Australian Government
Clean Energy Regulator

Public Disclosure Statement

Trovio access to the Unit and Certificate Registry and conflict of interest management

Overview

The Clean Energy Regulator (CER) has partnered with Trovio Operating Pty Ltd to deliver and operate the Unit and Certificate Registry through the CorTenX platform. To ensure transparency and public trust in the operation of the registry, this statement outlines the extent of Trovio's system access and the conflict of interest safeguards that are contractually and operationally in place.

Shared commitment to fair access and public confidence

The CER and Trovio are jointly committed to ensuring:

- no third-party receives preferential treatment or access to the registry data or features
- interoperability with external systems will be offered transparently and equitably
- public interest, trust, and market integrity are paramount in all operational decisions.

Access to registry data by Trovio personnel

The majority of Trovio personnel have no access to the registry or any associated production systems or data.

Access to production data is strictly limited to 2 internal teams within Trovio:

1. Operations team – responsible for day-to-day back-end system management and infrastructure operations.
2. Support team – senior engineering and quality assurance personnel who will provide the CER with second level support and advanced troubleshooting when necessary.

Trovio's personnel operate within a secure, Australian-based Amazon Web Services (AWS) cloud environment. Access to production systems and data is governed by:

- role-based access control and attribute-based access control
- identity and resource-based AWS Identity and Access Management policies
- strict enforcement of the 'principle of least privilege' – access is only granted when essential to specific roles.

C E R CLEAN ENERGY REGULATOR

Trovio and its personnel must also comply with the Protective Security Policy Framework and the Australian Government Information Security Manual and are subject to obligations to protect information under Part 5.6 of the Schedule to the *Criminal Code Act 1995* (Cth).

Access roles

Access roles are divided into:

1. Business as usual (BAU) roles.

   The Trovio Operations Team and the Support Team have read-only access to:

   - system and application logs
   - system and application configuration parameters (excluding application secrets)
   - system infrastructure performance metrics.

   The Operations Team also has limited read-write access for scaling infrastructure and deploying software and infrastructure updates from pre-defined release repositories.

   Neither Trovio team has direct access to customer data from any of the BAU roles. Application logs contain transaction IDs, block numbers, the internal account IDs of the originator of the request and the originating IP address of the request, but no details of the transaction itself.

2. Emergency ('break glass') roles.

   If the CER requests Trovio to investigate specific transaction-related issues, a 'break glass' role with read-only access to customer data can be temporarily provisioned to the Trovio Operations Team and Support Team to facilitate investigations.

   If there are critical system issues or disaster recovery is invoked, a break glass role with read-write access to customer data can be temporarily provisioned to the Operations Team to assist with system recovery.

   If Trovio is required to access customer data to provide this support, Trovio may only use that data as needed to provide the services under the CER/Trovio contract.

   Under default operating conditions (that is, without a 'break glass' role provisioned), Trovio personnel cannot view or extract:

   - **the contents of reports, documents, or customer records in storage or databases**
   - **any personally identifiable information, except for limited system metadata (e.g. IP addresses in logs)**
   - **any transaction details.**

Conflict of interest management

The CER/Trovio contract prohibits Trovio and its personnel from engaging in any activity that may create an actual or perceived conflict of interest and requires Trovio to implement restrictions on Trovio's personnel from engaging in such activities. If any potential conflict of interest risk arises, Trovio is contractually obligated to:

1. immediately notify the CER in writing

2. fully disclose all details of the actual or potential conflict of interest
3. take steps reasonably required by the CER, such as:
    a. propose mitigation measures
    b. refrain from proceeding with an activity that may create an actual or perceived conflict of interest until an approved mitigation plan is agreed with the CER, or if the risk cannot be mitigated, refrain from the activity altogether.

Oversight, monitoring and auditing

CER and Trovio maintain the following governance mechanisms:

- a mutually agreed conflict of interest management policy
- weekly contract management and monthly service management meetings to raise any emerging concerns including conflict of interest risks
- a formal Conflict of Interest Register, reviewed annually
- real-time audit logging of all access, especially break glass usage
- process for resolving any contested conflict of interest decisions.