System access for specific groups

Source Policy

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

- VPMP Information access
- Standards for Victoria Police law enforcement data security

Application

Procedures and 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 Procedures and Guidelines.

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

Procedures and Guidelines

1. General

- In accordance with **VPMP Information access**, this document details the various mandatory procedures for specific groups of authorised personnel to be granted system access in order to perform specific approved functions.
- It covers the granting of system access to Work Unit Manager, Authorised Investigators, Corporate Management Review Division (CMRD) personnel and IT Coordinators.

2. Access to personal directories

In all cases access to the personal drive of another person must only be granted for a specific period of time sufficient to complete the specified enquiry and be READ-ONLY.

2.1 Access by Work Unit Managers

- Work Unit Managers may access the personal directory of another person under their direct supervision provided they:
  - have a legitimate business reason to do so
  - have made every reasonable effort to contact the person concerned, stating the reason for the request and documenting that effort for audit and review purposes
  - obtain written authority from their manager via a BITS Service Request [Form 1234] stipulating:
    - reason for the access
    - activity to be carried out
    - length of time access is required so that access is removed on the task is completed

- On the return of the person concerned the Work Unit Manager must advise them that access was granted and the purpose for which it was granted.

2.2 Access by authorised investigators

- An authorised investigator is any person authorised by the Tasking and Coordination Group, Professional Standards Command (PSC) or a Regional/Departmental Professional Development Committee to undertake or support an investigation. Access will be removed once the investigation is completed.

- Such individuals may access the personal directory of another person provided they:
  - have a legitimate business reason to do so (such as a criminal and/or disciplinary investigation)
  - submit a Data Request [Form 1351].

- Forms 1351 to be approved by:
  - Superintendent, Investigations – for an PSC authorised investigation
  - their Superintendent or nominated Regional/Departmental Professional Development Committee member – for a Regional/Departmental authorised investigation.

2.3 Access by CMRD

Authorised employees of CMRD may access the personal directory of another person provided they:

- have a legitimate reason for doing so (such as part of an authorised audit task)

- obtain written authority from their Department Head via a Form 1234 stipulating:
  - reason for the access
  - activity to be carried out

- length of time access is required so that access is removed when the task is completed.

3. Access by IT co-ordinators to shared and personal directories

3.1 General

- IT Coordinators may access shared and personal directories for data administration purposes (i.e. to identify and reduce the overflow of information stored on IT infrastructure servers) provided that the directories are within their authorised control.

- Access should only be granted for a specific period of time sufficient to complete the specific data administration task and be READ-DELETE ONLY.

- Access granted to an IT Coordinator cannot be used for the purpose of criminal and/or disciplinary investigation, or other activity unrelated to data administration.

- If an IT Coordinator becomes aware of a file or information that appears suspect, refer the matter to PSC for investigation, as required by **VPMP Information access**.

3.2 Access to shared directories

IT Coordinators may access shared directories for data administration purposes provided they:

- have a legitimate business reason to do so (such as an operational imperative)

- obtain written authority from their Department Head via a Form 1234, stipulating:
  - reason for the access
  - activity to be carried out
  - length of time access is required

- record any actions affected by the remediation activity and ensure the records are available for audit review purposes. The records need to be co-signed by the authorising Department Head.

3.3 Access to personal directories

IT Coordinators may access personal directories for data administration purposes provided they:

- have a legitimate business reason to do so (such as an operational imperative)

- have made every reasonable effort to contact the persons concerned stating the reason for the request and documenting that effort for audit and review purposes

- obtain written authority from their Department Head via a Form 1234 detailing:
  - reason for the access
  - activity to be carried out
  - length of time access is required
  - a notation that every effort was made to contact the persons concerned, for audit and review purposes

- on return of the person concerned they advise them access was granted and the purpose for which it was granted

- record any actions affected by the remediation activity and ensure the records are available for audit review purposes. The records need to be co-signed by the authorising Department Head.

Further Advice and Information

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

Update history

Date of first issue	22/02/10	
Date updated	**Summary of change**	**Force File number**
21/01/13	Updated to reflect organisational governance and structural changes.	FF-074790
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207