

# Password management

## Source policy

These Guidelines support and must be read in conjunction with the following:

- VPMP Information access
- VPMP Appropriate use of information
- VPMG Information system access

## Application

Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Guidelines.

Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Guidelines, the Guidelines must be used to help make decisions in support of the rules.

## Guidelines

### 1. Password controls

- As required under the Authorised User responsibilities in **VPMP Appropriate use of information** passwords must not be shared or discussed. Individuals are accountable for the activities performed using their security credentials.
- Passwords must be changed at least every 90 days. The majority of Victoria Police information systems are designed to prompt authorised users of this requirement.

### 2. Password creation

Authorised users who have been granted access to Victoria Police information systems are responsible for taking appropriate steps to secure the password they create.

### 3. Password standards

As required by **VPMP Information access** authorised users are to comply with the following standards (as well as the 'password complexity business rules' in section 4) when creating a new password.

#### 3.1 Local Area Network (LAN)

- The LAN password is to be changed prior to updating any passwords on other Victoria Police applications.
- Once the LAN password has been updated, authorised users are then to enter the new LAN password (i.e. the same password) in each one of the applications authorised for their use except Mobile Data Terminals (MDTs).
  - Due to MDTs operating on a non Victoria Police network a different password (still complying with the password complexity business rules) is to be entered when logging on.

#### 3.2 MDTs

- MDT users require two passwords:
  - MDT password; and
  - LEAP Password, which will be your normal LEAP password as used by the Station PCs as this data is encrypted on the Mobile Data Network
  - Apart from this one exception (of logging onto LEAP through the MTD) the LAN password must not be used on internet based or non Victoria Police applications or systems.

### 4. Password complexity business rules

For compatibility across all Victoria Police systems (as well as the separate password for the MDT), the following business rules are to be adopted:

| Business rule | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| 1             | At least 1 or more uppercase alpha characters (eg. A – Z)                   |
| 2             | At least 1 or more lowercase alpha characters (eg. a – z)                   |
| 3             | At least 1 numeric (eg. 0 – 9)                                              |
| 4             | At least 1 special character (* Note: See below)                            |
| 5             | At least 5 other characters (uppercase, lowercase, numeric or special)      |
| 6             | Do not include blanks within the password                                   |
| 7             | No more than 2 identical characters may be used in a row                    |
| 8             | Password lengths: Minimum 9 characters. Maximum 11 characters               |
| 9             | A minimum of 24 separate passwords must be used before they can be repeated |

|                                 |                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>10</b>                       | Passwords should not end in a numeric.                                                                 |
| <b>Password Format Examples</b> | vicToria5@s ; tobenot2B& ; 42Long&song ; 594?Katop<br><b>Please do not use these example passwords</b> |

Only the following special characters may be used: ! % ^ & \* ( ) + = ? \$ @ #

## Further advice and information

For further advice and assistance regarding these Procedures and Guidelines, contact Protective Security or your supervisor.

## Update history

|                            |                                                                                    |                          |
|----------------------------|------------------------------------------------------------------------------------|--------------------------|
| <b>Date of first issue</b> | 22/02/10                                                                           |                          |
| <b>Date updated</b>        | <b>Summary of change</b>                                                           | <b>Force file number</b> |
| 23/09/2013                 | Incorporation of 'Password complexity business rules' and supporting amendments    | 073882/12                |
| 25/03/2019                 | Administrative amendment to reflect name change from IMSSD to Protective Security. | FF-139207                |
|                            |                                                                                    |                          |
|                            |                                                                                    |                          |
|                            |                                                                                    |                          |