



OFFICIAL: Sensitive

GENERAL ORDER DIGITAL EVIDENCE

General Order title	Digital evidence
Date of issue	14 June 2023
Date of operation	29 May 2023
Review date	May 2026
Review responsibility	Officer in Charge Financial and Cybercrime Investigation Branch
Replaces	General Order, Digital evidence
PCO reference	2007/2211
Gazette reference	SAPG 105/23
Enquiries to	Manager, Digital Evidence Section
Corporate Policy Sponsor	Assistant Commissioner, Crime Service

General Orders provide an employee with instructions to ensure organisational standards are maintained consistent with SAPOL's vision. To this end, General Orders are issued to assist an employee to effectively and efficiently perform their duties. It is important that an employee constantly bears in mind that the extent of their compliance with General Orders may have legal consequences.

Most orders, as is indicated by the form in which they are expressed, are mandatory and must be followed. However, not all situations encountered by an employee can be managed without some form of guidance and so some of these orders are prepared as guidelines, which should be applied using reason. An appendix to a General Order will be regarded as part of the General Order to which it relates. At all times an employee is expected to act ethically and with integrity and to be in a position to explain their actions. Deviation from these orders without justification may attract disciplinary action.

To ensure best practice an employee should be conversant with the contents of General Orders.

The contents of General Orders must not be divulged to any person not officially connected with SAPOL. Requests for General Orders will be managed as follows:

- Civil subpoena and disclosure requests—contact the Information Release Unit.
- Criminal subpoena and disclosure requests—refer to General Order, **Disclosure compliance and subpoena management**.
- Freedom of information requests—contact the Freedom of Information Unit.
- Any other requests (including requests by employees)—refer to instructions provided within General Order, **Corporate policy framework, 5. GENERAL ORDER REQUESTS/RELEASE**.

CONTENTS

1. GENERAL ORDER STATEMENT..... 3

Scope..... 3

2. SEIZING DIGITAL EVIDENCE..... 3

4(2)(a)(iii) and 4(2)(b)

5. CLOSED CIRCUIT TELEVISION 6

Photographs from video tape cassettes and digital media..... 6

Delivering video tape cassettes and digital media 7

Chain of evidence 7

6. ANALYSIS OF DIGITAL EVIDENCE 7

4(2)(a)(iii) and 4(2)(b)

8. CRYPTOCURRENCY..... 10

9. REFERENCES 11

10. DOCUMENT HISTORY SINCE 12/08/2009 11

1. GENERAL ORDER STATEMENT

South Australia Police (SAPOL) is committed to the delivery of dedicated and professional forensic services by effectively and efficiently managing all digital evidence that is seized or otherwise taken into the custody of an employee of SAPOL.

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.

Scope

This General Order applies to all employees of South Australia Police (SAPOL).

