

National Police Reference System – Persons Business Practice Management Agreement

Between

New South Wales Police, Victoria Police, Queensland Police, Western
Australia Police, South Australia Police, Northern Territory Police,
Tasmania Police, ACT Policing, Australian Federal Police and The
CrimTrac Agency



Table of Contents

1.	Introduction	5
1.1.	Scope of this agreement.....	5
1.1.1	Services.....	5
1.1.2	Standards and Processes	5
1.1.3	NPRS information.....	6
1.2.	Out of scope	6
1.3.	Objectives.....	6
1.4.	Participating Australian Police Jurisdictions	7
2.	Interpretation.....	8
3.	Provision and consumption services covered under this agreement.....	9
3.1.	Provisioning and storage of NPRS data	9
3.1.1	Acceptable NPRS payload	9
3.1.2	CrimTrac processes for data provision.....	9
3.1.3	Jurisdictional processes for data provision.....	9
3.1.4	CrimTrac provisioning and hosting responsibilities	10
3.1.5	Participating Australian Police Jurisdiction provisioning responsibilities	11
3.1.6	Data ownership and accuracy	11
3.2.	Consumption of NPRS data	12
3.2.1	Consumption services provided by CrimTrac.....	12
3.2.2	PAPJ consumption considerations.....	12
3.2.3	NPRS consumption dependencies.....	12
3.2.4	Consumption performance	13
4.	Supporting services covered by this agreement.....	14
4.1.	Auditing.....	14
4.1.1	CrimTrac responsibilities	14
4.1.2	PAPJ responsibilities.....	14
4.2.	Service Desk support	15
4.2.1	CrimTrac Customer Support Services.....	15
4.2.2	Incident management.....	15
4.2.3	Problem resolution	15
4.2.4	Definitions of priority, impact and urgency	17
4.2.5	Prioritisation of incidents	17
4.2.6	Escalation of incidents.....	17
4.2.7	PAPJs Service Desk responsibilities	18
4.3.	System availability	18
4.3.1	Target availability	18
4.3.2	Calculation of service availability.....	19
4.3.3	Notification of planned outages	19

4.3.4	Maintenance windows	19
4.4.	Backup and Restoration	19
4.4.1	CrimTrac responsibilities	19
4.4.2	PAPJ responsibilities.....	20
4.4.3	Shared backup and restoration procedures	20
5.	Supporting standards used by this agreement	21
5.1.	Security.....	21
5.1.1	System Security	21
5.1.2	User security	21
5.1.3	Commonwealth security obligations.....	22
5.1.4	Access authorisation	22
5.2.	Legislative constraints	22
5.2.1	Supply of information to CrimTrac.....	22
5.2.2	Use of NPRS information within PAPJs	22
5.2.3	Privacy Principles	22
5.2.4	Freedom of Information	22
5.2.5	Records Management.....	23
5.3.	NPRS as a non-authoritative source	23
6.	Management processes	24
6.1.	Change management.....	24
6.1.1	Procedures	24
6.1.2	Notifications.....	24
6.2.	Consultation.....	24
6.3.	Dispute resolution.....	24
6.4.	Reviews and Improvement.....	25
6.5.	Termination of Agreement.....	25
7.	Signatories.....	26

Figures

Figure One: Provisioning.....	11
Figure Two: Consumption.....	14
Figure Three: Network boundaries.....	19

Tables

Table One: Search performance.....	14
Table Two: Response times.....	17
Table Three: Recording requirements.....	17
Table Four: Priority levels.....	18

Documents Referenced

- CrimTrac Change Management Strategy Version 2
- Service Transition Standard Process Procedures (Version 1)
- Australian Government Information Technology Security Manual – ACSI 33
- Australian Government Protective Security Manual (PSM)
- CrimTrac Communications Plan 2008
- CrimTrac Security Policy
- Agency Partnership Memorandum of Understanding (MOU)
- Inter-Governmental Agreement (IGA)
- NPRS (MNPP) Interoperability Document (Parts 1-6)

1. Introduction

This Business Practice Management Agreement (BPMA) in conjunction with the Partnership Memorandum of Understanding (MOU) frames the agreement between CrimTrac and Australian police jurisdictions participating in the National Police Reference System (NPRS).

The purpose of the BPMA is to provide a high level document detailing the mutually agreed scope, principles, processes and responsibilities which will allow all participating agencies to manage NPRS effectively; and to encourage best efforts by all parties. This document will be reviewed on an ongoing basis as other services come within CrimTrac's ambit.

The BPMA describes the responsibilities of all parties involved, and some of the performance levels that jurisdictions and CrimTrac will aim to achieve through best efforts. It does not prescribe required levels of performance and it is not intended to perform the role of a Service Level Agreement (SLA). Rather, the BPMA provides the basic principles needed to cooperatively share information using NPRS and is intended to be the basis upon which an SLA can be developed as the system and its usage matures.

Consequently the BPMA, by design, does not impose or suggest binding commitments to any of the participating agencies; however it does detail the ideal levels of service and necessary processes to support the sustainable operation of NPRS now and into the foreseeable future.

