**Publication Date:**
05/07/2024

**Version:**
V1.1

**Contact:**
Ecosystem Restoration Standard
25 Rue de Frémicourt
75015 Paris, FRANCE
info@ers.org

PROGRAMME

# Registry Procedures

## SUMMARY

This document summarises all procedures applicable to the ERS Registry. It aims to provide clarity over its operations, administration, governance, and the efforts put in place to ensure the highest level of transparency and compliance with the carbon market requirements and regulations. This document also sets forward all security compliance elements as provided by APX as the ERS Registry third-party host.

# Table of *Contents*

## NORMATIVE REFERENCES

This document must be read in conjunction with the following documents:

- ERS Programme
- ERS Governance
- Validation and Verification Procedure
- ERS Anti-Fraud Policy
- Code of Ethics and Business Conduct

# Registry *Guidelines*

In addition to the requirements laid out in the ERS Programme, the ERS Registry complies with the following rules.

## TRANSPARENCY AND ACCESSIBILITY

1. Maintain a publicly accessible online platform where participants can access *documentation* and *operations* regarding Restoration Units.
2. Make public any disputes or challenges related to unit issuance or retirement. More details can be found on the ERS Website.
3. Ensure that data privacy and security measures are in place to protect confidential information. More details can be found in ERS' Privacy Policy.

## ACCURACY AND VERIFICATION

1. Allow a robust Validation & Verification process, in collaboration with third-party Validation and Verification Bodies (VVBs), to confirm the accuracy and legitimacy of Restoration Units submitted for registration, via independent audits of ERS-certified Projects. More details can be found in the Validation and Verification Procedure.
2. Maintain the history of every Restoration Unit and its equivalent net GHG removal.

## RETIREMENT AND DOUBLE COUNTING PREVENTION

1. Maintain a secure system for retiring VRUs, preventing double counting (double issuance, double claiming and double use) and double selling of Restoration Units.
2. Enable mechanisms to track retired VRUs and ensure they are not reintroduced into the market.

## GOVERNANCE AND OVERSIGHT

1. Enable a clear governance structure with independent oversight.
2. Define roles, rights, responsibilities and accountabilities for registry administrators, users and Account Holders.
3. Enable procedures for handling conflicts of interest among registry administrators, users and Account Holders. More details can be found in ERS Anti-Fraud Policy.

## CONTINUOUS IMPROVEMENT

1. Regularly review and update its procedures and guidelines to align with evolving best practices and market developments.
2. Seek participant, stakeholder, and expert feedback to improve registry operations and transparency. More details can be found in the Standard Setting and Methodology Development Procedure.

# Registry *Administration*

## ERS REGISTRY HOSTING AND ACCESS

1. The ERS Registry is hosted by APX.
2. The ERS Registry can be accessed at registry.ers.org.

## ADMINISTRATION AUTHORITY

The ERS Registry is administered by the ERS Secretariat. Only Secretariat associates are authorised to issue, cancel, and convert Restoration Units.

## ROLES & PERMISSIONS IN THE REGISTRY

1. The ERS Registry offers four distinct roles, each with specific permissions and responsibilities. These roles are built into the technical specificities of our Registry and cannot be bypassed.

    1.1. **Registry Administrator.** Registry Administrators have the highest level of permissions, including the management of units, Projects, and users. This role is held by the Director of ERS Secretariat.

    1.2. **Secretariat.** Secretariat users can issue and manage units, including the ability to convert, transfer and cancel PRUs and VRUs.

    1.3. **Certification**. Certification users are responsible for creating and managing Projects within the Registry. They have the capability to upload Project-related files and update Project status.

    1.4. **Account Holder.** Account Holders (such as Developers or Restoration Unit Buyers) have the authority to hold Restoration Units in their accounts and manage them, including transferring and retiring units.

## GOVERNANCE AND OVERSIGHT

1. The governance of the ERS Registry includes ensuring that roles and permissions are assigned and managed effectively. To maintain integrity and transparency within the Registry, governance mechanisms include:

    1.1. The ERS Secretariat commitment to enforcing the Registry procedures;

    1.2. Annual reviews of user permissions and roles to prevent unauthorised access;

    1.3. Annual audit of the ERS Secretariat and Certification teams and of the ERS Registry by a third-party auditor.

## COMPLIANCE WITH REGULATIONS

1. The ERS Registry must adhere to all relevant regulations and standards governing carbon markets, including but not limited to the following accreditation schemes:

    1.1. CORSIA;

    1.2. ICROA;

    1.3. IC-VCM.

2. The ERS Registry publicly commits to supporting initiatives working to enable transparency in the carbon market, notably CADTrust.