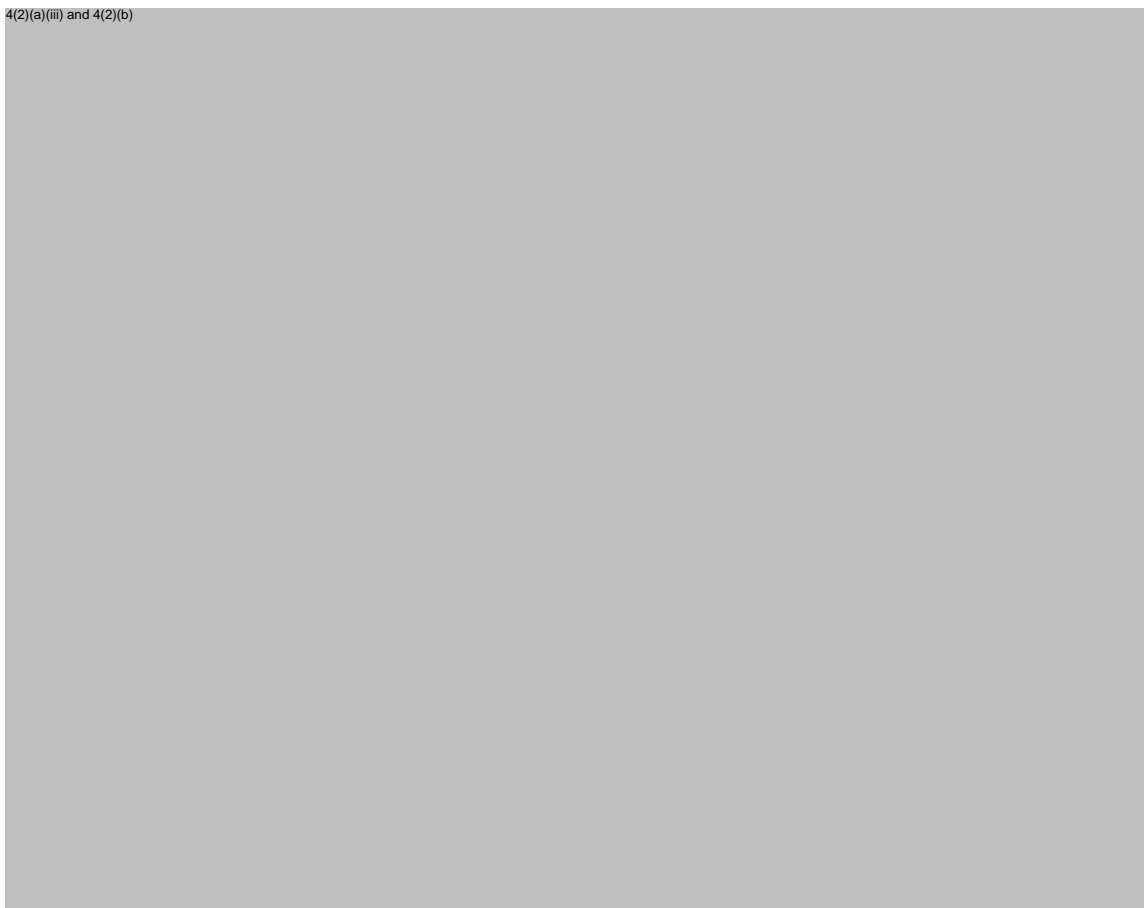
2. SEIZING DIGITAL EVIDENCE

In many investigations, members will seize digital evidence in the form of computers and other electronic devices. In such investigations a plan should be developed in relation to the identification, preservation and seizure of that evidence. As part of that planning process, the Digital Evidence Section (DES) can provide specialist advice prior to the commencement of any operation.

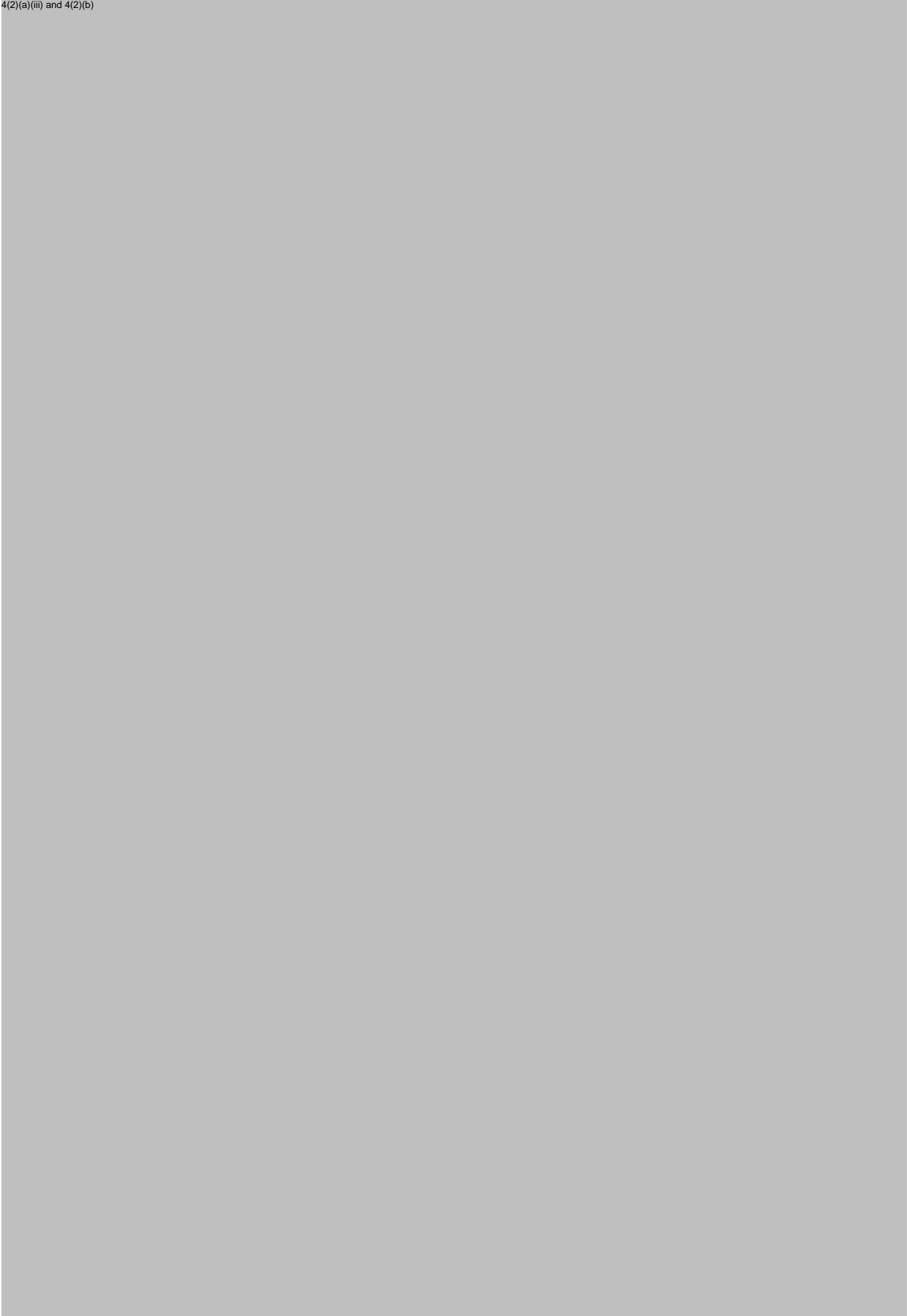
Advice and support is available from the DES in respect to the investigation, identification, seizure, preservation, analysis and presentation of digital evidence. The DES may provide a digital evidence analysis service in respect to exhibits seized by a member.