1.1. Scope of this agreement

1.1.1 Services

The scope of this document specifically deals with the use of NPRS for the exchange of NPRS persons information in accordance with the CrimTrac Agency's deliverable under the Inter-Governmental Agreement (IGA) i.e.: *"the provision of rapid access to national operational policing data"*. Accordingly, this agreement covers the following services:

- a. Provisioning and storage of NPRS persons information sent by participating Australian police jurisdictions (detailed in Section 3);
- b. Exchange of NPRS persons information between participating Australian police jurisdictions i.e. consumption of NPRS persons information (detailed in Section 3); and
- c. Ongoing support and development of the NPRS system and the management of related business processes between participating Australian police jurisdictions and the CrimTrac Agency (detailed in Section 4).

1.1.2 Standards and Processes

The scope of this agreement also includes the necessary standards and processes that are needed to support the services listed above in clause 1.1.1. These include:

- a. security
- b. dispute management and
- c. change management.

These standards and processes are detailed in Sections 5 and 6 respectively.

1.1.3 NPRS information

Under the scope of this agreement, the sharing and use of information contained within NPRS is limited to persons information which would be needed by police in the course of their duties, to determine if a person is:

- a. a threat to police
- b. a threat to the public
- c. a threat to themselves
- d. of interest to police or
- e. wanted by police.

1.2. Out of scope

As of 15 February 2009, the scope of this agreement is limited to all functions of police as determined by operational need and does not include the use of NPRS Persons information for the purposes of criminal history checking or access by non-police law enforcement agencies. All payloads other than persons are also out of scope.

1.3. Objectives

The central premise of this agreement is to foster a sustainable operational environment for NPRS which encourages the mutual best efforts of all participating agencies. Whilst this agreement does not hold any party to a given level of performance, it is designed to support and encourage the achievement of the following objectives:

- a. increased capability in delivering policing services that enhance community safety;
- b. increased police confidence in their ability to deal with field incidents, persons in custody and investigations;
- c. increased efficiencies and effectiveness in law enforcement through enhanced information exchange between police jurisdictions; and
- d. CrimTrac compliance with IGA deliverables to be able to support future information exchange between police jurisdictions.

1.4. Participating Australian Police Jurisdictions

In addition to the CrimTrac Agency, the following police services are included in this agreement under the term Participating Australian Police Jurisdictions (PAPJ):

ACT Police	(ACTPOL)
Australian Federal Police	(AFP)
New South Wales Police	(NSWPOL)
Northern Territory Police	(NTPOL)
Queensland Police	(QPOL)
South Australia Police	(SAPOL)
Tasmania Police	(TASPOL)
Victoria Police	(VICPOL)
Western Australia Police	(WAPOL)

2. Interpretation

Words, phrases and concepts used in this agreement:

Business Practice Management Agreement (the agreement) refers to this document;

Common Information Model means the data entities and elements and their semantic and technical features to be exchanged, as agreed between PAPJ and CrimTrac;

CrimTrac Board of Management means the CrimTrac Board of Management established by the Inter-Governmental Agreement;

Inter-Governmental Agreement (IGA) means the agreement of 2000 between the Commonwealth and the States and Territories of Australia for the establishment and operation of CrimTrac;

Participating Australian Police Jurisdictions (PAPJ) means each of the police services and police forces of the Commonwealth, States and Territories of Australia, which have entered into the Partnership MOU with CrimTrac;

Partnership Memorandum of Understanding (MOU) means the Memorandum of Understanding between The CrimTrac Agency and participating Australian Police Jurisdictions;

Party means a party who has entered into this agreement, and 'parties' will have the corresponding meaning;

Person record means specified information about a person as defined in the Common Information Model;

The CrimTrac Agency (CrimTrac) means the executive agency established under the Public Service Act 1999 (Commonwealth), with responsibilities for the day-to-day management of CrimTrac systems; and

Third party means any organisation or individual outside of CrimTrac or a Participating Australian Police Jurisdiction.

3. Provision and consumption services covered under this agreement

3.1. Provisioning and storage of NPRS data

3.1.1 Acceptable NPRS payload

The full list of acceptable data entities and elements is documented in the most recent Common Information Model. The following broad categories of data describe NPRS persons information, such as:

- a. persons of interest identity information
- b. involvement information
- c. protection orders and
- d. photos.

3.1.2 CrimTrac processes for data provision

CrimTrac will apply data received from PAPJs to the NPRS database, on behalf of all jurisdictions, in accordance with the following processes:

Validate:	CrimTrac receives the extract from the PAPJs systems and checks the message syntax and data content (in accordance with the business rules outlined in the NPRS (MNPP) Interoperability documentation.
Apply:	The valid payload is applied to the NPRS database.
Log:	The transaction is logged.
Report:	The application of data is recorded in the Inventory; CrimTrac will provide monthly inventory reports, quarterly referential integrity reports and any reports on demand.

This process is illustrated in **Figure One**.

