

Presentation on IT Security Policy

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

MPUMALANGA
THE PLACE OF THE RISING SUN

Presentation Outline

- Purpose of the IT Security Policy
- Information Security Requirements
- Regulatory Framework
- CyberSecurity
- Measures to Protect Information
  - Strong Password
  - THINK Before You Click
  - Surf Securely
- Latest Cyberattack Incidents examples
- Monitoring and Evaluation

Purpose of the IT Security Policy

- To promote information protection and Systems Security.
- To protect information and information systems from loss, misuse and damage.
- To promote proper usage of IT solutions.
- To provide guidelines on the acquisition of IT solutions.

Information Security Requirements

- High availability of IT Services.
- Provide effective tools to detect, prevent and resolve information security incidents.
- Conduct regular review of existing information security measures.
- Allow important updates to install by regularly connecting to the government network.
- Maintain information security risk at an acceptance level.
- IT Security Awareness.
- IT Security incidents reporting.

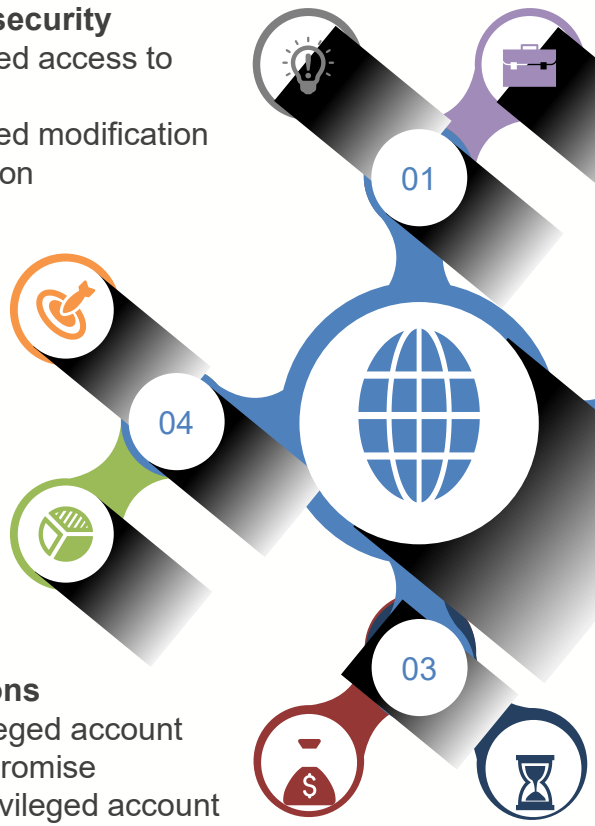
Regulatory Framework

- Communication Security Act 2002 (Act No. 68 of 2002)
- National Cybersecurity Policy Framework (NCPF)
- Electronic Communication and Transaction Act, 2000 (Act No. 25 of 2000
- Protection Of Personal Information Act (POPIA) and Information Regulator (IR)
- Public Finance Management Act 1999 (Act No.1 of 1999) and Treasury Regulations (Asset Management)

CyberSecurity 1/2

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- Cyberattacks are attempts by cyber criminals to access, change, or destroy sensitive information, extort money from users, or disrupt normal business processes.
- Examples of cyberattacks include phishing scams, malware infections, ransomware attacks, and denial-of-service (DoS) attacks.
- Businesses should be aware of the importance of implementing robust cybersecurity measures to safeguard their data and operations.

CyberSecurity 2/2



Information security
- Unauthorized access to information
- Unauthorized modification of information

Abusive Content
- Spam
  Cyberbullying
  Cyber stalking
  Child Pornography
- Violence

Fraud
- Online fake stores
- Fraudulent Domains
- Crypto Investments

Malicious Code
- Viruses
  Worms
  Trojans
  Spyware

Availability
- Denial of service
- Distributed Denial of service
- Sabotage

Information Gathering
- Scanning
  Sniffing
  Phishing
- Spoofing

Intrusions
- Privileged account compromise
- Unprivileged account compromise
- Application compromise

Intrusion attempts
- Exploitation of known vulnerabilities
- Login attempts
- New attack Signature

Measures to Protect Information

- Use strong passwords that are at least 8 characters long and include a mix of upper- and lower-case letters, symbols (special characters), and numbers.
- Regularly change your passwords and use different passwords for different systems.
- Never share your password with others.
- Install antivirus software on all your devices.
- Take advantage of self-service password reset options and avoid password sharing.
- Be cautious of any email or text message that asks for your personal or financial information and verify the legitimacy of websites before entering any personal or financial information online.
- Don't click on links in emails or text messages if you don't know the sender.
- Perform regularly backup to safeguard valuable information from loss, damage, or cyberattacks, ensuring its availability for restoration in case of accidental deletion, hardware failure, or cyber incidents.
- Always lock your computer when you leave your desk/ workstation.