In instances where members seize computers and other electronic devices, the following guidelines apply:

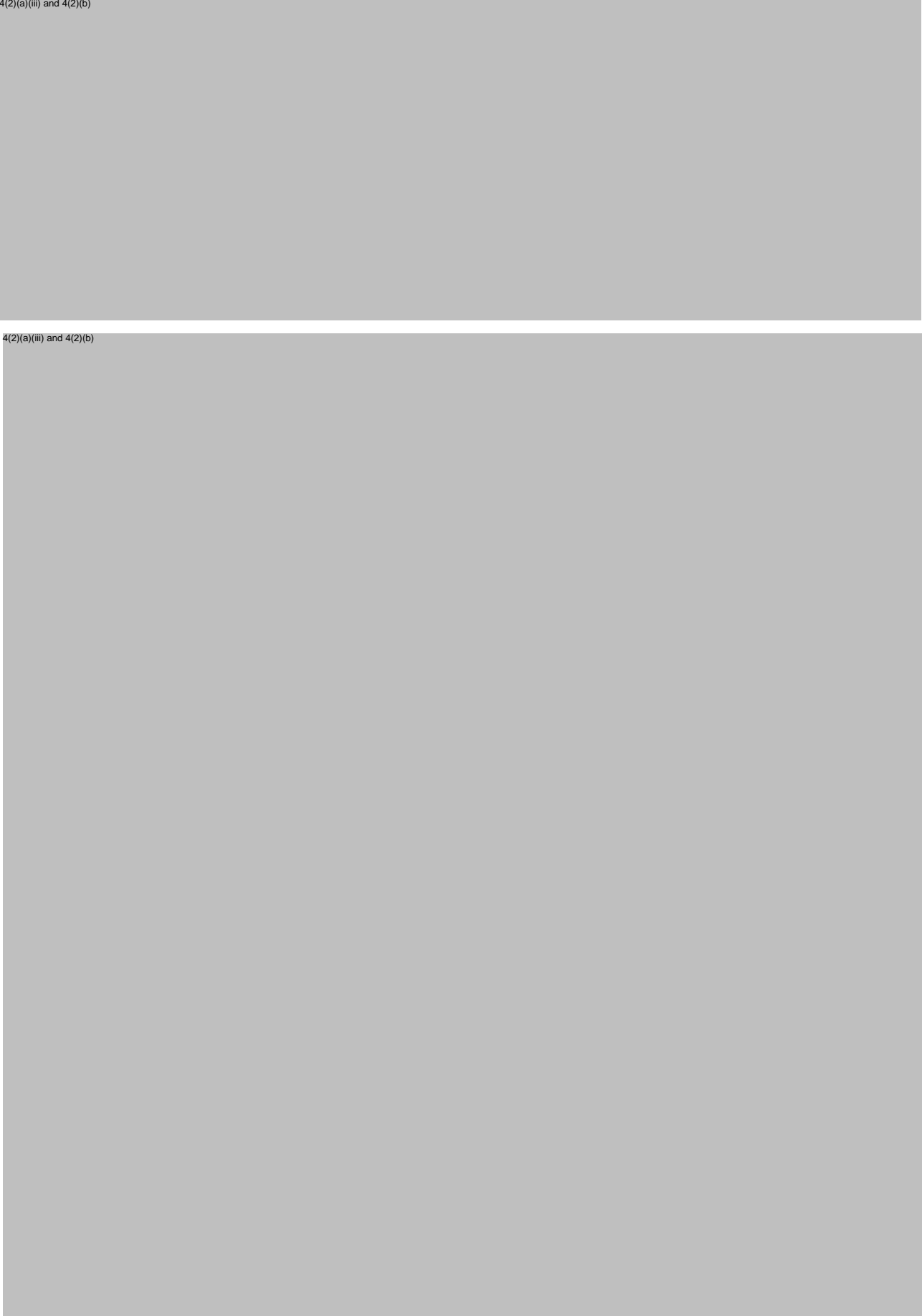
4(2)(a)(iii) and 4(2)(b)



