Policy: Endpoint Security Policy

Reference Number:
8/7/2/6/9/ Endpoint Security

Version: 3.0
Date: 15/12/2021

Contents

1 Document Version Control

Changes:

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
04/04/2019	Louis van Dyk	1.0	First Draft
16/04/2019	Louis van Dyk	1.1	Change applicability section 3 to include external service providers and consultants
16/04/2019	Louis van Dyk	1.2	Add responsible office section 4
03/07/2019	Louis Van Dyk	1.3	Overall format change
25/08/2019	Louis Van Dyk	3.0	Added intended audience section & Change version for sign off

Reviews:

DATE	AUTHOR	VERSION NUMBER	REVIEW DETAILS
12/08/2019	Michael Stadler	1.3	Reviewed
25/08/2019	Michael Stadler	2.0	Reviewed
15/02/2021	Michael Stadler	2.1	Updated policy details
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 07:52:09 +02'00'
	Augi de Freitas	CD: GMS	A De Freitas 2022.03.28 22:08:26 +02'00'
	Hilton Arendse	DDG: Be-I	Hilton Arendse 2022.03.30 20:00:43 +02'00'

2 Policy Overview

The purpose of this policy is to protect the WCG network and corporate information by regulating the configuration and use of endpoint computing systems such as desktops, laptops, tablets, mobile devices and servers. The objective is to reduce the risk of primarily cybersecurity attacks that could target endpoint devices or end-users. This policy seeks to limit security threats by:

- Ensuring staff are aware of the requirements and restrictions around endpoint devices.
- Enabling protective measures and controls to manage endpoint security and reduce software risks.

3 Applicability

This policy applies to all individuals that provide and manage IT resources and services under the custodianship of 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

This policy addresses all forms of endpoint devices from computing devices to servers and network devices. It also addresses IT end users and their interaction with endpoint devices and applications. 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 Virtual Private Network (VPN) used by multiple provincial departments in the Western Cape. Other IT areas may make use of this policy, but enforcement is limited by the scope of IT governance and security controls.

6 Related Policy Detail

Policy Section	6.1 Endpoint Device Security
Rationale	Endpoint devices are the most common target for modern cyber-attacks usually allowing an easy point of access to the network and other resources. It is important to have well designed endpoint security because security on the endpoint is the first line of defence.
Policy Statements	6.1.1 The large and complex ecosystem of the WCG's endpoint devices must be managed using automated tools and processes that enable an authoritative source of endpoint assets and centralised management. 6.1.2 Endpoint Operating Systems (OS) and application software must be kept up to date with the latest security and related patches in accordance with the WCG patch management requirements. 6.1.3 Operating Systems that reach the end of support are not permitted to connect to the WCG network. 6.1.4 The removing or disabling of endpoint device management or security software without prior formal approval is prohibited. 6.1.5 All endpoint devices connecting to the trusted network must run the WCG antivirus software. This must be the latest software version and have the latest virus signature definitions. 6.1.6 Disabling or removing of antivirus software or disabling antivirus software definition updates on endpoints without prior formal approval is prohibited. 6.1.7 All endpoint devices capable of running a local firewall must have it enabled with a WCG approved configuration. 6.1.8 Appropriate host-based protection systems, such as up-to-date anti-malware, endpoint detection and response (EDR) and host-based firewalls must be implemented on endpoint devices to commensurate with the security risk. 6.1.9 Corporate and classified data must be stored only in authorised locations in line with the data protection policy and standards. 6.1.10 Corporate and classified data stored on an endpoint device must have the appropriate security controls to restrict and prevent retrieval or interception by an unauthorised third-party. 6.1.11 Physical access to endpoint devices that store sensitive data and configurations should be controlled and restricted to authorised personnel only. Where endpoint devices are not secured by physical controls (e.g. laptops), adequate logical access controls must be applied. 6.1.12 Endpoint admission control systems must be in place to ensure that only authorised endpoints can connect to the WCG networks. 6.1.13 The bridging of the WCG network with 3rd party networks or the Internet, such as through a mobile connection, is not permitted.

