user events.

6.2.2	Information security events must be detected and reported. The definition of these events must follow use cases that consider cyber and internal threats.
6.2.3	All relevant information relating to the nature of the event such as type, source, time/date, related identity and event detail must be recorded.
6.2.4	The event types to be recorded must be identified based on a consideration of risk and retained for an appropriate period to assist in future investigations.
6.2.5	Forensic techniques must be followed for real time observation, investigation, analysis and reporting. This supports the evidence collection process. Only personnel with the relevant skillset should be appointed to carry out this responsibility.
6.2.6	Appropriate technical analysis of security events must be performed, including analysis of events from Network and system logs, physical access logs, Intrusion Detection Systems/Intrusion Prevention Systems logs, system event logs, router and firewall logs, anti-virus logs, application logs and vulnerability scan reports.
6.2.7	Security information and event management system (SIEM) should be implemented to help the organisation improve threat detection and incident response capability. A SIEM tool will collect and correlate security event and log data from disparate network devices and enterprise information systems for analysis and identification of security threats in real time.
6.2.8	A security operations centre (SOC) should be established to monitor and analyse the organisation's security posture on an ongoing basis. The SOC staff must work closely with information security incident response teams to ensure security issues are addressed quickly upon discovery.
6.2.9	The incident response function will identify the source (root cause) of the threat, breach, compromise or infection.
6.2.10	The incident response function will record and classify the incident and follow the relevant incident response plan and playbooks.
6.2.11	The incident response function will assess what has been affected and define any impact on the business.
6.2.12	The BE-I Security function will confirm the nature of the incident, and the type of data that are involved, whether the data is personal data relating to individuals or otherwise confidential or valuable.
6.2.13	New risks identified as a result of an incident must be assigned to the relevant risk owner and unacceptable risks must be mitigated promptly in accordance with the WCG's risk management processes.
6.2.14	The BE-I Security function must maintain a confidential log of all information security incidents.
6.2.15	The necessary internal and external referrals of findings and actions for incident response/handling must be initiated by the CSIRT.

Related Policies and Procedures	

Policy Section	**6.3 Remediation**
Rationale	Once a threat has been identified, the incident response team will work to contain it to prevent further damage to other systems and the organisation at large. Once the threat has been sufficiently contained, the incident response team will work to implement a more permanent fix. This might include patching hardware, reconfiguring systems and application architecture, or rebuilding a system for production use. The goal is to eliminate the entry point that the threat actor used to obtain access to the network, system and data.
Policy Statements	6.3.1 Information Security incidents must be contained, remediated and mitigated. 6.3.2 Forensic data handling and storage procedures supersede any other existing procedures for the compromised systems to ensure the chain of command integrity and preservation of evidence. 6.3.3 All remediation/mitigation must be subject to the existing change control process. 6.3.4 Existing and relevant incident remediation playbooks must be followed. 6.3.5 All information security incidents will be subject to summary review by the BE-I security function so that any threats, weaknesses or vulnerabilities that may have contributed to the incident are identified, documented and eradicated.
Related Policies and Procedures	

Policy Section	**6.4 Recovery and Lessons Learned**
Rationale	At the recovery stage, any production systems affected by a threat will be brought back online. This includes any data recovery or restoration efforts that need to take place as well. The incident response team will need to decide when operations will be restored, test and verify that infected systems are fully restored, continue to monitor for malicious activity and validate the recovery. The purpose of the recovery process is to restore normal service operations as quickly as possible and minimise any long-term adverse impact on business operations, ensuring that agreed levels of service quality are maintained.
Policy Statements	6.4.1 Where temporary mitigating controls have been implemented these should be reversed or follow the change control process.

	6.4.2 Where systems have been isolated these must be evaluated before reintroduction or segmentation should prevail or decommissioning. 6.4.3 Assess the effectiveness of current security controls to prevent/discourage, detect and respond to any future attacks. 6.4.4 Update/reconfigure relevant IT systems to help prevent any future recurrences of similar incidents. 6.4.5 For crown jewels systems, asses and implement additional monitoring and security controls as needed. 6.4.6 Assess and update relevant policies, standards, procedures and incident playbooks to help prevent any future recurrences of similar incidents.
Related Policies and Procedures	

Policy Section	**6.5 Vulnerability Management**
Rationale	Both applications and infrastructure are based on software. This software in the form of operating systems, desktop applications or enterprise applications is vulnerable to flaws due to human error or lack of security foresight. These vulnerabilities are often discovered and exploited, leading to breaches of security. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures Vulnerability scans often report hundreds or thousands of items (security events) without much guidance as to what is really a threat to your system. Typically, reports sort threats into critical, high, medium, and low-risk categories. Critical and high vulnerabilities can be treated as security incidents and can be fed into the incident response process.
Policy Statements	6.5.1 The WCG must implement processes to scan for vulnerabilities in information systems and hosted applications at least monthly and when new vulnerabilities potentially affecting the information systems or applications are reported. 6.5.2 BE-I must analyse vulnerability scan reports and ensure appropriate remedial action is taken in a timely manner. 6.5.3 All endpoint devices, operating systems, databases and network infrastructure connected to both public and trusted segments of the network must be scanned. 6.5.4 The vulnerability scanning tools must be maintained to ensure the vulnerability scan signatures are up to date. 6.5.5 Automated scans must be configured to ensure that tests are run at pre-determined slots and adhere to the agreed frequency. 6.5.6 Data from scans must be treated as internal-confidential. 6.5.7 Scanning of applications must make use of Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), risk reviews and penetration tests to identify vulnerabilities.