4(2)(a)(iii) and 4(2)(b)



4(2)(a)(iii) and 4(2)(b)



4(2)(a)(iii) and 4(2)(b)

5. CLOSED CIRCUIT TELEVISION

Many institutions/agencies/members of the public have surveillance camera systems which either operate continually or are activated manually.

The equipment can record:

- suspects entering and leaving
- people committing armed hold-ups or other offences
- other incidents requiring action by SAPOL.

Some older systems may record the footage to video tape but it is more likely the footage is saved in digital format to data storage either at the location of the system or at another location.

Where incidents have been recorded in some way, the investigating member or other nominated member must obtain a copy of the incident on DVD, hard drive or other form of digital storage device.

The following applies:


- an authorised person from the company or premises involved should facilitate the copying of the required footage
- CCTV footage may be collected using a SAPOL-issued portable storage device (including USB drives) which have been issued specifically for CCTV collection
- third party portable storage devices **must not** be accepted (including USB drives)—refer to General Order 8450, **Information technology management, Portable computing and data storage**
- where the recording equipment is maintained by security firms who install and service the system, a representative of the security firm should assist with obtaining a copy
- in all cases, the seizing member should ensure that footage is suitable for viewing by standard computer hardware and software and to facilitate this, a copy of any proprietary reader program (where required) should be included with the copied footage
- where such copying is difficult or an appropriate medium is not readily available, advice should be sought from the DES.

When a copy of the incident has been obtained the seizing member should:

- identify the cassette, DVD, hard drive or other media with the member's name, date and time of collection, who copied and details sufficient to identify the location and incident
- ensure the medium has been marked and dealt with in accordance with General Order, **Property**.

It is preferable (for quality and integrity reasons) for the footage to be supplied in the proprietary format with a reader supplied.

4(2)(a)(iii) and 4(2)(b)



4(2)(a)(iii) and 4(2)(b)

Delivering video tape cassettes and digital media

Exhibit video tape cassettes and digital media containing evidentiary footage must not be forwarded through the internal despatch system.

When video tape is the recording medium used, where possible ensure that original video tapes are provided for processing. A member must not unnecessarily replay an original video tape prior to having still images or additional copies made.

Video tape cassettes, CD, DVD and other electronic media for processing are to be submitted to the DES. Before video tape cassettes, CD, DVD and other electronic media are submitted to the DES for processing a [Request for Examination of Digital Evidence](#) form must be completed and include the following information:

- Shield occurrence number
- offence details
- date of offence
- victim/suspect details
- name, identification number, contact phone number and posting of the member in charge of the case
- precise details as to where the incident/suspect appears on the video tape or other media as indicated by the time(s) appearing on the footage
- description of the suspect/incident
- precise details of the end product required (for example full page print or electronic files).

The DES must also be advised of the following:

- whether the video tape is a multiplex or multi-screen image
- the brand, type and format of the recording system
- the security company responsible for the installation of the system.

Chain of evidence

Whenever a member removes or seizes video tape cassettes or digital media they must ensure the chain of evidence is maintained and documented in accordance with General Order, **Property**.

6. ANALYSIS OF DIGITAL EVIDENCE

The DES is responsible for the analysis of digital evidence. Members seeking analysis of digital evidence are to complete a [Request for Examination of Digital Evidence](#) form. The form is to be emailed to the DES at sapol.digitalevidencerequest@police.sa.gov.au.

When submitting a request for digital evidence analysis, investigating members must supply the following information:

- particulars of the investigating member and their supervisor
- the offence under investigation
- a brief synopsis of the investigation relevant to the DES
- the expected forensic outcome and details of any specific evidentiary requirements
- critical dates
- keywords, user names, et cetera, to be used in a search criteria in the analysis phase
- PIN or PUK codes identified during the course of the investigation
- identified hazards associated with the exhibits
- identified risk factors to victims, witnesses or SAPOL
- other relevant information.