Related Policies and Procedures	Logical Access Management Policy Data Protection policy Network Security Policy

Policy Section	**6.2 Computer Platform Security**
Rationale	Improperly configured information systems or their components can introduce vulnerabilities that could be exploited for the purpose of committing cybercrime or lead to damage or disruption of information systems operation.
Policy Statements	6.2.1 Operating system and end user application software images must be configured, version-controlled and used for the building of servers and end user computers. 6.2.2 Only the software or applications necessary to fulfil the device's required functions must be installed. 6.2.3 An accurate inventory of information system components and CI's that need to be managed and secured through the secure baseline configurations management process must be established and kept up to date. The inventory must cover, at a minimum, the following categories of configuration items: • Operating systems including desktop and server operating systems; • Cloud providers; • Server software including web servers, application servers, database servers, collaboration servers, DNS servers, authentication servers and virtualisation software; • Desktop Software, including web browsers, productivity software and protection software; • Mobile devices; • Network Devices; • Desktop hardware; • Server hardware 6.2.4 Security baseline configuration management activities must be integrated into (or complement) the existing broader configuration management and other related information technology management processes such as change control, asset management, etc. 6.2.5 For each information system platform identified in the inventory, a minimum-security configuration baseline must be defined, documented, reviewed and approved by the relevant WCG system owner. 6.2.6 Where available, platform security configuration standards must be used to ensure the appropriate hardening of Operating Systems, Databases, Applications and Network Infrastructure. 6.2.7 If applicable, legal and regulatory requirements must be considered and integrated when defining security baseline configurations.

	6.2.8 Reviews must be periodically performed to ensure compliance with baseline configuration standards and the use of and supported system build images that are approved by EAB. 6.2.9 All security configuration changes must also be evaluated for consistency against the WCG's enterprise architecture standards and requirements.
Related Policies and Procedures	CIS Configuration Standards

Policy Section	**6.3 End User Security**
Rationale	People are often the weakest link in the security chain as they are often not aware of the security risks and implications. Users must, therefore, be trained to understand how their actions can impact the overall security of the WCG.
Policy Statements	6.3.1 The principle of least privilege must be applied to 'day-to-day' computing accounts and should only be used for performing routine tasks. Separate system administrative accounts must be used to perform tasks requiring elevated privileges. 6.3.2 Security training must be provided to relevant staff (e.g., system administrators, system/software developers, system security officers, system owners, etc.) if necessary, to ensure that they have the skills to perform security related duties. 6.3.3 Users shall be accountable for all activity associated with their allocated technology devices and user accounts.
Related Policies and Procedures	

Policy Section	**6.4 Mobile Device Management**
Rationale	Mobile devices, such as smartphones and tablet computers are important tools for the organisation and their use is leveraged to achieve business goals. However, mobile devices (personal or WCG owned) also represent a significant risk to the WCG information and data protection. If security controls are not applied to mobile devices, they can be a conduit for unauthorised access to the WCG's data and IT infrastructure. This can subsequently lead to costly data leakage.
Policy Statements	6.4.1 Only approved mobile devices will be allowed access to the WCG network and applications. 6.4.2 A separate wireless network (or Guest Network) must be allocated to mobile devices with no direct access to the WCG trusted network. 6.4.3 In order to prevent unauthorised access, mobile devices must be password protected using the features of the device and must comply with the WCG password standard.

	6.4.4 Rooted or jailbroken (e.g., iOS) mobile devices are strictly forbidden from accessing the WCG network or to run WCG applications. 6.4.5 Users must not load pirated software or illegal content onto their mobile devices. 6.4.6 Mobile devices must be kept up to date with the manufacturer or network provided patches. Patches should be checked weekly and applied at least once per month. 6.4.7 Only install applications from trusted resources. Applications can host malware that will expose passwords, credit card numbers, or anything else you type into your mobile device. 6.4.8 Any handheld device that is used in conjunction with the WCG activities, including retrieval of email and calendar data must be configured so that it can be locked or erased if lost or stolen.
Related Policies and Procedures	Mobile Device Management Policy (Draft)

7 Enforcement

The BE-I Security team 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 teams must be notified of any exceptions having a risk impact.

9 Glossary

Term	Definition
OS	Operating System
Trusted Network	A trusted network is a network of devices that are connected to each other, open only to authorised users and allows only secure data to be transmitted.
MDM	Mobile Device Management
CI's	Configuration Items
Physical Access	Access to a physical asset

Wireless Network	Computer networks that are not connected by cables
Rooted	Allows you to attain root access to the Android operating system
Jailbroken	Allows you to attain root access to the Apple operating system
End of Support Life	When a vendor does no longer support/patch a device/software/OS

10 References

- NIST Cybersecurity Framework v1.1
- National Institute of Standards and Technology (NIST) Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations
- NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organisations
- ISO/IEC 27002:2013 – Information technology, Security techniques, Code of practice for Information Security Controls
- The Centre for Internet Security (CIS) Critical Security Controls
- COBIT 5