Department of Education
GOVERNMENT OF WESTERN AUSTRALIA

# Information security statement
## Protecting your information

### Personnel Screening Unit

The Department of Education takes the privacy and personal information of applicants consenting to a Nationally Coordinated Criminal History Check (screening) seriously, and will only collect, hold, use and disclose personal information in accordance with the *Privacy Act 1988* and manage this information in accordance with the Department's Records Management policy and procedures.

### Protecting privacy

The Screening Unit is further bound by strict requirements regarding the use and storage of personal information, including copies of identification used to verify applicants' identity, as part of a formal Agreement with the Australian Criminal Intelligence Commission which are consistent with the Privacy Act 1988 and the Australian Privacy Principles.

Our employees are trained in the importance of confidentiality and maintaining the privacy and security of personal information. Access to personal information, as part of the screening process, is restricted to authorised persons who are employees who require it to undertake mandatory services as part of the Department's probity check processes, as outlined in the Department's Criminal History Screening for Department of Education Sites policy and procedures.

This Information security statement applies to personal information pertaining to screening applicants (for example, name, address, contact details, identification documents), and any identified criminal history information pertaining to applicants. The personal details of screening applicants are entered into the Department's online Criminal Record Information System (CRIS) system by the applicant direct. The CRIS has undergone stringent penetration testing and is safe and secure from external ICT threats.

The Department is provided criminal history information via a secure web service with the Australian Criminal Intelligence Commission. The connection is via a static IP Address and directly connects the ACIC system with the Department's Criminal Record Information System. The CRIS system is only accessible to the 4 employees in the Screening Unit and the Manager, Screening. Each of these 5 employees is trained in the use, security and importance of maintaining confidentiality in relation to personal information and any identified criminal history information.

The Screening Unit staff and manager, Screening are required to undergo an annual Nationally Coordinated Criminal History Check. In line with the Department's Criminal History Screening for Department of Education Sites policy and procedures, any change in circumstances must be reported to their line manager. Screening Unit staff are also required to sign a Deed of Confidentiality regarding the use and disclosure of criminal history information (refer to the Privacy Management Plan of the Screening Unit).

Members of the Department's Screening Committee, who are responsible for making decisions on behalf of the Director General, and make recommendations concerning employees/applicants

for a Nationally Coordinated Criminal History Check with identified criminal history, are required to consent to an annual NCCHC and also sign a Deed of Confidentiality regarding the use and disclosure of criminal history information.

The Criminal Record Information System has also undergone stringent penetration testing and is safe and secure.

The access to the Criminal Record Information System (CRIS) is restricted to the 5 Screening staff (Manager, Screening; Senior Screening Officer; 2 x Screening Case Management Officers; Assistant Screening Officer). Roles in CRIS are assigned by the Manager and/or Senior Screening Officer, and are either an 'Administrator' or a 'User' role.

CRIS was implemented on 1 July 2018, at which time all 5 Screening staff received training on the use of the system, where the importance of managing personal and criminal history information was reinforced.

ACIC requirements in relation to the storage of applicants' identification documents and criminal history information have been automated in CRIS. In line with the ACIC Agreement, criminal history information is automatically redacted in three (3) months from date of receipt, and Identification documents are redacted at two (2) years from date of uploading into CRIS.

The Screening Unit office within the Department of Education building is a secure and restricted area, with access controlled by electronic proximity readers. Only the 5 Screening staff have access to the Screening Unit, with a record kept of all access to this secured area. Additional security measures are that the Screening Unit office has a stand-alone, monitored alarm, with individual alarm codes to enter the Screening Unit assigned to each staff member. All arming and dis-arming of the Screening Unit alarm is recorded and auditable. The Screening Unit also contains locked cabinets where printed information is stored. Any hard copy files created for assessment purposes are destroyed within 3 months of the decision to clear or refuse clearance is made.

In the event of any unauthorised access to the Screening Unit outside of normal business hours, this is reported to the Senior Screening Officer and Manager, Screening. Any such breaches of security are reported to the Australian Criminal Intelligence Commission.

