Western Cape Government

Network Security Standard

Version 2.2 as of 03 December 2018

Contents

Document Version Control

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
17-11-2010	Deidre Marais	Draft 1.0	
29-11-2010	Deidre Marais	Draft 1.1	Define acronyms ISO, RICA and PFMA
30-11-2010	P&S	Version 1	
12-05-2011	Deidre Marais	Version 1.1	Firewall configuration using Network Address Translation.
24-02-2015	Security Team	Version 2.0	Revision and editing to conform to newer policies
16-05-2016	Security Team	Version 2.0	Annual review
16-08-2017	Security Team	Version 2.1	Amended: Legal Framework
03 -12-2018	Security Team	Version 2.1	Amended queries section

Approvals

JOB DESIGNATION	NAME	SIGNATURE	DATE
CHIEF INFORMATION OFFICER (Acting)	MR. Hilton Arendse		04/12/2018

1. PURPOSE

The purpose of this document is to formulate and define the policy and standards applicable to secure and manage communications on the Western Cape Government (WCG) network. This Standard will minimize the risk of any threats to the security of the network. The Network Security Standard represents the security "laws" that must be enforced to ensure the network is sufficiently protected. The Network Security Standard provides the foundation rules for the implementation of security controls on the network. This policy document is based on best practice considerations and guidelines. Its aim is to define the elements that are required to perform effective and secure management of the network so as to minimize the possibility of a security breach on the network.

2. SCOPE

This Information Security Standard makes provision for a set of system and manual controls to safeguard the Western Cape Government's information obtained, created or maintained by Western Cape Government employees and other parties. It covers both accidental and intentional disclosure of, and or damage to, the province and / or its suppliers' and / or clients' information.

3. LEGAL FRAMEWORK

This policy draws its mandate from the following prescripts:

- The Electronic Communications and Transactions Act (Act No. 25 of 2002)
- The Constitution of the Republic of South Africa, 1996
- The Public Service Act (Proclamation 103 of 1993) and its Regulations
- The National Strategic Intelligence Act (Act No. 39 of 1994)
- The Promotion of Access to Information Act (Act No. 2 of 2000)
- The Protection of Information Act (Act No. 84 of 1982)
- The Copyright Act (Act No. 98 of 1978)
- The Provincial Archives and Record Service of the Western Cape Act (Act No.3 of 2005)
- The State Information Technology Agency Act (Act no. 88 of 1998)
- The Minimum Information Security Standards (MISS)
- The Regulation of Interception of Communications and Provision of Communication Related Information Act (Act No. 70 of 2002)
- Minimum Information Interoperability Standards (MIOS)
- King III
- SABS/ISO 17799/ISO27k standards

4. VIOLATION AND INCIDENT REPORTING

Any breach to this policy must be reported to the Information Security Officer. Employees who fail to comply with this policy will be subject to disciplinary action in accordance with departmental and provincial disciplinary policy. The Western Cape Government shall have the right to recover from any person, any cost/expenses of whatsoever nature, including damages, that it may suffer as a result of the said person or persons acting in breach of this policy.

5. GENERAL GUIDELINES

Managers within the network environment are responsible for ensuring that personnel receive and understand the Network Security Standard.

The responsibility for host security rests with the administrator of the host system/s. The network shall be exempted and indemnified from any liability in this regard. This does not indemnify the administrators of the network from applying reasonable controls, e.g. using infrastructure components such as firewalls, to attempt to ensure that hosts are not compromised.

No non-government employees shall have access to the network except via approved controls which are administered by the IT Security team. For the purpose of this document, a "non-government" employee is defined as a person not employed in a permanent capacity by WCG. Consultants and Contractors employed in a permanent capacity are classified as WCG employees.

6. INTERNET MAIL

This standard aims to act as a guideline in setting the standards for e-mail usage to:

- ensure the optimum protection of network resources and information on the WCG network;
- ensure electronic mail usage is granted for the sole purpose of supporting organizational business activities however personal communications that are brief and do not interfere with work responsibilities are allowed;
- ensure that the transmission of information is done securely;
- ensure that periodic checks are carried out to ensure that the e-mail policy has been effectively implemented;
- provide guidance in terms of e-mail use to all WCG employees thereby ensuring that all employees know what use/abuse of e-mail entails.

- ensure emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of obscene or harassing language/images
- No contracts or firm commitments shall be entered into using e-mail.

6.1 SMTP

Electronic mail facilities shall be provided according to the standards laid down in the Request for Comments (RFCs) which define the Simple Mail Transfer Protocol (SMTP). These standards shall be strictly enforced to maintain full compatibility with all SMTP-based systems on the Internet.