3.1.3 Jurisdictional processes for data provision

The PAPJs will provide an initial load of NPRS data and then provide, at a minimum, daily to real-time updates of NPRS data to CrimTrac. These processes include:

Extract:	Jurisdictions extract data from their respective operational systems.
Log:	Extracted records are logged.
Update:	Updates applied to the extraction based on the CrimTrac provision status reports.
Reconciliation:	Request sent to CrimTrac for inventory report.

This process is also illustrated in **Figure One**.

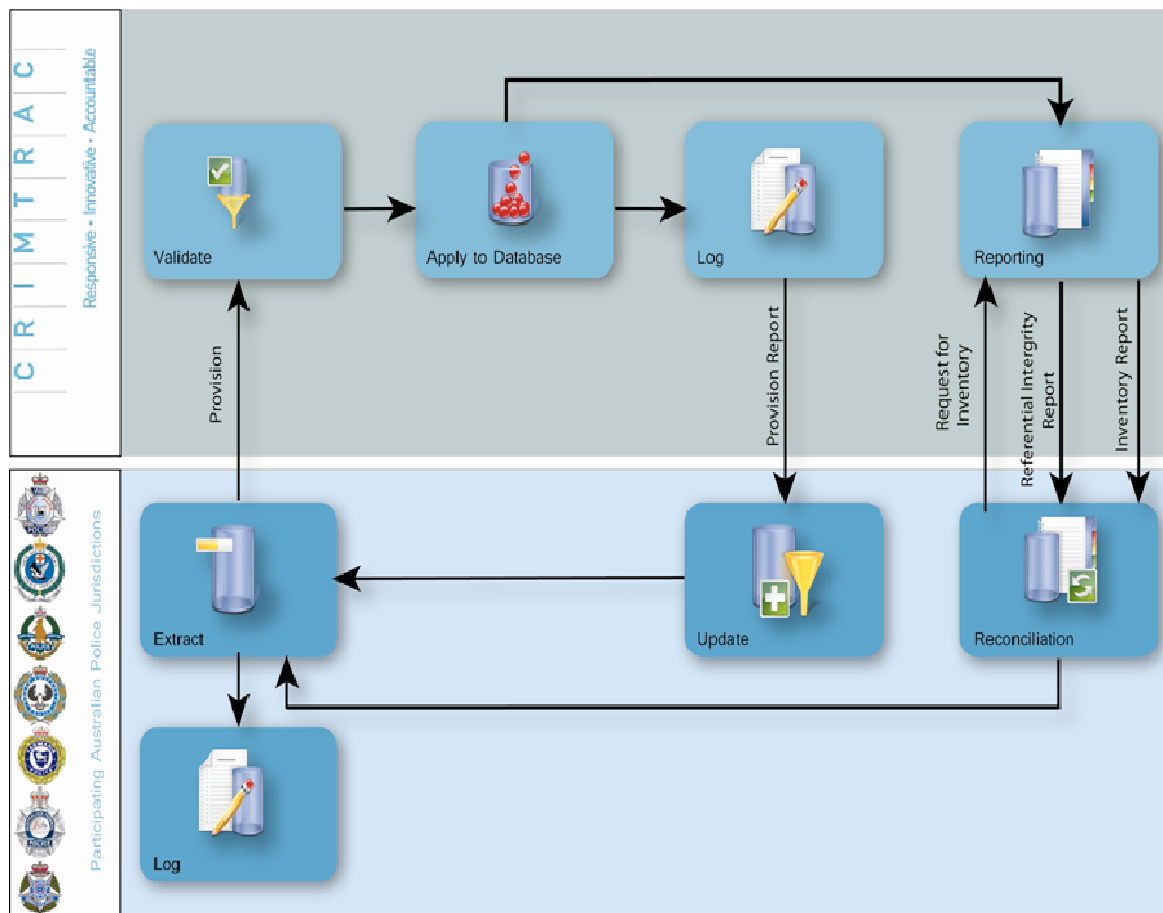


Figure One: Provisioning

3.1.4 CrimTrac provisioning and hosting responsibilities

In order to support the provisioning process in a sustainable manner, CrimTrac will endeavour to meet the following responsibilities:

- Timing and frequency:** CrimTrac will apply jurisdictional data to the NPRS database within 24 hours upon receipt of a provision request. CrimTrac is able to clear 20,000 requests per day per PAPJ. This incorporates a 20% above average surge capacity.
- Notification of delays:** CrimTrac will notify relevant PAPJs, in line with Service Desk procedures, of any delays to the provisioning process.
- Reporting:** CrimTrac will provide PAPJs with monthly NPRS Provision and Reconciliation Reports; and quarterly Referential Integrity Reports, as well as reports on request by PAPJs.

