3.8 User Policy

3.8.1 Password Policy

Password to the Electronic Government server storing payroll data was easily guessed hence payroll data of all civil servants were captured and then displayed on the internet

Audience All users

Policy All hardware passwords and software passwords should be secured to prevent any compromise by unauthorized persons.

Standard All passwords should be non trivial, periodically changed, and not easily accessible.

Procedure

All passwords must be created, changed and protected as follows :

Creation of Password

A password must be :

- at least 8 characters in length.
- a combination of upper and lower-case alphabets, numbers and special characters.
- NOT the same as or similar to any personal information of user.
- NOT a word in any dictionary, language and jargon.

Change of Password

- Any new password received must be changed immediately upon the first login.
- Password must be changed immediately when suspected of being compromised.
- All changed password must comply with Creation of Password procedure.
- Password must be changed at least once in every 6 months.
- The same password must never be used more than once.

Protection of Password

- Password must not be written down or stored electronically.
- Password must not be hinted to anyone. (e.g. “my family name”, “my pet’s name”, etc.)
- Password must not be revealed in any manner (e.g. over phone, SMS, email, messenger, questionnaires / security forms, etc) to anyone.
- “Remember Password” feature of applications (e.g. Internet Explorer, Firefox, Opera, Messenger, Netscape, Eudora, Outlook etc.) must not be enabled.

Guidelines

1. Combination of password may include:
   i. Upper case: A – Z
   ii. Lower case: a – z
   iii. Numbers: 0 – 9
   iv. Special characters: ~!@#$%^&*()_+<>?;:[]\

2. Examples of weak passwords:
   i. Names of family, pets, friends, co-workers
   ii. Computer terms and names, sites, companies, hardware, software
   iii. Birthday, addresses, phone numbers, car plate number