## CONTINUOUS IMPROVEMENT

The ERS Registry is committed to continuously improving its operations and user experience. Feedback from users and stakeholders is actively sought to enhance the Registry's functionality and ensure alignment with best market practices. More details can be found in the ERS Programme.

# Registry *Operations*

## ACCOUNT CREATION

1. All Registry Account Holders must:

    1.1. Accept the ERS Registry Terms and Conditions.

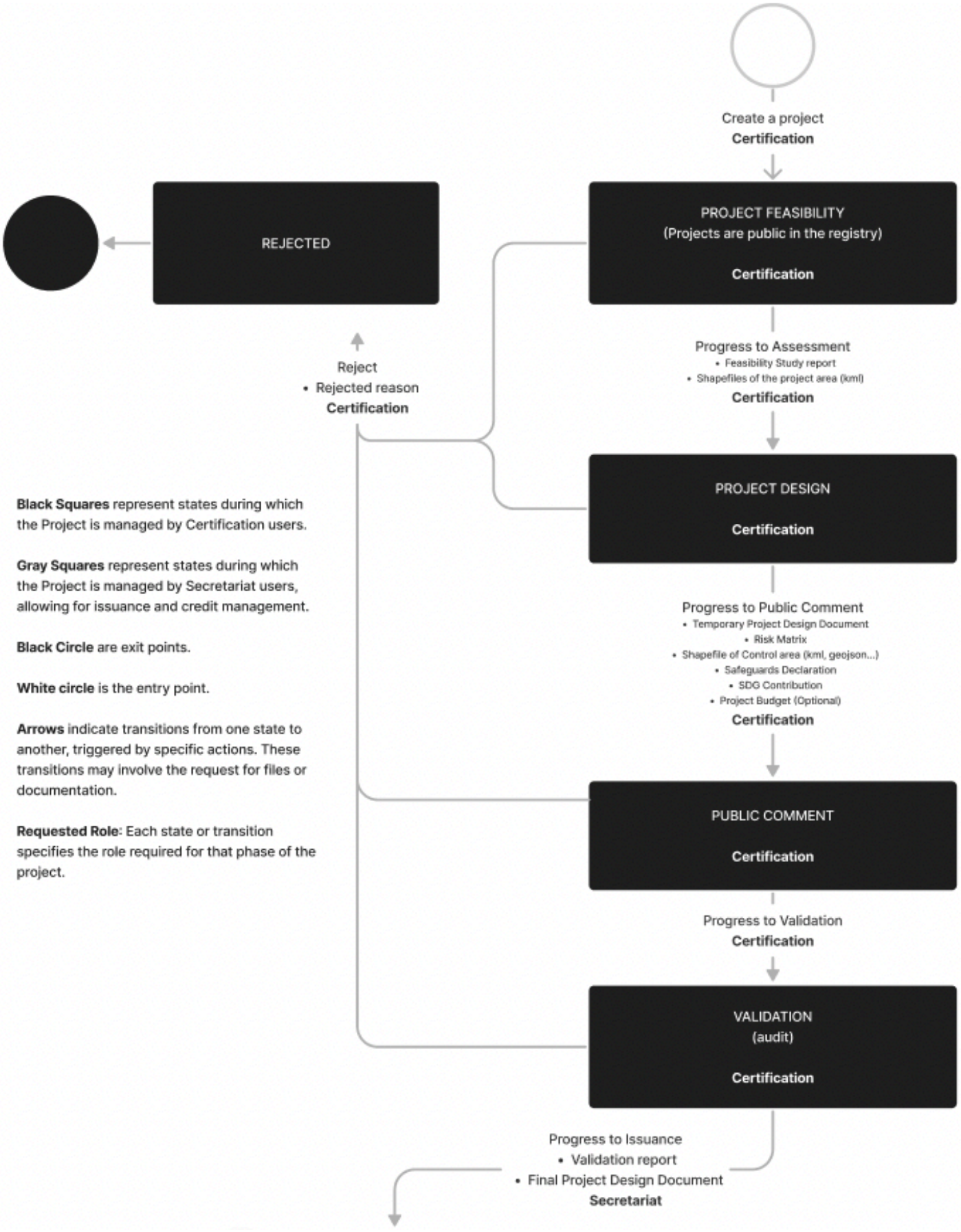
    1.2. Go through KYC/AML verification. Detailed information about the protocol can be found in the Anti-Fraud Policy.