3.1.5 Participating Australian Police Jurisdiction provisioning responsibilities

PAPJs will provide CrimTrac with person information that is in accordance with agreed candidature rules and the Common Information Model. In addition, PAPJs, will aim to:

- Timing and frequency:** ensure supply and upload of batch data will be completed prior to 0300 each day unless otherwise agreed in advance.
- Notification of delays:** notify CrimTrac, in a timely manner, of any delays to the upload process.
- Payload changes:** notify CrimTrac, at least 24 hours in advance, of non-routine changes to volume of uploaded information.
- Reconciliations:** reconcile against their source databases and action any corrections upon receipt of a Reconciliation Report from CrimTrac.
- Holding of logs:** hold logs of details of provision request transactions to allow for resubmission for a period of at least 14 days.

3.1.6 Data ownership and accuracy

All parties to this agreement will, through best efforts, ensure that the quality of data provided to NPRS is of the highest degree possible for users of the system. Accordingly:

- a. the ownership and responsibility for the accuracy, currency and completeness of NPRS data will at all times be vested with the supplying PAPJ;
- b. CrimTrac will not delete, add to, amend or otherwise modify information supplied by PAPJs to the NPRS;
- c. CrimTrac will notify PAPJs if it identifies or is made aware of any errors;
- d. once an error is identified, PAPJs have a collective responsibility to ensure that they notify all other PAPJs and CrimTrac and aim to resolve the issue collectively; and
- e. each PAPJ accepts responsibility for validating the ownership of data that it provides, and ensuring that appropriate authorisation has been received from the originating source to provide the data to CrimTrac for inclusion in the NPRS.

3.2. Consumption of NPRS data

3.2.1 Consumption services provided by CrimTrac

CrimTrac will provide all PAPJs the generic web application or web service(s) for the consumption of NPRS data. Sub-services for consuming NPRS data include:

- a. search;
- b. persons of interest, Orders and Photo retrieval; and
- c. consumption logging.

These services and associated processes are illustrated in **Figure Two** below.

3.2.2 PAPJ consumption considerations

Under this agreement, PAPJs agree to consume NPRS data through web services via their nominated operational systems or through the generic web application provided by CrimTrac.

3.2.3 NPRS consumption dependencies

Retrieval of information from NPRS relies on auxiliary systems, which add value to NPRS but reside within PAPJs (e.g. NSW photo service). These systems are acknowledged because NPRS is directly dependent on their availability or performance.

Under this agreement, PAPJs providing such an auxiliary system agree to notify CrimTrac, in a timely manner, of any changes to the operations of that system, which may affect the performance or quality of service provided by NPRS. Where these changes are known in advance (e.g. usage policy changes, planned outages) the PAPJs agree to notify CrimTrac at least 24 hours in advance.

The NSW Photo History Service is considered to be an auxiliary system for the purposes of this agreement, and is illustrated below in **Figure Two**.

