Australian Government
Department of Employment
and Workplace Relations

# Government Access Request form:

## Electronic Commonwealth Assistance Form (eCAF) API System

Please email completed form to:

| | |
|---|---|
| VET Student Loan providers | VETStudentLoans@dewr.gov.au |
| Higher Education providers | HEenquiries@education.gov.au |
| Dual providers | VETStudentLoans@dewr.gov.au and HEenquiries@education.gov.au |

Given name: ____________________ Surname: ____________________

Phone no: ____________________ ***Generic*** Email address: ____________________

Role/Position ____________________

HITS Provider Code (e.g. 7123): ____________________ Legal Entity Provider Namer: ____________________

*Please ensure all fields above are completed, access will not be granted if any information is missing.*

## Roles and description

### Production

**eCAF Application Group**

☐ eCAF Provider API access – Access to the eCAF Provider Application Programming Interface (API). This is a provider service account only role and **one** account will be created per organisation. The API account is to enable provider's Student Management Systems to interface with the eCAF system.

### Training

**eCAF Application Group**

☐ eCAF Provider API access – Access to the eCAF Provider Application Programming Interface (API). This is a provider service account only role and **one** account will be created per organisation. The API account is to enable provider's Student Management Systems to interface with the eCAF Training system.

### Applicant Declaration

I certify that:

☐ I must comply with the Australian Privacy Principles in the *Privacy Act 1988* and ensure suitable security arrangements exist for all records containing personal information.

☐ I must comply with the requirements in HESA and the VSL Acts in respect to the management of personal information.

☐ I am responsible for ensuring access is terminated within 24 hours when work commitments no longer require this access.

☐ *(VSL only)* I am listed as a contact in the HITS Contact List **OR**

☐ If 3rd party SMS provider, I have provided written approval from the relevant approved Provider.

*Please attach written approval with this signed request form*

Applicant's signature:

x ____________________

Date: ____________________

### Manager/Supervisor Authorisation (all fields required)

Manager/Supervisor name:

____________________

Phone no:

____________________

Manager/Supervisor's signature:

x ____________________

Date: ____________________

Australian Government

Department of Employment
and Workplace Relations

## Terms and Conditions for access to department systems

### Privacy Obligations

The Department is collecting this information for the purpose of verifying your identity to determine whether access is provided to the Department's ICT systems.

The Department may use this information for the purpose of managing and administering ICT systems, protecting against unauthorised access, verifying security problems and ensuring compliance with policy.

The Department will not disclose this information unless it is required or authorised by or under law. Alternatively, the Department may seek your consent to disclose this information.

### Usage Obligations

The *Higher Education Support Act 2003* (HESA) provides penalties for officers who use information obtained or created for the purposes of Chapter 2, 3 or 4 or Schedule 1A of HESA outside the course of their official employment. The maximum penalty for contravening this requirement is two years imprisonment.

Similar penalties apply under the *VET Student Loans Act 2016* (VSL Act) if an officer uses or discloses personal information in their employment and the use or disclosure is not authorised or required by law, or if it is not for a permitted purpose, or if the officer causes any unauthorised access to or modification to the personal information.

Personal information must be properly handled in accordance with relevant privacy requirements under HESA and the *Privacy Act 1988* (Privacy Act).

Individual credentials are issued to enable access to department system environments as specified on this form. To maintain the integrity of access to this system, users are required to ensure the safekeeping and confidentiality of their passwords and not share their user account, nor use another person's user account.

Each officer is accountable for all actions undertaken using their logon IDs / passwords.

If the user, or any third-party for which the user is responsible, breaches any part of the terms for the issuing of production credentials, then the department may, at its sole discretion, withdraw or restrict system access, immediately and without notice. The Department reserves the right to deny future requests for access to the Department's ICT systems.

Users will identify and avoid conflicts of interest. Where there is a perceived or actual conflict of interest, users will notify their supervisor or manager and follow appropriate advice before accessing Department ICT systems.

Users must report all suspected breaches of the Department's ICT Systems as soon as they become aware of the breach.