

# MPUMALANGA PROVINCIAL GOVERNMENT

No. 7 Government Boulevard  
Building No 4, Upper Ground  
Riverside Park  
Extension 2  
NELSPRUIT, 1200



Private Bag X 11205  
NELSPRUIT, 1200  
Tel: (013) 766 4228  
Fax: (013) 766 9406  
e-mail emashile@nel.mpu.gov.za

## Department of Finance

Litiko LeteTimali

UmNyango weZeemali

Departement van Finansies

Kgoro ya Matlotlo

Enquiries : Mr ZR Mkhathswa  
Tel (013) 766 4429

### PROVINCIAL TREASURY CIRCULAR 3 OF 2008

**TO: Heads of Departments  
Chief Financial Officers**

1. The National intelligence Agency (NIA) has through recent investigations identified in a number of organs that criminal syndicates are utilizing key logging software and similar devices to surreptitiously obtain user credentials. The criminals subsequently utilise these credentials to access information systems under the guise of legitimate users and fraudulently obtain benefit, thereby defrauding the State.
2. Key logging software and devices operate through all key entries. These key entries may be recorded in either a file on the victim's computer, or recorded on a physical device that is attached to the computer. Criminals subsequently scan the contents of these recorded files to identify user credentials and passwords that can be used to gain access.
3. To mitigate against the risks of key loggers being used, NIA has identified the following countermeasures that should be adopted by personnel in all Departments:-
  - Do not click on any links that may be included in any electronic mails.
  - Do not access or utilise any peer to peer sharing network to share files or install any file swapping software.
  - User credentials should only be utilised to, and / or under the control of the personal whose user credentials are being utilised.
  - Ensure that anti-spyware software is utilised, in conjunction with the implementation of all the service packs and patches for all installed software.
  - Ensure that all of the security levels on the Internet Browser setting are set to medium or higher.


*"Always Stretching Our Arm, to Accelerate Service Delivery"*

- Attachments, whether they are transmitted through electronic mail and/ or through physical electronic media (e.g. USB devices) should only be opened after they have been scanned by an up to date anti-virus programme with the latest definitions.
- Executable files should never be open except on a stand alone, quarantined computer that is not connected to the Province's computer network.
- No content should be downloaded and opened from web sites, without their content having been examined by an up to date anti-virus programme with the latest definitions.
- To protect against key logger devices, it is necessary to ensure that effective physical security is maintained. Personnel should scrutinise their workstations to establish whether there has been any evidence of tampering, or the addition of any unknown hardware devices. This should be reported to the Security Manager
- Consideration should be given to whether or not all users who access the Internet require such functionality and whether or not this functionality can be segregated from the internal network.

4. IT Components in all Departments should ensure that:-

- Default user identifiers and passwords for all information technology and communication equipment should be changed monthly.
- Administrative user identifiers and passwords should under no circumstances be shared, and should be assigned on a per administrator basis.
- All remote access must be undertaken using secure remote access and not through the use of Telnet functionality.
- All servers and workstations should be regularly inspected to ensure that rootkits have not been installed.
- In instances, where Dynamic Host Configuration Protocol (DHCP) is being used, the number of network masks and subnets should be optimised to the number of authorised network users.
- The lease period for any Internet Protocol (IP) addresses issued should also be increased to a minimum of 14 days.

5. Should any department identify that key loggers are being used in their environment this should be reported to NIA.

  
 \_\_\_\_\_  
**MRS TSHUKUDU**  
**HEAD OF DEPARTMENT**  
**DATE: 3/07/2008.**