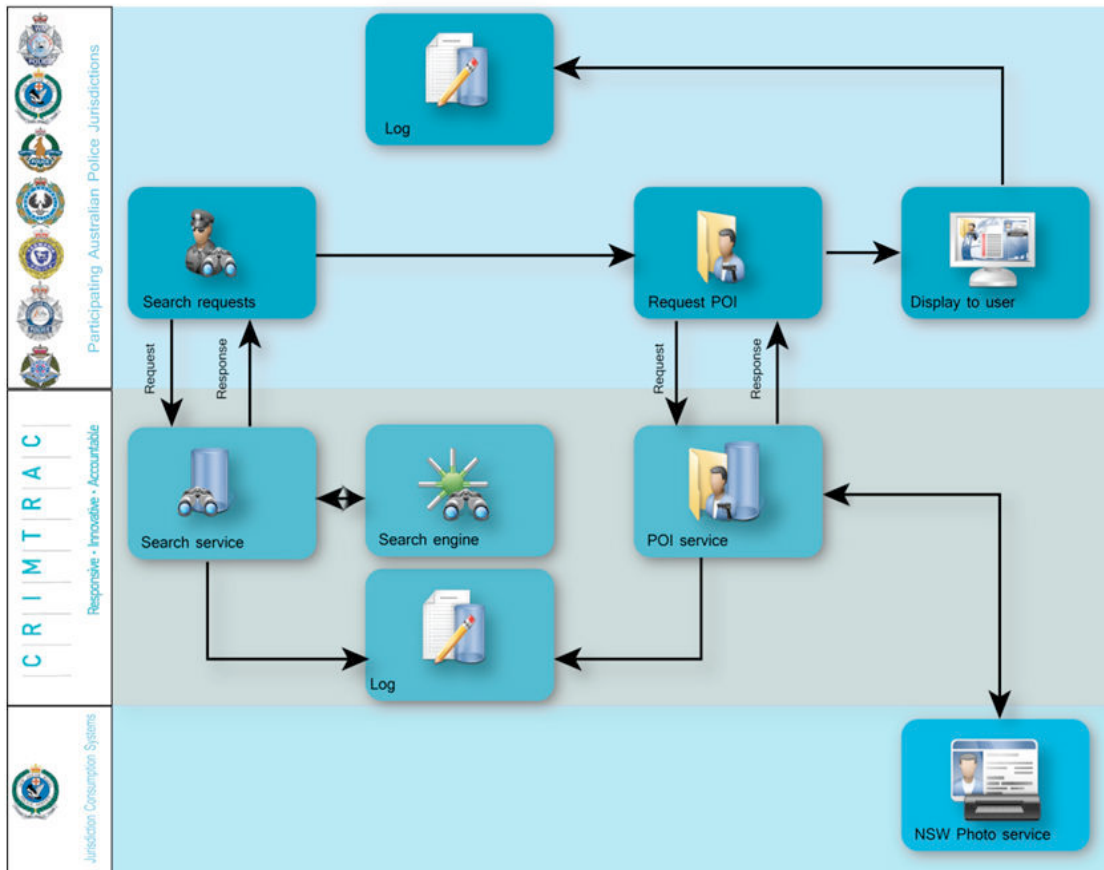


Figure Two: Consumption

3.2.4 Consumption performance

Under a best efforts approach, CrimTrac will aim to ensure that the NPRS will achieve reasonable average response times within a tolerance of 90% of all searches based on **Table One**, below. Under this agreement CrimTrac will have responsibility for performance of the NPRS database and related services and PAPJs will maintain responsibility for performance within their respective jurisdictional network boundaries.

Activity	Average Response
Exact search	5 Secs
Fuzzy search	20 Secs
Keyed lookup	3 Secs

Table One: Search performance

4. Supporting services covered by this agreement

4.1. Auditing

This section covers the audit of access to data contained within NPRS and does not cover unauthorised logon attempts.

4.1.1 CrimTrac responsibilities

CrimTrac is responsible for the audit of the generic web application and NPRS web services called from PAPJ systems. CrimTrac can only audit information requested by and supplied to jurisdictions and not what is displayed to the end user. Accordingly:

- a. CrimTrac will log details of all search requests and responses from all applications and web services that access NPRS data.
- b. CrimTrac will log data that is displayed to the user of the generic web application (i.e. this data may be all or part of the data returned by the NPRS System to the generic web application as part of a user search response).
- c. CrimTrac will log all logon attempts and record each reason for access to the generic web application.
- d. CrimTrac will provide PAPJs with extracts from the NPRS Audit log upon receipt of an authorised request from the PAPJs IT Security section. The request is to be sent to the CrimTrac Service Desk. The audit log extract will be limited to information about:
 - a. search requests and responses pertaining to users belonging to the requesting jurisdiction.
 - b. data accessed by a user from the requesting PAPJ.
 - c. data that is owned by the PAPJ but accessed by a user from any PAPJ.

The extracts of the audit logs will be supplied within 5 working days from receipt of the request.

4.1.2 PAPJ responsibilities

- a. PAPJs will log data that is displayed to the user (this data may be all or part of the data returned by the NPRS System to the jurisdictional system as part of user search response).
- b. PAPJs will make available, on request, an extract from the consumption application audit log, to other PAPJs.
- c. PAPJs consuming data through web services will be responsible for audit of data used by their members through their own systems.
- d. PAPJs are responsible for logging reason for access.
- e. PAPJs should aim to keep audit logs indefinitely.

4.2. Service Desk support

4.2.1 CrimTrac Customer Support Services

The CrimTrac Service Desk will provide a single point of contact for all enquiries related to CrimTrac systems. CrimTrac will also maintain a security infrastructure to allow access only to authorised users.

The CrimTrac Service Desk can be contacted on 02 6268 7750. It is fully resourced between 0800 and 1800 EST (and EDST) each business day. CrimTrac Service Desk staff provide 24x7 on-call support outside business hours for priority one issues. CrimTrac will ensure that trained staff are available 'on-call' 24 hours a day, 7 days a week for first level support. Refer to Table Four for description of priority levels.

For the purposes of this section, a day is a normal working day, which is any day of the week other than a Saturday, Sunday, national or ACT public holiday, or Commonwealth Public Service holiday.

4.2.2 Incident management

Where an incident is reported to the CrimTrac Service Desk, the Service Desk will:

- a. log the incident and provide a workaround where possible;
- b. resolve or escalate the problem to second and third level support as required; and
- c. keep the client informed as to the progress towards resolution of the incident or issue.

4.2.3 Problem resolution

CrimTrac's problem resolution service is to provide for:

- a. problem resolution support;
- b. the formal recording of all problems on receipt;
- c. the categorisation of each problem, including whether the resolution of the problem is the responsibility of CrimTrac or a third party and, for problems outside the responsibility of CrimTrac, referral of the problem to the responsible party;
- d. initial and ongoing reporting to PAPJs on progress toward resolution;
- e. resolution within the specified time for each category of problem as set out in **Table Two**;
- f. escalation of those problems not resolved within the specified time; and
- g. CrimTrac is to record the required problem resolution activities in accordance with **Table Three**.