## PROJECT CREATION

1. Projects within the ERS Registry are initiated by the ERS Certification team.
2. Projects are created under the ERS account. Each Project undergoing ERS certification has a registry page under the ERS account, referred to as “Project Page”.
3. The Project lifecycle commences with the status "Project Feasibility."

## PROJECT LIFECYCLE

The Project lifecycle is visualised using a State Machine, which illustrates the progression of a Project through various states and the user roles responsible for managing each state. The State Machine is a visual representation of the Project lifecycle, ensuring clarity and consistency in managing Projects within the ERS Registry.




**Black Squares** represent states during which the Project is managed by Certification users.

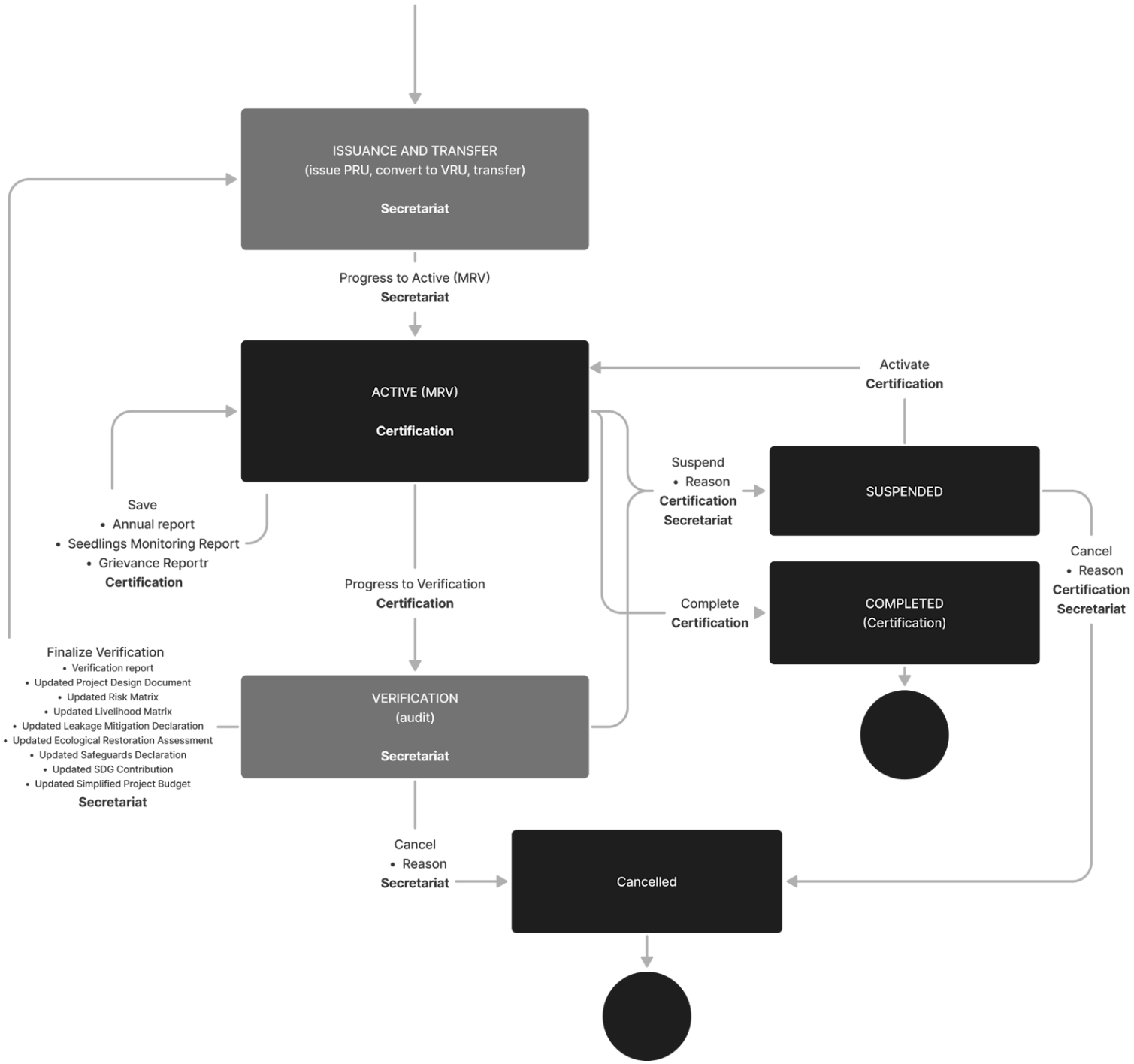
**Gray Squares** represent states during which the Project is managed by Secretariat users, allowing for issuance and credit management.

