AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION

Agreement for controlled access by duly Accredited Bodies to Nationally Coordinated Criminal History Checks

Extract of Annexure B

COMMONWEALTH OF AUSTRALIA
REPRESENTED BY THE AUSTRALIAN CRIMINAL
INTELLIGENCE COMMISSION

Annexure B – Protection of Personal Information and Police Information Safeguards

1. Introduction

(a) In accessing the Service, Accredited Bodies must implement the security management measures set out in this **Annexure B** to ensure against:

(i) misuse, interference, loss, unauthorised access, modification or disclosure of Applicant's Personal Information;

(ii) unauthorised access to and use of the Service;

(iii) unauthorised access to Police Information in the National Police Checking Service Support System (**NSS**); and

(iv) loss and unauthorised access, use, modification or disclosure of Police Information stored outside of NSS.

(b) This information is provided to assist Accredited Bodies understand their obligations and comply with the ACIC's security management standards.

2. Information Security Policy

(a) The Accredited Body must develop, document and maintain an Information Security Policy (**Policy**) that clearly describes how it protects information.

(b) The Policy should be supported by the Accredited Body's senior management and be structured to include any legal framework relevant to the Policy, such as the *Australian Crime Commission Act 2002* (Cth) and this Agreement.

(c) The Policy must include adequate details on how it is enforced through physical, technical and administrative controls, including details on:

(i) the type or class of information that the Policy applies;

(ii) information security roles and responsibilities relating to the Service;

(iii) security clearance requirements and its Personnel's responsibilities;

(iv) configuration and change control;

(v) technical access controls;

(vi) staff training;

(vii) networking and connections to other systems;

(viii) physical security (including media security); and

(ix) incident management.

(d) The Accredited Body's privacy policy must reference the Policy, in terms of how the Applicant's Personal Information is held (as per APP 1.4(b)).

3. Technical Access

The Accredited Body's ICT environment must be secured in accordance with the Policy and should:

(a) be protected by appropriately configured gateway environment (including firewalls);

(b) include technical access controls protecting any Police Information stored electronically outside of NSS, for example, restricted file system permissions; and

(c) maintain a static IP address to avail web services (if applicable).

4. Technical Infrastructure

(a) Workstations and server infrastructure involved in the storage or processing of Police Information and Personal Information should be secured in accordance with the Policy and should:

(i) run current and patched operating systems;

(ii) run current and patched software, including browsers (N-1 on browsers is acceptable providing patching is maintained);

(iii) have anti-virus software application installed up-to-date virus definition files; and

(iv) run application whitelisting software (desirable).

(b) Administrative or privileged access to infrastructure is to be minimised and only used when an administrative function is required.

5. Digital Certificates

Digital certificates used in the connection to the Service must be managed securely and ensure:

(a) certificates are not distributed beyond that required for connection;

(b) certificates are only installed on the Accredited Body's corporate infrastructure (certificates must not be installed on home or personal computers); and

(c) passwords relating to certificates are securely stored.

6. Password policy

System accounts that are involved in the storage or processing of Police Information and/or Personal Information should be subject to a password policy that sets out:

(a) no less than 10 character passwords including a minimum of one numerical and one upper case character;

(b) password reset cycle no longer than 90 days;

(c) users to select strong passwords (avoid dictionary words);

(d) ensure unused accounts are disabled and removed; and

(e) computers lock after 15 minutes of inactivity.

7. Training

All Accredited Body's Personnel involved in storage or processing of Police Information and Personal Information must be provided with the information security awareness training related to:

(a) their responsibilities as defined in the Policy;

(b) what constitutes authorised access to information; and

(c) their obligations with regard to reporting of information security issues or incidents.

8. Incident Management

Any information security issues or incidents must be reported immediately to the ACIC where the consequence may impact or has impacted on the ACIC systems or information. This includes, but is not limited to, loss or compromise of digital certificates or associated passwords.