Time of incident	Priority of problem	Response time
0800 - 1800 Monday - Friday	Problem affecting service	Immediate telephone response
0800 - 1800 Monday - Friday	Problem not directly affecting service	2 hour response
0800 - 1800 Monday - Friday	Enquiry only	8 hour response
Outside business hours	Problem affecting service	1 hour response

Table Two: Response times

Activity	Requirement
Logging	Log each request allowing separate identification.
Categorisation	Categorise responsibility for problem resolution.
Prioritisation	Log the priority accorded to the problem.
Affected area	Log the physical area (i.e. jurisdiction) affected by the problem.
Incident type	Log the nature of the incident in terms of service loss.
Progress reports	Log details of each progress report.
Escalation	Log escalation details.
Resolution	Log resolution details.

Table Three: Recording requirements

4.2.4 Definitions of priority, impact and urgency

CrimTrac's Service Desk categorises incidents on a priority rating system of 1 (most severe) to 4 (single user low impact). These are detailed in **Table Four**.

Priority	Description
Priority 1 Incident	The application/IT Service is not able to run in a production environment. There is no workaround for the problem to allow users to continue processing with minimal or no loss of efficiency or functionality. For example, if an outage with a jurisdiction, either totally; or to one or more systems resulted in the consumption services being unavailable to users.
Priority 2 Incident	The incident restricts the usability of the application/system, but the application/IT Service itself is running. There is no workaround available. For example, the NPRS system is running slow or the provisioning data services are unavailable.
Priority 3 Incident	The application/IT Service is up and running, but there is a moderate impact on the usability of the application. There is a workaround available. For example, if the links from one person record to another fails via the "orders" links, the user could still access the information by performing another person search.
Priority 4 Incident	The application/IT Service is running with a minor flaw. There is a workaround for the issue and the usability of the application is not affected. For example, a system tester raises an incident for a heading description on the Generic Application that is not displayed as specified in the original specification.

Table Four: Priority levels

4.2.5 Prioritisation of incidents

Incidents are prioritised by the CrimTrac Service Desk in accordance to the priority and impact of the incident. In the event of two equally serious issues, prioritisation of the incidents would be sought from the CrimTrac Business Manager.

4.2.6 Escalation of incidents

The CrimTrac Service Desk and the NPRS Business Team have an agreed internal escalation plan for the escalation of incidents. This plan includes contact names and telephone numbers for 24 x 7 contacts.

4.2.7 PAPJs Service Desk responsibilities

Under this agreement PAPJs will:

- a. maintain nominated hierarchical points of contact for CrimTrac support staff, for all enquiries related to NPRS and related systems;
- b. create and maintain administrative arrangements for the appropriate authorisation and access for all authorised personal, defined in Clause 1.1.3, to CrimTrac systems; and
- c. provide equivalent second and third level support.

4.3. System availability

4.3.1 Target availability

CrimTrac, under best efforts, aims to deliver maximum availability however there is a 96% per day target based on CrimTrac's provider availability. This excludes maintenance windows and agreed outages; and is dependent on jurisdictional availability. Target availability will be measured by:

- a. server availability as measured by service provider; and
- b. network availability to the user's end of the CrimTrac communication link where CrimTrac is responsible for the communications link. This is depicted in **Figure Three**.

Note: CrimTrac is only responsible for service availability to its external firewall connection.

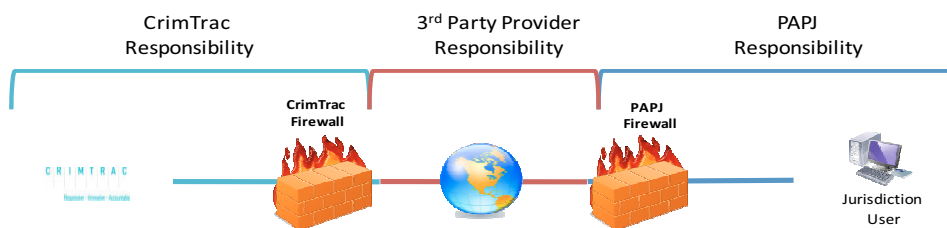


Figure Three: Network boundaries

4.3.2 Calculation of service availability

System availability is to be calculated by using the following formula:

$$\frac{\text{Required Service Hours minus Total Non - Allowable Downtime}}{\text{Required Service Hours}} \times 100$$

Required Service Hours = Service hours during a calendar month - actual hours in a month less downtime

Total non-allowable downtime = Sum of total non allowable downtime for the NPRS host system for the month

Allowable downtime is defined as the total number of hours for planned outages and maintenance windows.

4.3.3 Notification of planned outages

Where there is a scheduled system outage of more than 4 hours that is not able to be taken during the maintenance window, CrimTrac will provide at least 7 days notice of the outage.

4.3.4 Maintenance windows

Windows for system maintenance will occur one evening a week for a three hour interval. The current nominated day and time is available in the CrimTrac Change Management Strategy. If a window is to be utilised CrimTrac will provide:

- a. at least three working days notice of the outage;
- b. reasonable notification to PAPJs if the window should change; and
- c. external (3rd party) service provider outage notification.

External (3rd party) service providers will not provide continuous support. This means CrimTrac is not able to guarantee problem resolution before the next business day.

4.4. Backup and Restoration

4.4.1 CrimTrac responsibilities

CrimTrac will ensure that regular backups occur in line with its internal practices and will ensure that a process to check recoverability of backups is in place.