**Black Circle** are exit points.

**White circle** is the entry point.

**Arrows** indicate transitions from one state to another, triggered by specific actions. These transitions may involve the request for files or documentation.

**Requested Role**: Each state or transition specifies the role required for that phase of the project.


ISSUANCE AND TRANSFER
(issue PRU, convert to VRU, transfer)
Secretariat
Progress to Active (MRV)
Secretariat
ACTIVE (MRV)
Certification
Activate
Certification
Suspend
• Reason
Certification
Secretariat
SUSPENDED
Save
• Annual report
• Seedlings Monitoring Report
• Grievance Reportr
Certification
Progress to Verification
Certification
Complete
Certification
COMPLETED
(Certification)
Cancel
• Reason
Certification
Secretariat
Finalize Verification
• Verification report
• Updated Project Design Document
• Updated Risk Matrix
• Updated Livelihood Matrix
• Updated Leakage Mitigation Declaration
• Updated Ecological Restoration Assessment
• Updated Safeguards Declaration
• Updated SDG Contribution
• Updated Simplified Project Budget
Secretariat
VERIFICATION
(audit)
Secretariat
Cancel
• Reason
Secretariat
Cancelled

# DOCUMENTATION

This section outlines the documentation requirements within the ERS Registry, detailing when and which documents the ERS Certification and Secretariat teams are responsible for uploading throughout the certification process.

These requirements ensure the transparency and accountability of the certification process and support the ongoing measurement, reporting and Verification of Projects.

1. **Project Feasibility Phase.** Upon completing the Project Feasibility phase, a Certification Agent is required to upload the following documents:

    1.1. **Feasibility Study Report.** A comprehensive report detailing the Feasibility study's findings and outcomes.

    1.2. **Shapefile of the Project.** Geographic information system (GIS) shapefiles providing spatial data related to the Project.

    1.3. **Pre-submission Activities Report.** A comprehensive report detailing the results of pre-submission activities. This is only applicable if the Project has carried out pre-submission activities.

2. **Project Design Phase**. Upon completing the Project Design phase, ERS Certification must upload the following documentation:

    2.1. **Provisional Project Design Document.** A preliminary document outlining the project's design, key elements, and appendices.

    2.2. **Risk Assessment Matrix.** An assessment of the Project risks and their potential impacts.

    2.3. **Safeguards Declaration.** Developer’s declaration of environmental and social safeguards in place during the Project.

    2.4. **Project Budget**. A simplified overview of project expenses.

3. **Validation Phase**. Upon completing the Validation phase, a Secretariat Agent is responsible for uploading the following documents:

3.1. **Validation Report**. A report summarising the Project's Validation and its results.

3.2. **Final Project Design Document**. The finalised Project Design Document, including all Project's details and specifications.

4. **Annual Requirements.** On an annual basis, a Certification Agent is required to upload the following document:

4.1. **Annual Report**. A yearly report providing an update on the Project's progress, performance, and any significant changes.

4.2. **Grievance Reports** (if applicable). A report of any grievance filed against a Project, composed of the claim, investigation findings and conclusion.

5. **Verification Phase.**

5.1. Every two (2) to four (4) years, at the end of the Verification Period, a Secretariat Agent is responsible for uploading the following documentation:

5.1.1. **Verification Report**. A report summarising the Project's Verification, including findings and results.

5.2. Every four (4) years, at the end of the Verification Phase, a Certification Agent is responsible for providing the following documentation:

5.2.1. **Verification Report**. A report summarising the Project's Verification, including findings and results.

5.2.2. **Updated Project Design Document**. Any necessary updates or revisions to the project design document and its appendices.

5.2.3. **Updated Risk Assessment Matrix**. An updated assessment of project risks and their potential impacts.

5.2.4. **Updated Safeguards Declaration.** The Developer's declaration of environmental and social safeguards in place during the Project.

5.2.5. **Updated Project Budget**. A simplified overview of the Project's expenses.

## ISSUANCE

### 1. Issuance Authorisation

1.1. The issuance process within the ERS Registry occurs during the "Issuance and Transfer" status.

1.2. Certification Agents request Restoration Units issuance for a Project.

1.3. Only Secretariat users can approve an issuance request and concretely issue Restoration Units.

### 2. Issuance Allocation

2.1. Upon issuance, 20% (rounded up) of PRUs is allocated to ERS Buffer Pool's account.

2.2. The remaining 80% (rounded down) can subsequently be transferred to various Account Holders by the Secretariat.

### 3. Addressing Erroneous Issuance

3.1. Erroneous issuance is considered:

3.1.1. The issuance of PRUs or VRUs that do not exist.

3.1.2. The allocation of Restoration Units, PRUs or VRUs, that do not belong to the Account Holder to which it was credited.