6.2 MINIMUM SECURITY STANDARDS

- The WCG Messaging and Collaboration team is responsible for the installation, setup and maintenance of a SMTP compliant mail server on the Local Area Network (LAN). The mail server shall be configured to route e-mail to and from a defined mail server via an e- mail relay system.
- The user mail server shall be registered in the Domain Name Server (DNS) database before it will be able to receive e-mail via the relays.
- Inoperative or unreliable mail servers shall be removed from the network.
- Internet mail or other foreign networks shall be transported via the firewall. No user shall establish e-mail connections that bypass the firewall in any manner.
- All inbound and outbound emails are being scanned for spam messages via an email and web security gateway.
- All documents attached to email messages will be scanned for malware.
- Access to all departmental e-mail systems shall be terminated immediately when a user leaves the service of the WCG.
- WCG employees will not be able to receive or send email messages from domains that are blacklisted.

7. INTERNET

Internet usage is granted for the sole purpose of supporting organizational business activities however personal usage must be brief and should not interfere with work responsibilities. Internet connectivity shall be configured in such a way as to ensure that it does not pose a threat to WCG security. All communications systems and equipment, including Internet systems along with their associated hardware and software, shall be appropriately secured.

7.1 MINIMUM SECURITY STANDARDS

- All internet traffic must be filtered through the firewalls managed by the State Information Technology Agency (SITA).
- All connectivity paths and services that traverse the internet that is not specifically permitted will be blocked by the WCG firewall.
- Acquisition, storage, and dissemination of data that are illegal, pornographic, or which negatively depict race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth is specifically prohibited.
- All internet services such as domain registration, request for common access points, VPNC applications, applications for Customer Portals and VPN Firewall change requests must be logged via the online services catalogue portal.

7.2 TERMINATION OF ACCESS

Access to the Internet via the WCG systems and ISP shall be terminated immediately when a user leaves the service of the WCG.

7.3 DOMAIN NAMES

Registered domain names, whether or not actually used for the WCG's Web sites, are to be protected and secured in a similar manner to any other valuable WCG asset.

7.4 WEB SERVER CONFIGURATION

All Internet facing web servers must not have any direct Intranet connectivity. All servers should be hardened and patched to the latest patch levels. All servers shall operate within a single-network environment; no server will be dual-homed with multiple interfaces to a single computer system. It is recommended that if any administration of machines outside of the intranet needs to be performed, that this be performed from a machine outside the intranet. All dual homed machines in the infrastructure domain will be classified as firewall machines and should be under the control and administration of the IT security team.

7.5 WEB BROWSER CONFIGURATION

All browsers should be configured to access the Internet via the proxy server. Browser configuration must adhere to WCG Information and communications technology (ICT) Standards.

7.6 WEB BROWSER INTERFACE

The WCG has adopted the principle of all public-sector information systems being accessible through browser based technology. Other interfaces should be permitted, but only in addition to browser based ones.

8. FILE TRANSFERS

8.1 POLICY STATEMENT

A FTP-specific gateway shall only be implemented if the required security standards have been adhered to.

The following guidelines should be followed to create a secure FTP server:

- Users should only be provided necessary privileges to complete their tasks;
- Separate directories should be provided for each user;
- Executable rights should be removed when possible;
- FTP account passwords should be different than those used within the operating system;
- IP address and Port based restrictions should be placed where possible;
- Data between the client and server should be encrypted;
- FTP directories should be located outside of the web directories

9. HOST/APPLICATION ACCESS

9.1 POLICY STATEMENT

Access control standards for information systems must be established and approved by management to provide only the required access to meet the business needs. Restrictions on connection times / session lengths should be implemented to provide additional security for high-risk applications. Access to all systems must be authorized in writing by the owner of the system and recorded, detailing the access and the associated rights.

Access to information resources residing on the Intranet shall be controlled by means of a fire walling and/or proxy system.

No direct connections between external users and internal Intranet information resources shall be allowed. All access to information resources shall be via the applicable controls and only after the IT security team has determined that such access pose no or minimal threat to the network or other systems on the network. In all cases, the onus rests on the administrator of the host system to ensure that the system cannot be used as a 'springboard' from which a person may access other resources.

The onus also rests on the administrator of the host system to ensure that the host and its applications are adequately secured. System owners shall not rely on the network to provide host security. The network shall be exempted and indemnified from any liability in this regard. These conditions shall form part of the Security Undertaking that the hosting/client department will be required to sign.

10. FIREWALLS

Firewalls will be deployed at the perimeter of the network and must be aligned with the WCG Information Security Framework. The policies operate on a principle of `deny all, permit specific'. This means that unless specifically defined, no access is permitted. The policies will be documented separately, stored in a safe along with the Super-User password for the firewall and the password for an administrator account on the firewall. Any change of password on any of these systems is to be followed by the replacement of the updated information in the safe, under control of the CIO or his/her delegate. Any change to the flow control policies are to be accompanied by the relevant change control process, and the change control reference number should be documented with any changed policy rule set. Firewall logs and configurations should be backed up regularly.

No connectivity or data flow will take place from outside the network without the traffic traversing the relevant firewalls.

The firewall will be configured for network address translation. Private addresses will be used internally to WCG and public addresses for the external network.

Firewall operating systems and software will be maintained at the latest stable patch levels to keep current with any identified vulnerabilities.

