public works, roads & transport
MPUMALANGA PROVINCE
REPUBLIC OF SOUTH AFRICA

IT SECURITY POLICY SUMMARY

Table of Contents

IT SECURITY POLICY SUMMARY FOR MPUMALANGA DEPARTMENT OF PUBLIC WORKS, ROADS AND TRANSPORT

1. PURPOSE OF THE ICT SECURITY POLICY

The purpose of the ICT Security policy is to enable the Department of Public Works, Roads and Transport (DPWRT) to apply an effective and consistent level of security to all its information and information systems. Failure to comply with the policy shall be considered as misconduct and depending on the circumstances and seriousness of the offence, appropriate disciplinary action shall take place.

2. SECURITY MANAGEMENT

- Senior management supports and coordinates information security.
- Security committee addresses awareness, program management, business continuity, risk management, and audit review.

3. PERSONNEL SECURITY

- Employees accessing systems must meet security requirements.
- Non-compliance leads to immediate access termination.
- Roles and responsibilities defined in job descriptions.
- Acceptable Use Policy acknowledgment and compliance required.
- Third-party organizations need to sign a Non-Disclosure Agreement (NDA).
- Unique usernames and passwords required for DPWRT network access.
- Proper use of passwords emphasized.

4. NETWORK SECURITY

- The State Information Technology Agency (SITA) Security Policy applies to Wide Area Network (WAN) connections to DPWRT's network sites.
- Authorized LAN connections require approval.
- Strict control over secure remote access.
- Administrator passwords kept in a fireproof safe.

5. UNLICENSED AND UNAUTHORIZED SOFTWARE

- Prohibited to load illegal software on official computer.
- IT Section can remove illegal software without notice.
- Unauthorized software installation requires prior approval.

6. PHYSICAL SECURITY

- The Minimum Information Security Standard (MISS) applies.
- Server rooms access strictly controlled and restricted to authorized personnel.
- Fire prevention standards and evacuation procedures established.
- Access and removal control systems implemented for computer equipment.

7. SERVER SECURITY

- Servers hosting data located in physically secure environments with strict access control.
- Servers Loaded with approved anti-virus software and regularly updated.
- Authorized administrators granted administrative rights.
- Servers backed up according to DPWRT procedures.
- Strict access control to server rooms/ patch rooms.

8. WORKSTATION SECURITY

- Workstations located in physically protected environments with access controls.
- Loaded with approved anti-virus software.
- Users responsible for security measures and protection.
- Unattended workstations require password-protected screen savers.
- Two-factor authentication for classified information access.

9. PASSWORD SECURITY

- Strong passwords required, avoiding personal details.
- Passwords displayed and printed securely.
- Regular password changes enforced.
- Initial passwords only valid for first session, must be changed immediately.
- Account lockout after three unsuccessful logon attempts.

10. ACCEPTABLE USE

- Connecting to IT resources a privilege.
- Strong passwords and confidential treatment emphasized.
- Auto-lock login screen saver and computer locking when unattended.
- User responsibility for document backup and IT resource security.

11. PROHIBITED USE

- Unauthorized access, weak passwords, illegal software, password sharing, fraudulent activities prohibited.
- Misuse of email system and offensive messages prohibited.

12. ENCRYPTION

- Encryption required for classified information transmission.
- Non-use of encryption reported as a security breach.

13. THIRD PARTY CONNECTIONS SECURITY

- Approval required for third-party access.
- Changes monitored and analysed for risk.
- Approved changes must minimize risk to IT infrastructure.

14. FIREWALL

- Physical access to firewalls restricted.
- Rules established for incoming and outgoing services.
- Firewall logs regularly monitored for network activity analysis.
- Threat and vulnerability analysis performed regularly.

15. INFORMATION TECHNOLOGY

- IT solution procurement aligned with departmental procurement policy.
- IT officials responsible for configuration, installation, and repair.
- Users responsible for securing IT solutions and reporting faults.

16. MANAGEMENT OF IT INCIDENTS

- Incident management team formed to investigate and report incidents.
- Incidents affecting information systems escalated to IT.
- Incidents affecting physical security escalated to the Security Manager.

17. MANAGEMENT OF IT INCIDENTS

- Incident Management team formed with specific tasks.
- Incidents include network attacks, denial of services, theft, etc.

18. PRIVATE EQUIPMENT

- Private equipment allowed only for legitimate business needs with approval from the accounting officer.

19. ELECTRONIC MAIL

- Electronic communications considered property of the organization.
- Should be used for business purposes only.
- Misrepresenting or obscuring user identity is prohibited.
- Content and usage are monitored for various purposes.
- Caution when forwarding sensitive information.
- Exchange of confidential information in unencrypted form is not allowed.

20. INTERNET POLICY

- Access granted based on legitimate need with formal application.
- Connections restricted to approved Internet service provider.
- Acceptable use must be legal, ethical, and respectful.
- Authentication required through username and password system.
- Internet usage monitored by web content filtering software.
- Prohibition of misrepresenting user identity.
- Non-disclosure of internal information affecting the organization.
- Limitations on Internet use determined by supervising authority.
- Content filtering blocks inappropriate websites.
- Management reserves the right to examine computer information.

21. SOCIAL MEDIA GUIDELINES

- Refer to Government Communication policy approved by Cabinet in October 2018.

22. ROLES AND RESPONSIBILITIES

- The Accounting Officer is accountable for the policy.
- All officials and stakeholders must be aware of and adhere to the policy.

23. MONITORING AND EVALUATION

- ICT Management monitors and evaluates policy implementation.