3.2. Every issuance goes through a redundancy system, under which an ERS Secretariat Agent issues Restoration Units, and another ERS Secretariat Agent reviews all issuances of the past week.

3.3. If an erroneous issuance is identified, a report is filed, and the Secretariat Agent cancels the Restoration Units in question.

3.4. Account Holders are subsequently notified of the issue.

3.5. The Registry Administrator retains the authority to cancel erroneously issued assets on behalf of any Account Holder.

3.6. These measures ensure the integrity and accountability of the issuance process within the ERS Registry, safeguarding against errors and discrepancies.

## CONVERSION

1. **Conversion Authorisation**. Conversion of PRUs to VRUs can only be done by Secretariat Agents. This conversion action can occur exclusively when the Project status is "Issuance and Transfer".

2. **Volume Calculation.** The volume of PRUs to be converted into VRUs is determined according to the *Units & Issuance* section of the ERS Programme. This calculation ensures accuracy and transparency in the conversion process.

3. **Distribution of Converted Units.** Upon successful conversion, PRUs must be sequentially converted into VRUs, with each PRU having a unique serial number that determines its conversion order.

## TRANSFER

**1. Secretariat-Initiated Transfers**

1.1. Secretariat users possess the authority to initiate transfers of PRUs and VRUs. These transfers can originate from the Project Account and be directed to any Account Holder's account.

**2. Account Holder-Initiated Transfers**

2.1. Account Holders can initiate proprietary PRUs and VRUs transfers at their discretion. This transfer privilege is not restricted by Project status, allowing Account Holders the flexibility to manage their units as needed.

2.2. Erroneous transfers initiated by an Account Holder are not remediated by ERS.

# CANCELLATION

## 1. Cancellation Events

1.1. Unit cancellations within the ERS Registry are initiated by the Secretariat in response to:

1.1.1. A reversal event. For more details about compensation, refer to the *Compensation* section in ERS Programme.

1.1.2. A double counting event, in the context of Article 6 transfers. For more details about double counting, refer to the *Double Counting* section in the ERS Programme.

1.1.3. A Project's failure. For more details about Project failure, refer to the *Project Failure* section in the ERS Programme.

1.1.4. A Project's underperformance. For more details about Project underperformance, please refer to the *Over/Underperformance* section in the ERS Programme.

1.2. All units cancelled in the ERS Registry can no longer be transferred, retired or cancelled.

## 2. Secretariat's Authority

2.1. Only the Secretariat can cancel VRUs in the Buffer Pool or a Project's account whenever a cancellation event is identified.

## 3. Reversal Events

In case of Reversals, the Secretariat must follow a systematic cancellation approach detailed below:

3.1. **Step 1 - Reversal Quantification.** At Verification, ERS determines if the impact of loss events resulted in Reversal or not. If one or more reversal(s) are confirmed, their nature - avoidable or unavoidable - is established pro-rata to the loss events. Refer to the *Reversal Procedures* at the Methodology level for more details.

3.2. **Step 2 - Reversal Accounting.** The quantified Reversal is accounted for the Verification Period's RUs issuance. Refer to the quantification methods at the Methodology level for more details.

3.3. **Step 3 - VVB Verification.** An accredited VVB presents the ERS Secretariat with a Verification Report. If the Verification confirms the Reversal accounting, the Secretariat must proceed to cancellation.

3.4. **Step 4 - Notification.** The Developer associated with the affected VRUs is notified by ERS, via email, of the incoming cancellation event, and if it has been considered as 'avoidable' or 'unavoidable'.

3.5. **Step 5 - Cancellation.** The ERS Secretariat must cancel VRUs in the Buffer Pool in an amount equal to the net GHG loss during the Verification Period as full compensation for the Reversal. Refer to the *Compensation* section in the ERS Programme for more details.

3.6. **Step 6 - Unit Replacement (if applicable).** If the Reversal has been qualified as avoidable, the Developer must deposit VRUs issued by the Project or other ERS-certified Projects in the Buffer Pool in an amount equal to the net GHG loss of the Verification Period.

## 4. Double Claiming

4.1. **Step 1 - Identification and Quantification.** The Secretariat identifies the double claiming event following the double counting principles in the ERS Programme.

4.2. **Step 2 - Notification.** The Developer is notified and must elaborate and execute the mandatory compensation plan. The plan guarantees that any double-claimed units must be compensated with the same volume of eligible units, as detailed in the Avoiding Double Claiming procedure.