Strong Password



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

the dpsa
Department: Public Service and Administration
REPUBLIC OF SOUTH AFRICA

Powered by SITA
state information technology agency

MPUMALANGA
THE PLACE OF THE RISING SUN

THINK Before You Click



the dpsa
Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

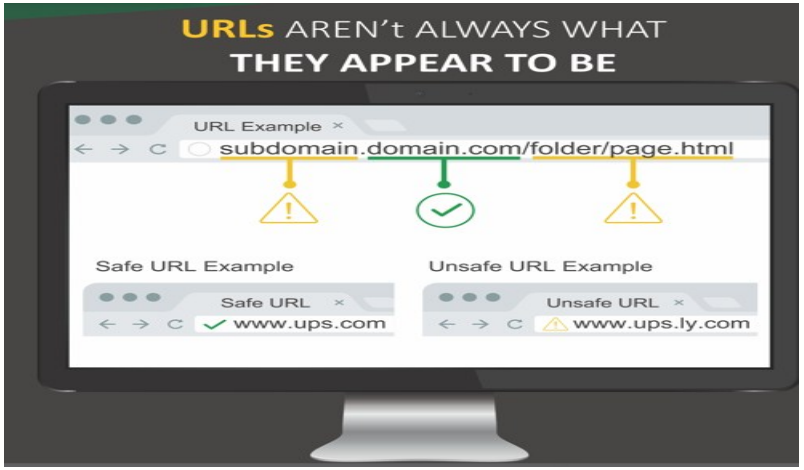
Powered by SITA
stateinformationtechnologyagency

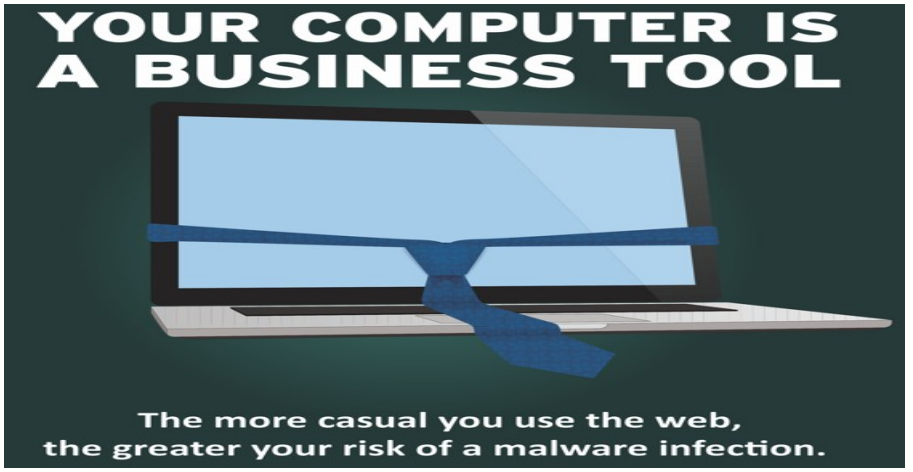
public works, roads & transport
MPUMALANGA PROVINCE
REPUBLIC OF SOUTH AFRICA

MPUMALANGA
THE PLACE OF THE RISING SUN

Surf Securely

- Surf Securely - make sure the URLs of the sites you use or shop on start with “https” not “http””
- **Why?**
- HTTPS sites are more secure.





What to do:

- T – Think before you click on links and attachments.
- H – Hover over links to see their real destination.
- I - Install only approved software.
- N – Never ignore warning signs.
- K – Keep operating systems up-to-date.

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

MPUMALANGA
THE PLACE OF THE RISING SUN

Latest Cyberattack Incidents examples

- **Ransomware -** a type of malicious software designed to block access to a computer system until a sum of money is paid. (Do not pay as you will be enabling the hackers financially to attack more people, there are no guarantees that you will have access to your data).

    - **Department of Justice:** In September 2021, the Department of Justice was hit by ransomware attack. All DOJ systems were unavailable to internal employees and members of the public .The DOJ referred to phishing emails and “drive-by downloads” as possible origins of the cyber attack.
    - **TransUnion:** Attackers demanded R225 million over 4 terabytes of data (credit scores, ID numbers and banking details).
    - **DisChem:** On 1 May 2022, an unauthorized party managed to gain access to the contents of their database, accessing personal information of over 3.6 million South Africans.

- **Other attacks:**
    - **Online scams (phishing)**: fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information.
    - **Crypto currency – (using social media):** fake trading websites and accounts.
    - **Abusive content – (digital extortion):** victims are tricked into sharing sexually compromising images which are used for blackmail.

Monitoring and Evalution

- The section shall monitor the implementation of the policy and report any deviations to the Head of Department.

- Information Security is everyone's responsibility!


Thank you!