File recovery for operating system and database files must be available as needed 24 hours per day 7 days per week - these will support any disaster recovery or business continuity plans.

4.4.2 PAPJ responsibilities

Each agency will align its backup and restoration procedures as well as any disaster recovery and business continuity plans.

4.4.3 Shared backup and restoration procedures

All parties will ensure that their backup facilities and services are adequate including ensuring that backup copies of files are stored in a secure environment.

All parties will check the recoverability of backups on a regular basis.

All parties will ensure that adequate system restoration measures are in place with network providers to minimise any disruptions to services provided under this agreement.

5. Supporting standards used by this agreement

5.1. Security

5.1.1 System Security

While NPRS data is held, or processed by CrimTrac, and while it is being transmitted on the Australian Federal Police's encrypted network, CrimTrac will store, process and transmit NPRS data applying the protections and security mechanisms specified by the Commonwealth Protective Security Manual (PSM) for PROTECTED information. In addition:

Generic Web Application Security: CrimTrac will encrypt the data provided via the Generic Web application from end-to-end (i.e. from CrimTrac through to the actual user) by using Secure Sockets Layer (SSL). All police users accessing the Generic Application are known and registered in the CrimTrac security system.

Web Services Security: CrimTrac will secure the data and systems up to the CrimTrac / PAPJ data communications boundary only (i.e. the PAPJs firewall). CrimTrac will authenticate the calling web service program. CrimTrac does no authentication or authorisation checking of the user IDs - it will trust that the PAPJ's application has authenticated the end user and validated the authorisation of the end user to view the requested data.

PAPJs will secure the data and systems beyond the CrimTrac/PAPJ data communications boundary (i.e. the PAPJ firewall). All NPRS Web Service transactions will be encrypted using CrimTrac provided SSL certificates. This will ensure that NPRS data returned from queries remains at PROTECTED. However the consumption and storage of that data within the PAPJ will be managed at the Law Enforcement - In Confidence level on non-Commonwealth systems.

The existing Partnership MOU covers the requirements pertaining to consumption, non-disclosure and protection of data. The level of protection, based on the requirements as defined in the Partnership MOU, remains the responsibility of the PAPJ consuming and storing the data.

5.1.2 User security

Access to physical communications facilities is restricted to authorised staff, in accordance with specific system security plans. Accordingly:

- a. PAPJs will ensure that only appropriately trained and approved personnel are granted access to CrimTrac systems;
- b. PAPJs are responsible for ensuring that adequate facilities and computer infrastructure exists (distinct from CrimTrac network responsibilities) in order to access CrimTrac systems; and
- c. user security used in production environments should be applied to pre-production environments.

5.1.3 Commonwealth security obligations

Australian Government Information Technology Security Manual ACSI - 33

In planning and implementing security aspects for its communication facilities, CrimTrac bases its guidelines and standards on those promulgated by the Defence Signals Directorate in ACSI 33 - Security in Electronic Information Processing Systems.

The selection by PAPJs of communications devices and services must take into account requirements to minimise the risk of tapping, bugging or interference to both voice and data communications.

Australian Government Protective Security Manual (PSM)

CrimTrac will operate within the parameters of the CrimTrac Security Policy and, more broadly, in keeping with the requirements of the PSM.

5.1.4 Access authorisation

The PAPJs authorise the CrimTrac Service Desk to access their data in order to assist with the identification and resolution of reported defects, providing that:

- a. those Service Desk and support staff gain access using individual, unique identifiers;
- b. all actions undertaken by them are logged by CrimTrac; and
- c. PAPJs have access to those audit log records upon request.

5.2. Legislative constraints

5.2.1 Supply of information to CrimTrac

Information collected and supplied to CrimTrac is in accordance with relevant legislation within each PAPJ.

5.2.2 Use of NPRS information within PAPJs

Information obtained from the NPRS is used in accordance with relevant legislation and policies within each PAPJ.

5.2.3 Privacy Principles

Parties to this agreement understand they are required to act in accordance with their respective privacy legislation and source data privacy legislation. CrimTrac is bound by the Information Privacy Principles as set out in the Privacy Act 1988 (Cwth).

5.2.4 Freedom of Information

The parties agree to consult fully in relation to any freedom of information requests relating to the NPRS system and act in accordance with relevant legislation and protocols. This aligns with Clause 13 of the Partnership MOU and Clause 9 of the Inter-Governmental Agreement.

5.2.5 Records Management

PAPJs which receive data from NPRS must also comply with the relevant Commonwealth, State and Territory legislative requirements that apply within their jurisdictions to records management, which includes creation, storage, retention and disposal of records.

5.3. NPRS as a non-authoritative source

Under this agreement it is acknowledged by all parties that information contained in the NPRS system cannot be considered to be definitive in nature. That is, data contained in PAPJ operational systems is accepted as the authoritative source pertaining to any person of interest and supersedes any data contained in NPRS. NPRS remains a reference tool whose data is sourced from PAPJ systems but is not linked in a manner to reflect exactly PAPJ operational systems.