4.3. **Step 3 - Cancellation.** The Developer must cancel the replacement units as full compensation for the double counting. Replacement units

can be ERS units or comparable eligible units approved by ERS that have not been sold or otherwise retired.

**5. Double issuance**

**5.1. Step 1 - Identification and Quantification.** The Secretariat identifies the double issuance event following the double counting principles in the ERS Programme.

5.2. **Step 2 - Notification.** The Developer is notified by the ERS Certification Agent.

5.3. **Step 3 - Cancellation.** The Secretariat must cancel the affected Restoration Units.

## RETIREMENT

**1. Identifying The Retirement Reason**

1.1. Account Holders must select the retirement reason from the following list of options:

1.1.1. **Compensation Claim.** When the retirement aims to balance or neutralise the negative effects of GHG emitted.

1.1.2. **Contribution Claim.** When the retirement aims at adding up to GHG reduction efforts, but does not replace or balance emissions.

**2. Retirement on Behalf of a Specific Entity**

2.1. Account Holders must retire Restoration Units on behalf of a specific Legal Entity or Individual, ensuring that the retirement is attributed to the rightful owner.

2.2. Units can only be retired **once,** regardless of the reason for retirement. Units retired in the ERS Registry can no longer be transferred or cancelled.

3. **Documentation**

3.1. Documentation of the retirement action includes:

3.1.1. The Account Holder requesting the retirement;

3.1.2. The legal entity or individual attributed to the retirement;

3.1.3. The chosen retirement reason and any supporting details;

3.1.4. This documentation is recorded and maintained within the ERS Registry for transparency and verification purposes.

## UNIT STATUS

Every Restoration Unit in the ERS Registry must have one of the following status:

- Active;
- Cancelled;
- Retired.

## DOCUMENTATION DISCLOSURE

1. **Documentation and Record-Keeping**

1.1. The ERS Registry publicly discloses the content of the Buffer Pool, including details about the origin of Restoration Units such as the Project type, vintage, etc.

1.2. The ERS registry publicly discloses on every Project page:

1.2.1. Project ID;

1.2.2. Project Name;

1.2.3. Country;

1.2.4. Geographic coordinates on a map;

1.2.5. Project description;

1.2.6. Project Developer;

1.2.7. Type;

1.2.8. Methodology;

1.2.9. Status;

1.2.10. Labels

1.2.11. Project registration;

1.2.12. Crediting period start;

1.2.13. Crediting period end;

1.2.14. Project size (hectares);

1.2.15. Annual Reports containing all loss events, including those leading to cancellations;

1.2.16. Project Design Documents.

## INTER-REGISTRIES OPERATIONS

1. **Definition**

   Inter-registries operations involve the interaction and exchange of carbon credits and related data between different carbon registries or platforms. These operations may include credit transfers, retirement tracking, and credit issuance across multiple registries.

2. **Transfer Restrictions**

   As of the current policy and operational framework, ERS' Restoration Units held within the ERS Registry cannot be transferred out from the APX registry. This restriction ensures the integrity, tracking, and transparency of ERS unit transactions while maintaining consistency within the APX registry ecosystem.

3. **Future Considerations**

3.1. ERS remains committed to exploring opportunities for inter-registries operations that align with industry standards and regulatory requirements. Future considerations include potential collaborations, partnerships, or regulatory changes that enable the secure and compliant transfer of ERS units between registries.

3.1.1. ERS closely follows the work done by Climate Action Data Trust and is willing to connect the ERS Registry at a more developed stage.

## 4. Compliance and Adaptation

ERS is committed to monitoring industry developments, regulatory changes, and best practices related to inter-registry operations. The organisation is prepared to adapt its policies and procedures as needed to facilitate such operations while maintaining the highest standards of transparency and accountability.

# Labelling and *Serialisation*

This section outlines the principles of labelling and serialisation within the ERS Registry, highlighting their role in ensuring the uniqueness and traceability of Restoration Units.

## UNIQUENESS

1. Each Restoration Unit within the ERS Registry is unique and represents the net removal of one tonne of carbon dioxide equivalent, alongside positive impacts on ecological recovery and local livelihoods. To maintain this uniqueness, the following principles apply:

    1.1. **Ownership**: A unit is owned by only one account at a time within the ERS Registry.

    1.2. **Transfer**: A unit can be transferred to only one account at a time within the ERS Registry.

## SERIALISATION

Serialisation is a critical aspect of unit management. It ensures transparency and accountability and protects against the risks of double counting. The ERS Registry employs a unique serialisation methodology.