11. REMOTE ACCESS

VPNC Services

Access to the WCG VPN via the use of VPN Client technologies is permitted under carefully monitored and implemented conditions. Access via means and mechanisms other than those that comply with these conditions is not permitted. The facility providing access is to be maintained as part of the GOV VPN firewall architecture by the applicable persons within SITA tasked to maintain the firewall architecture.

Access to the facility is by means of a client application loaded on specified and recorded workstations or laptop computers only. While connected to the VPN, access to any other network (including the host network) must not be possible. All sessions to the VPN service must be properly authenticated. Authentication credentials must be issued to the actual end- user of the facility, as a "real person" as defined in South African law. Access shall not be granted to fictitious or juristic persons. Sufficient personal data must be collected from the actual end-user to positively and uniquely identify that person in order to create the necessary authentication credential association.

Authentication credentials may only be issued to WCG employees for the purposes hereof, person employed by WCG on a contract basis that is normally furnished with office space and facilities in departmental premises, is to be considered an employee.

Authentication credentials are deemed to be classified information and must be treated as such in accordance with the MISS and the Protection of Information Act. No person may disclose their authentication credentials, or any part thereof, to any other person without exception.
This prohibition applies equally in respect of disclosure to other WCG employees as well as non-employees.

Access to the WCG VPN, via the VPN Client service, is for the use of WCG employees and third parties that provide support services to the WCG. Persons to whom access has been granted must ensure that their access is not used by any other person for any purpose or reason whatsoever without any exception.

A person, to whom access credentials have been issued, will be held responsible for any and all actions or activities traced back to the use of such credentials, whether or not such activities were deliberate.

Passwords, pass-phrases or other variable data required for authentication must be maintained as a manual entry and may not be stored on the workstation or laptop computer. Such variable data must meet generally accepted criteria for strength and be changed on a regular basis.

The VPN Client service shall maintain log files recording all Authentication, Access and Accounting data and such log data shall be retained in accordance with the provisions of the relevant Legislation.

12. CONNECTIONS TO AND FROM OTHER (FOREIGN) NETWORKS

Connections between third parties that require access to non-public departmental resources fall under this standard, regardless of the technology that is being used.

The DMZ Internet segment shall be utilized to provide connectivity between external 'foreign' networks (including the Internet) and the WCG network.

Direct unfiltered incoming traffic from the Extranet to the Intranet shall not be allowed.

No LAN or WAN that has a non-DMZ connection to the Internet or to any other foreign network shall be connected directly to the WCG network.

Foreign networks desiring connection to any application residing on the WCG network will connect via the DMZ and through the relevant controls. Such a connection will only be considered after the foreign network representative has completed the appropriate application for service and provided all the information required therein. All new extranet connectivity will go through a security review by the IT security team. The reviews are to ensure that all access matches the business requirements in the best possible way and that the principle of least access is followed. An application for service shall only be granted after the review has been completed and a risk analysis has been performed by the IT security team.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the IT security review. In no case will the WCG rely upon the third party to protect the network or its resources.

IP addresses for network connections via the DMZ shall be legal, globally-unique addresses. Private network addresses or stolen/duplicated addresses shall not be used.

This standard makes provision for exceptions on occasional conditions and must be approved by the Director General. All exceptions must be reflected in the IT Security Risk register.

13. INCIDENT HANDLING

Any event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, abuse, compromise of information, loss or damage of property or information shall be reported to the IT security team. This team has the mandate and is tasked with the monitoring of the network for security-related incidents which prove to be a threat to the network. Incident handling shall address internal incidents as well as those instigated by external threats.

Information relating to Information Security incidents may only be released by the CIO's office.

Security on the network is to be maintained at the highest level.

All employees should be made aware that evidence of Information Security incidents must be formally recorded and retained and escalated to the IT security team.

Plans should to be prepared, maintained and regularly tested to ensure that damage done by possible external cybercrime attacks can be minimized and that restoration takes place as quickly as possible.

The threat posed by the infiltration of a virus is high, as is the risk to the organization's systems and data files. Formal procedures for responding to any such incidents are to be developed, tested and implemented. Incident responses must be regularly reviewed and tested.

The IT security team shall disconnect any network segment which compromises network security and is in breach of the network security standard. This shall be done in conjunction with the CIO after consultation with the Directorand the IT security manager.

Any such disconnection during office hours will take place only with written confirmation by the IT Security Manager or delegate and will be followed by a comprehensive report, detailing the offence and attempts to remedy the effects and actions leading up to this last resort action.

Re-connection of the segment shall be affected as soon as the cause for the breach has been rectified and the situation normalized. Once re-connected, the above-mentioned parties shall be notified via the same channels.

In the event of less serious security breaches, the security team shall follow the same procedure and notify all parties of the breach and request corrective action within a 24-hour period. If the situation is normalized within the time-frame, all parties shall be notified accordingly and the case will be closed. If, however, no corrective action is forthcoming, the incident shall be treated in the same way as serious incidents.

14. Enforcement

Violation of this policy, (e.g., willful 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 WCG. Additionally, employees, contractors and agents who violate this policy may be subject to civil and criminal prosecution.

15. 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

- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by the Accounting Officer and the Ce-I Security Officer.