Storage of personal information (and the disposal of information when no longer required) is managed in accordance with the Australian Government records management regime, including the *Archives Act 1983*, Records Authorities and General Disposal Authorities. The Screening Unit maintains a publicly available Privacy Statement.

## Specific ICT safeguards within the Department of Education, Western Australia

The below information pertains to Annexure B of the ACIC Agreement.

### 3. Technical Access

a) The Remote Desktop Service is provided by a server farm behind a virtual IP address. All external traffic has to pass through a firewall that limits access to port 443. All traffic is inspected by an IPS which is used to geoblock any connections external to Australia. The servers are patched to the latest available patch level and are included in the regular monthly patch cycle which includes provision for out-of-band patching. The servers are

configured to Microsoft best practices for securing IIS servers. The encrypted connection terminates on the servers themselves and an encrypted connection is made from the server to the workstation within the Departments network. The servers are protected by the regular Endpoint Protection service with daily signature updates. A vulnerability scan is run just before business commences each morning to detect any new vulnerabilities that may have been exposed overnight. The Vulnerability engine is a cloud service which is updated for new and emerging vulnerabilities as they become known.

b) After successful authentication, users are directed to a Remote Desktop session on their regular workstation which they would access when physically in the facility. All access and permissions on the workstation remain the same as when an authenticated user has physical access. Users are prevented from sending files, in either direction, between their work and home workstations. Users are only permitted an interactive session with their workstation.

c) The external web service is presented on a static IP address using a network Load Balancing Router (LBR). This address is resolved externally using DNS that is managed by the Department on Department servers. The servers behind the LBR also have static IP addresses, but servers may be added or removed from the server pool as the service scales. Adding or removing servers is a manual process.

## 4. Technical Infrastructure

(a) Workstation and server infrastructure:

(i) Yes, the agency uses current and patched operating systems
(ii) Yes, the agency uses current and patched software including browsers
(iii) Yes, the agency currently using McAfee AV software with updated virus definition files
(iv) No, the agency does not use application whitelisting software.

## 5. Digital Certificates

(a) Certificates are not distributed beyond that required for connections
(b) Certificates are only installed on the Department of Education's infrastructure (not personal computers)
(c) Passwords relating to certificates are securely installed.

## 6. Password policy

Each individual staff member is provisioned with their own personal User ID and Password for logging into the Department of Education's network. The Department's network password system requires:

(a) Minimum of eight (8) characters, including at least three (3) of the following character types:
- One digit
- One upper case character
- One lower case character
- At least one special character
- No dictionary words

(b) Password changes forced every 60 days
(c) Passwords cannot be repeated within 10 changes:

- New passwords cannot be changed for 24 hours, except where the password has been reset or by a privileged user or Administrator
- Users logging on in the last six days before password expiry are warned that their password will expire soon
- Users are permitted five unsuccessful attempts at logon with the incorrect password within a 30 minute period before their account is locked (if locked, users must request there account be unlocked by a privileged user or Administrator)

(d) Unused accounts are disabled and deleted
(e) Computers lock after 10 minutes of inactivity

## 7. Training

Screening Unit staff are trained in their responsibilities with respect to storing and processing of criminal history information, and managing personal information of applicants. This induction training specifies what is considered authorised and unauthorised access of criminal history information, and their obligations to report any alleged misuse of such information or security issues or incidents where a possible breach has occurred. All staff of the Department who are required to access criminal history information must sign a Deed of Confidentiality in relation to the use and disclosure of criminal history and personal information, as outlined in the Screening Unit's Privacy Management Plan.

## 8. Incident management

In the event of a potential breach of security in relation to the accessing of criminal history information, personal details, or unauthorised access to the Screening Unit, or the compromising of passwords or digital certificates, line management will report this to the Australian Criminal Intelligence Commission.

| Contact | |
|---|---|
| **Telephone** | (08) 9264 4477 |
| **Email** | screening@education.wa.edu.au |
| **Internet** | www.education.wa.edu.au/screening |