1. All units within the ERS Registry are assigned a unique serial number with the following format:

    *ERS-[project type]-[project id]-[countrycode]-[unit type]-[issuance date or vintage]-[batch]-[block start]-[block end]*

2. System Identifier or Originating Registry: ERS

3. Project Type:
    3.1. 0 - for Reforestation;
    3.2. 1 - for Terrestrial Forest Restoration.
4. Country Code;
5. Unit Type;
6. Issuance date (for PRU) or vintage (for VRU);
7. Batch Number: Numeric value assigned to each batch of credits per originating issuance;
8. Serial Block Start: Numeric values assigned by the registry from 1 - 999,999,999;
9. Serial Block End: Numeric values assigned by the registry from 1 - 999,999,999.

These unique and immutable serial numbers allow for the complete traceability of each unit throughout its entire lifecycle.

## PUBLIC INFORMATION AND CROSS-REFERENCE

Information about the Project's location is available on the Project page, using the project-ID represented in the serial number. Stakeholders can cross-reference this information with Project publications that provide geodetic coordinates, ensuring transparency regarding each unique unit's country and sector of origin, vintage, and original (and, if relevant, revised) Project registration date.

## LABELLING

1. Assets meeting the eligibility requirements for ICAO's CORSIA, ICROA, and IC-VCM are labelled as such. Labels are reflected in the data warehouse views.
2. Retroactive labelling is applied for previously issued units, ensuring compliance with international standards.

# Conflicts of *Interest*

## PREVENTING CONFLICTS OF INTEREST

ERS is committed to preventing conflicts of interest in the governance and provision of registry services through robust policies and processes. The primary measure in place is the clear separation between the Certification and Secretariat teams at the registry level.

1. **Certification/Secretariat Scopes**: The roles and permissions of the Certification and Secretariat teams are carefully defined to minimise potential conflicts. Each team has specific responsibilities, ensuring a clear and distinct division of tasks. Refer to the ERS Governance document for more details.

2. **Conflicts of Interest provisions**: ERS has established explicit conflict of interest policies that are readily accessible to all relevant parties, outlining the principles and guidelines to prevent conflicts and promote transparency. ERS mandates its Agents to avoid conflicts of interest that interfere with ERS' objectives, encompassing financial, commercial, and fiduciary conflicts. Agents must declare all actual and potential conflicts, and failure to do so may result in the termination or adjustment of their role within ERS. Agents' external interests, relationships with immediate family members in business contexts, and misuse of ERS resources are subject to strict guidelines. More information is available in ERS' Code of Ethics and Business Conduct and Anti-Fraud Policy documents.

## DETECTING AND ADDRESSING CONFLICTS OF INTEREST

When conflicts of interest arise, ERS ensures that they are appropriately declared, addressed, and isolated. Refer to ERS Anti-Fraud Policy and Code of Ethics and Business Conduct for more details.

# Security *Compliance*

All information contained in this section was provided by APX (the registry service provider) through electronic mail and was received by ERS on August 16 2023, as part of the contractual relationship between the companies.

## SOC2

The registry technology provider has been SOC2 certified since 2018 and recently concluded its 2022 audit. The audit affirms that they conform to Trust Services Principles and Criteria for Security, Availability and Processing Integrity by the American Institute of Certified Public Accountants (AICPA). The completion of this audit provides additional assurance that the technology provider designs and implements services according to the highest standards to protect the availability of the ERS Registry, and execution of internal processes.

## MAINTENANCE OF SOFTWARE AND HARDWARE

1. The registry technology provider utilises rich web-based client technology, working on Angular UI framework and Java mid-tier server application and associated services, leveraging Azure-hosted replicated SQL Server databases to provide a robust underlying data service. This ensures high-speed storage that permits the retention of multiple years of transaction-level historical data online and includes:

    1.1. Fully redundant data centre locations in geographically separated regions of the United States;

    1.2. Fully redundant network infrastructures in each data centre location and Operations facility;

    1.3. Data replication between the data centres and off-site backup of the database;

1.4. Off-site operations facilities to handle the program in the event that the primary Operations facility cannot be used. This includes workstations, network access, and automated phone rerouting.

## DISASTER RECOVERY

1. The system must be backed up for two types of failures:

   1.1. Loss of the hardware due to damage;

   1.2. Data loss or data corruption.

2. For "loss of hardware," the "image" backup method is used. The "image" allows the operating system to be re-constructed in a short period of time once the damaged hardware has been repaired.

