Security Administrator Duties

When completed return to DRIVES Help Desk
Email: **driveshelpdesk@transport.nsw.gov.au** or Fax number: (02) 4924 0482

Line Manager

The Line Manager must complete sections 4 and 5 to approve the appointment of the nominated Security Administrator. Your organisation's Security Administrator will have responsibility for managing your organisation's access.
This includes implementation of procedures that will:

- prevent any activity which may compromise the security of information on or obtained from DRIVES.
- monitor compliance with the DRIVES Terms of Access Agreement.

Security Administrator

The nominated Security Administrator must complete sections 1, 2 and 3. The Security Administrator must ensure:

- all authorised users are given a copy of the organisation's "User Guidelines" for the protection of DRIVES and/or DRIVES Information, and
- monitor compliance with the DRIVES Terms of Access Agreement.

1. Organisation's Security Administrator details

Surname *(please print)*

Given names *(please print)*

Organisation name

Position

Contact phone number

Facsimile number

e-mail address

2. Attached documentation

Date of birth

day / month / year

NSW driver licence number/customer number

Existing user ☐

User ID

Add Security Administrator ☐

Delete Security Administrator ☐

3. Security Administrator's declaration

I confirm that the information in this application about me is accurate and complete, that I have read the Personal Information Collection Notice and that I understand my obligations under the Drives Terms of Access Agreement and under this application.

Signature

Date

day / month / year

4. Line Manager details

Surname *(please print)*

Given names *(please print)*

Contact phone number

Facsimile number

e-mail address

5. Line Manager's declaration

I confirm that the person described at item 1 on this form is named as the Organisations Security Administrator.

I confirm that the information in this application about me is accurate and complete, that I have read the Personal Information Collection Notice and that I understand my obligations under the Drives Terms of Access Agreement and under this application.

Signature

Date

day / month / year

Personal Information Collection Notice
Transport for NSW is collecting your personal information is being collected in connection with ensuring an appropriate level of security for our DRIVES database. The provision of the information is voluntary however, failure to provide the information, or any part of it, may mean the proposed Security Administrator will not be permitted to access our DRIVES database. Your personal information will be held by Transport for NSW and you may contact us to access and correct your information. We may also use and disclose your personal information in order to verify and validate the contents of this application and any supporting documentation and in connection with the proposed Security Administrator's (or your organisations') access to DRIVES.

Office use only

Security Administrator setup ☐

Security Administrator deleted ☐

Name of application

Reg ID

B Reg ID

Activity log number

Staff number

Signature

Date

day / month / year

UNCLASSIFIED
SENSITIVE: PERSONAL

Guidelines for external user access to DRIVES

User Responsibilities and Obligations

- Information accessed on DRIVES is confidential and may constitute “Personal Information” within the terms of the NSW *Privacy and Personal Information Protection Act*.
- You are accountable for every access recorded against your password and identification number.
- You may be liable for penalties under the *Privacy & Personal Information Protection Act 1998* should you access or disclose personal information from DRIVES if you are not authorised to do so.

Security Requirements

- You have been issued with an individual User ID and password as a security measure for the prevention of unauthorised access to DRIVES.
- Your user ID/Password combination is your “Electronic” signature and it must not be disclosed.
- You must not share this information with anyone.

Passwords

- As a security measure, the protection of your password is critical.
- Your initial password will be given to you and you will be forced to reset it by the system to a password of your choice.
- Memorise your password, do not write it down; if someone learns your password change it immediately.
- A user will be locked out of the system if they have made five (5) attempts to log in with an incorrect password.
- The DRIVES account is set to expire 6 months from the time of extension/creation. Any account that is unused for 30 days is automatically expired by the system. If the account is extended the user must log in on that same day otherwise it will be deemed to be expired. New accounts have 30 days for the user to access before it expires.
- Any user can change their current DRIVES password at any time by pressing the up or down arrow key whilst at the login (User ID/Password) screen.
- Passwords must consist of six to eight characters.
- Include at least one numeral and have a combination of alphabetic/numeric characters.
- Be substantially different from the previous password and not be cyclic (eg pword1, pword2, pword3).

Other important information

- If as a user you find that your access to the system is denied, contact the Drives Help Desk.
- Your Security Administrator must ensure that your DRIVES user account is cancelled if your position no longer requires DRIVES access.