Upon receipt, the request will be entered into the DES database and the submitting member will be advised of the allocated DES request number. The type and/or urgency of the request will determine analysis priority. Investigating members will be contacted and advised when the exhibit property is to be taken to the DES.

In the normal course of events exhibits will be accepted at the DES between 9 am and 4 pm Monday to Friday.

Unless exceptional circumstances exist, the DES will not accept exhibits until a [Request for Examination of Digital Evidence](#) form has been submitted and assessed.

Electronic exhibits seized by members and requiring examination may be progressed by analysis or review. The following applies:


- **Analysis**—the full analysis of exhibits relating to a request may be lengthy and as such members should seek direction from DES employees as to possible time frames in order to keep prosecutors apprised.
- **Review**—matters determined as reviews are those where the request for analysis requires the identification of certain data such as images or documents. No interpretation of the data other than identifying its presence and possibly extracting the data to other media is required.

Reviews are able to be conducted at terminals linked through the Distributed review system (DRS) at the following locations:


- Metropolitan
 - Northern District (Elizabeth Police Station)
 - Southern District (Christies Beach Police Station)
 - Western District (Port Adelaide Police Station)
 - Eastern District (DES—two terminals).
- Regional
 - Barossa LSA (Gawler Police Station)
 - Eyre Western LSA (Ceduna, Port Lincoln and Whyalla Police Stations)

- Far North LSA (Port Augusta Police Station)
- Hills Fleurieu LSA (Mount Barker and Victor Harbor Police Stations)
- Limestone Coast LSA (Mount Gambier Police Station)
- Murray Mallee LSA (Berri and Murray Bridge Police Stations)
- Yorke Mid North LSA (Port Pirie Police Station).


4(2)(a)(iii) and 4(2)(b)



4(2)(a)(iii) and 4(2)(b)



4(2)(a)(iii) and 4(2)(b)



8. CRYPTOCURRENCY

Cryptocurrency is a digital currency, which is an alternative form of payment, created using an encryption algorithm. The Financial and Cybercrime Investigation Branch (FCIB) members are the only SAPOL personnel authorised to seize cryptocurrency.

FCIB members are well situated to assist investigators in the identification of best evidence, scene triaging of devices, exhibit collection processes, and general advice on the identification, handling and collection of digital exhibits. Always ensure a FCIB member is consulted during any investigation where the seizure of cryptocurrency is contemplated.

Guides to assist in investigations involving cryptocurrency are also available on the [FCIB intranet site](#).

9. REFERENCES

General Order 8450, **Information technology management, Portable computing and data storage**

General Order, **Photographs**

General Order, **Property**

[Major investigation emergency response plan](#)

[Property management manual](#)

[Request for Examination of Digital Evidence](#) form

10. DOCUMENT HISTORY SINCE 12/08/2009

Gazette reference (SAPG)	Date	Action (amendment/deletion/new/review/temporary variation)
267/09	12/08/09	Review 2009.
408/10	1/12/10	Review 2010.
31/12	25/01/12	Amendment—deleted references to General Order 8460, Serious crime plan and inserted Major investigation emergency response plan.
116/12	02/05/12	Amendment—reference to General Order, Exhibits deleted and replaced with General Order, Property .
115/13	29/05/13	Amendment—insertion of text at 3. SEIZING ELECTRONIC EVIDENCE and 4(2)(a)(iii) and 4(2)(b) . Heading 5. PERSONAL DIGITAL ASSISTANTS and text deleted.
51/14	19/02/14	Review 2013—amendment of 5. CLOSED CIRCUIT TELEVISION .
150/18	04/07/18	Amendment—district policing model implementation.
49/20	11/03/20	Review 2020—including implementation of Financial and Cybercrime Investigation Branch and renaming of the General Order.
83/22	04/05/22	Amendment—amendments at 5. CLOSED CIRCUIT TELEVISION to include information removed from General Order, Photographs
105/23	14/06/23	Review 2023—references to PPMS deleted and replaced with Shield. Insertion of text at 4(2)(a)(iii) and 4(2)(b) , 5. CLOSED CIRCUIT TELEVISION , and 4(2)(a)(iii) and 4(2)(b) . Insertion of 8. CRYPTOCURRENCY .

APPROVED BY COMMISSIONER/DEPUTY

.....
Print Full Name

.....
ID Number

.....
Signature

29/5/23
Date

Documentation certification and verification

General Order draft—prepared by: Detective Sergeant Martin Burke, Cybercrime Investigation Section, Crime Service

General Order—verified by: Detective Senior Sergeant First Class Jamie Dolan, Manager, Digital Evidence Section, Crime Service