3. For "data loss or data corruption," the provider electronically places multiple copies of the database backup across geographically distributed storage. This allows to retrieve and, if necessary, restore the data to the same or different hardware.

4. Ad-hoc backups (archives) of the databases are a normal course of operation for the registry. This is currently employed by the registry technology provider in their database operations and is executed as required. The archived backups are stored using the previously described redundant, geographically distributed storage.

5. Recovery of the Operating System, Application, or Database must use existing procedures which include some of the following:

   5.1. Reload of the database from a known recovery point using the "backed up" copy of the database.

   5.2. Reload of the database to a known recovery point using the database transaction logs applied to the restored database created from a "backed up" copy.

5.3. Reload of the database on the existing production system or test system available as part of our SaaS services.

6. Backups are maintained for a minimum of two (2) weeks.

## NETWORK SECURITY

The registry technology provider data centres are protected using industry-standard equipment and access methods, including firewalls and other associated networking infrastructure with fine-grained policies defining exactly which traffic is allowed into and out of the servers, both from internal services as well as the public internet. Their Network Security Group model allows the provider to ensure only traffic appropriate for their applications is allowed into the environment. Events related to the networking and application infrastructure are recorded to a central console that must be monitored 24-hours/day by dedicated security staff who must review reported events of excessive login failures and report the events to the appropriate staff.

## SERVER SECURITY

Server systems are deployed with fine-grained access policies. Direct access to the servers is only allowed for approved personnel responsible for the administration of infrastructure. Personnel access to the servers is only allowed from the registry technology provider's Corporate network. There is no direct access to the servers from the internet. Servers have anti-virus and file system monitoring utilities that report events to a central console monitored by the 24-hour operations group and IT security staff. Login/authentication events are recorded and available for review. Backup of each server's operating system is taken to allow for the quick restoration of a server in the unlikely condition that the system becomes unavailable.

## DATABASE SECURITY

1. The database configuration must be performed to allow appropriate access to records depending on the individual's roles/privileges:

1.1. Users are only able to access and modify the records appropriate for their function.

1.2. The Administrator is only able to access and modify the records appropriate for their function.

1.3. Staff responsible for the maintenance of the system have only the minimum level of access to the database needed to complete their job function.

1.4. Database administrators have full access to the database records. This is required for them to fulfil their job function.

1.5. IT staff have no access to the system database.

1.6. Access to the database is available to the regular application users and application users with Administrator roles solely via the application user interface. Such users are not allowed direct access to the database.

2. Under no circumstances can direct access to the database occur directly from the internet.

## APPLICATION SECURITY

Access to application features is based on the Account and privileges granted to the authenticated user. The login name and password must be used to authenticate each user. Multi-factor authentication is also available. Each user is assigned a role. The role grants the user access to a set of modules and also dictates specific data records that the user is entitled to have access to. Each module provides a set of functions that enables the user to accomplish a task or set of tasks. Each attempt at login, success or failure, is recorded in the system log for review by the System Administrator login role.

## END-USER SECURITY

1. Access to the Registries is done via SSL/HTTPS-secured communication. Individual users are challenged for their unique username and password in

order to access the application. Additionally, multi-factor authentication is available if desired to be in place. After the username and password are authenticated and the second-factor authentication is completed, the user gains access to the application's home page. To protect the integrity of passwords, passwords are required to adhere to the following rules: 8 to 16 characters in length; at least one lower case character, at least one upper case character, at least one digit, and at least one special character.

2. To ensure compliance with security provisions, ERS regularly audits and evaluates the security measures in place within the registry. The specific protocols and processes are as follows:

    2.1. Security and Provisions for Regular Security Audits: ERS conducts periodic security audits or evaluations to assess the effectiveness of security provisions.

    2.2. Clarification: The nature of the audit or evaluation may encompass both ERS's auditing of the registry provider's security processes and protocols and the verification of evidence regarding the registry provider's security practices. The exact scope and details of the audit are determined based on the specific requirements and standards.

3. These provisions highlight ERS' commitment to preventing conflicts of interest, addressing them when they arise, and ensuring compliance with security provisions through regular audits and evaluations. These measures seek to maintain the integrity, transparency, and security of the ERS Registry.

## DATA BREACH

In the event of a data breach identified by the ERS or by the Registry's host APX, ERS must communicate via email and within forty-eight hours of notice all impacted Registry's account holders and relevant Accreditation Bodies Secretariats, such as the ICAO Secretariat.

ERS shall keep all parties impacted up-to-date with the breach investigation's advancements by providing regular email updates until the matter is solved.

**Ecosystem Restoration Standard**

info@ers.org | www.ers.org