6. Management processes

6.1. Change management

6.1.1 Procedures

The first point of contact for change requests will be the CrimTrac Service Desk. CrimTrac will use the change management procedures contained in its internal document entitled Change Management Strategy Version 2. This document has been reviewed and agreed to by the CrimTrac NPRS Team and CrimTrac NPRS Business Manager.

6.1.2 Notifications

PAPJs will also be responsible for formally advising CrimTrac of any which govern the exchange of information via the NPRS. All changes are to be made in accordance with change management protocols and configuration management procedures agreed by all parties.

6.2. Consultation

CrimTrac will consult with PAPJs in making decisions that affect the operation of the NPRS. The parties agree to consult with each other in relation to any significant public statements concerning the operation of the NPRS and funding arrangements.

All parties agree to nominate:

- a. a liaison officer to be the first point of contact for any consultation; and
- b. an expert user group representative to provide expertise and assistance.

Liaison officers will ensure correct escalation protocols and authorisations are adhered to in making decisions regarding public statements. All notices under this agreement are to be provided to the nominated liaison officer.

6.3. Dispute resolution

The parties agree to make every effort to resolve disputes as they arise.

Any party may give notice to the other calling for mediation of the dispute. The parties will elect a mediator within seven days of this notice.

Disputes that cannot be resolved, with and through a mediator (at the officer level) are to be referred to the CrimTrac Chief Executive Officer and the relevant Commissioner or equivalent.

6.4. Reviews and Improvement

Whilst this document aims to encourage a 'best efforts' approach among agencies, a culture of continuous improvement will be adopted. Regular reviews will allow this document's content to remain relevant and current as the police operational environment changes.

As a minimum it is agreed that a review should be undertaken annually. The primary forum for reviews is the NPRS sponsoring group. There are also a number of triggers which will require this document to be revisited as a matter of course. These include:

- a. The introduction of a Service Level Agreement
- b. New business services
- c. Changes to the NPRS payload
- d. Changes to support arrangements
- e. Hardware and software technical changes
- f. In addition, participating agencies should aim to undertake quarterly Service Desk performance teleconferences.

This Agreement may be varied by the written agreement of all Parties.

6.5. Termination of Agreement

Any party may withdraw from this agreement upon giving three months notice in writing to the other parties and to the Board of Management. The notice of termination must include reason(s) for the termination. An impact assessment should be undertaken and, at a minimum, this assessment should take into consideration (but not be limited to) impact on:

- a. the objectives of the IGA and other cross-agency agreements;
- b. the ability to achieve Australian or State Government policy objectives;
- c. public confidence and perceptions;
- d. current and planned policing operations;
- e. members of Police Services and partner agencies; and
- f. cost and efficiency of operations.

7. Signatories

The Commissioner of New South Wales
Police Force

Date ____ / ____ / ____

The Commissioner of Tasmania Police
Service

Date ____ / ____ / ____

The Chief Commissioner of Victoria Police

Date ____ / ____ / ____

The Commissioner of Northern Territory
Police

Date ____ / ____ / ____

The Commissioner of Queensland Police
Service

Date ____ / ____ / ____

The Commissioner of the Australian
Federal Police

Date ____ / ____ / ____

The Commissioner of Western Australia
Police

Date ____ / ____ / ____

The Chief Police Officer of Australian
Capital Territory Policing

Date ____ / ____ / ____

The Commissioner of South Australia
Police

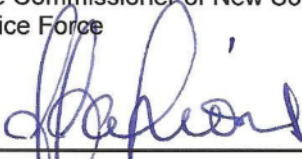
Date ____ / ____ / ____

The Chief Executive Officer of the
CrimTrac Agency

Date ____ / ____ / ____

7. Signatories

The Commissioner of New South Wales
Police Force



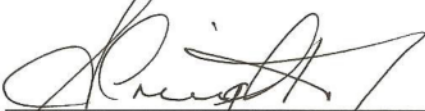
Date 19 / 03 / 09

^{for} The Commissioner of Tasmania Police
Service



Date 19 / 03 / 09

^{for} The Chief Commissioner of Victoria Police



Date 19 / 03 / 2009

The Commissioner of Northern Territory
Police



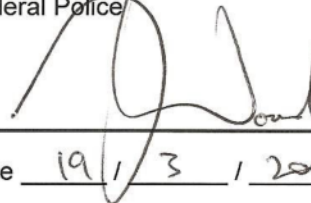
Date 19 / 03 / 2009

^{for} The Commissioner of Queensland Police
Service



Date 19 / 03 / 09

^{for} The Commissioner of the Australian
Federal Police



Date 19 / 3 / 2009

The Commissioner of Western Australia
Police



Date 19 / 03 / 09

The Chief Police Officer of Australian
Capital Territory Policing



Date 19 / 3 / 09

^{for} The Commissioner of South Australia
Police



Date 19 / 03 / 09

The Chief Executive Officer of the
CrimTrac Agency



Date 19 / 3 / 09