	6.5.8 Each vulnerability listed must have detailed information on how the vulnerability will be remedied or eliminated. 6.5.9 Authoritative sources of asset information must be referenced and correlated to establish the asset; owner, location and type associated with relevant vulnerabilities. 6.5.10 BE-I, IT service providers and departmental IT asset owners with IT assets on the WCG network will remedy and/or mitigate discovered vulnerabilities based on the **Common Vulnerability Scoring System** (CVSS): • **Critical** - Critical vulnerabilities that have a score of 10 must invoke the CSIRT, follow the critical patch management process and be remediated within service level of 3 days. • **High** - High-severity vulnerabilities that have a CVSS score of 8.0 or higher must be remediated within service level of 30 days. • **Medium** - Medium-severity vulnerabilities that have a CVSS score of 6.0 to 8.0 must be mitigated within service level of 90 days. • **Low** - Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0, they must be remediated within service level of 180 Days. 6.5.11 Any findings that need to be mitigated later than the service level must be approved through the security governance process and documented as exceptions. 6.5.12 All remediation must be subject to the existing change control process. 6.5.13 All remediation must be verified as being successful.
Related Policies and Procedures	Secure Development Policy

Policy Section	**6.6 Patch Management**
Rationale	Patching is the process of repairing software vulnerabilities which are discovered after the software has been released to the market. It is necessary to develop a patch management process to ensure proper preventive measures are implemented to protect against potential threats.
Policy Statements	6.6.1 All IT systems either owned by the WCG or those in the process of being developed or supported by third parties, must be manufacturer supported and have up to date security patched operating systems and application software. 6.6.2 Vulnerability Assessment scans and Vendor notifications must be analysed to determine the applicability of a security patch to remediate a vulnerability. 6.6.3 Any patches categorised as 'Critical' or 'High risk' by the vendor should be installed within 14 days of release from the vendor unless

	rejected by the Change Advisory Board (CAB) within the Change Management process. 6.6.4 All security patches must be subjected to User Acceptance Testing (UAT) and interoperability testing. The UAT must accompany the approved change request. Due diligence should be exercised by applying these patches in Development and Test environments before rolling out to production when possible. 6.6.5 Any patches that need to be applied later than the service level must be approved through the security governance process, documented as exceptions and reviewed quarterly.
Related Policies and Procedures	

7 Enforcement

The BE-I Security function will verify compliance with this policy through various methods, including but not limited to, security reporting tools, internal and external audits and management feedback to the policy owner.

Violation of this policy (e.g. wilful or negligent exposure of confidential information) may result in disciplinary action which may include termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the WCG. Additionally, employees, contractors and agents who violate this policy may be subject to civil and criminal prosecution.

8 Exception Handling

Exceptions to the guiding principles in this policy must be documented and formally approved by the relevant Accounting Officer of the department. Policy exceptions must describe:

- The nature of the exception
- Why the policy exception is required
- Risks created by the policy exception
- Evidence of approval by the Accounting Officer and Be-I Security Officer.

The IT and Enterprise Risk Management team must be notified of any exceptions having a risk impact.

9 Glossary

Term	Definition
BCP	Business Continuity Plan
CAB	Change Advisory Board
BE-I	Center of Innovation
CSIRT	Cyber Security Incident Response Team
CVSS	Common Vulnerability Scoring System (scale 1-10)
DAST	Dynamic Application Security Testing
DR	IT Disaster Recovery
RACI	Responsible, Accountable, Consulted, Informed
SAST	Static Application Security Testing
SIEM	Security Information and Event Monitoring
SoC	Security Operations Center

UAT	User Acceptance Testing
IT Assets	These include Infrastructure Systems, Servers, Databases and Applications (both endpoint and business applications)
Days	Any indication of days refers to Calendar Days.
Crown Jewel	A particularly valuable or prized possession or asset.

10 References

This policy references the following external artefacts:

- National Institute of Standards and Technology (NIST) Special Publication 800-61, Revision 2, Computer Incident Handling Guide
- NIST Cybersecurity Framework v1.1
- The Center for Internet Security (CIS) Critical Security Controls
- ISO/IEC 27035:2016 Standard on Incident Handling
- South African Cybercrimes Bill (draft