Vanuatu International Shipping Registry

(VISR)

Quality Management System (QMS)

Policy: Forgery Prevention, Detection & Response

Issued by the Maritime Administrator

Document Control

Document Title	VISR Forgery Prevention, Detection & Response Policy (FPDRP)
Policy ID	VISR-QMS-FPDRP
Version	1.0 (External copy)
Effective Date	01 January 2026
Issued By	Maritime Administrator, VISR (and in the exercise of delegated powers as Deputy Commissioner / Assistant Commissioner of Maritime Affairs)
Applies To	All VISR staff; VISR-appointed Special Agents; Recognized Organizations (ROs); Flag State Inspectors (FSIs); shipowners, operators and managers; and relevant stakeholders relying on VISR documentation.

Distribution	VISR internal; VMSA (for oversight); authorized partners (as applicable); external publication (as approved).

Introduction

This Policy establishes VISR's controls and procedures to prevent, detect, and respond to forgery, counterfeiting, alteration, unauthorized reproduction, circulation, or use of documents

and digital verification mechanisms purporting to be issued by, verified by, or affiliated with the Vanuatu International Shipping Registry (VISR). It is designed to protect the sovereign integrity of the Vanuatu flag, support sanctions compliance, and maintain audit readiness consistent with international best practice.

1. Policy Statement

VISR adopts a zero-tolerance position toward the forging, counterfeiting, alteration, unauthorized reproduction, circulation, or use of any VISR document, record, digital verification mechanism, or communication. Suspected forgery is treated as a serious regulatory and criminal matter.

2. Purpose

This Policy:

- Defines preventive controls to reduce forgery and misuse of VISR instruments;
- Sets verification and detection standards for stakeholders and VISR staff;
- Establishes a structured incident response procedure (intake, triage, preservation, containment, escalation);
- Defines enforcement measures and penalty pathways; and
- Assigns roles, responsibilities, and recordkeeping requirements.

3. Scope

This Policy applies to:

- All VISR-issued instruments (paper and electronic), including Certificates of Registry (permanent/provisional/interim), transcripts, endorsements, deletion letters, and official communications;
- All digital verification outputs and QR-code validation pathways associated with VISR documentation;
- All persons and entities producing, requesting, commissioning, distributing, presenting, relying upon, or facilitating use of VISR documentation; and
- All VISR staff, contractors, and authorized service partners (agents, FSIs, ROs).

4. Definitions

- VISR Document / VISR Instrument: Any paper or digital record that VISR issues, signs, endorses, validates, or represents as official.
- Forgery: Any unauthorized creation, alteration, reproduction, or misuse of a VISR document or identity element (seal, signature, serial number, QR code, verification link, letterhead, email identity), including presenting such items as genuine.
- False Flag Representation: Any representation that a vessel is entitled to fly the Vanuatu flag when it is not registered, has been deleted, suspended, or has otherwise lost entitlement.

- Impersonation Infrastructure: Any website, domain, portal, email address, or digital service that mimics or falsely claims VISR identity or verification capability.
- Incident: Any report, suspicion, or evidence of forged documentation, false flag claims, or impersonation infrastructure.

5. Governance and Authority

This Policy is issued by the Maritime Administrator and is enforced through VISR administrative authority governing registry operations and access. Where applicable, enforcement actions may also be taken in the exercise of delegated statutory authority vested in the Deputy Commissioner / Assistant Commissioner of Maritime Affairs under the Maritime Act [CAP 131] (as amended), the VMSA Act, and related delegations. Nothing in this Policy limits the powers of competent authorities or courts.

6. Prevention Controls

6.1 Document Issuance Controls

- Controlled templates (version controlled; restricted access).
- Authorized signatory controls (maintained authorized signatory list; periodic review).
- Unique serial numbering with non-reusable issuance register.
- Separation of duties (creation vs approval vs release) for certificates and letters.
- Sanctions/restricted-parties screening prior to issuance where required by VISR policy.
- Secure storage of seals and signature devices (physical and digital).

6.2 Security Features

- Unique certificate numbers and issuance timestamps.
- Machine-readable identifiers (verification code and/or QR code) linked only to VISR-authorized channels.
- Consistent formatting and mandatory security language.
- Where feasible, digitally signed PDFs and tamper-resistant certificate outputs.

6.3 Official Domains and Communications

- VISR designates official domains and official verification channels; any look-alike domain is treated as suspect unless confirmed in writing by VISR.
- VISR verification contact email for suspected fraud and document checks: technical@register-vu.com.

6.4 IT and Access Security

- Multi-factor authentication for systems that can generate or validate certificates.
- Administrative access logging and monitoring.
- Regular domain monitoring for look-alike registrations and email spoofing.
- Secure retention of deployment and change logs for verification systems.

7. Verification and Detection

7.1 Stakeholder Verification Standard

Any stakeholder presented with VISR documentation should verify authenticity through official VISR channels. Verification requests and suspected forgery reports must be sent to: technical@register-vu.com.

7.2 Internal Verification Steps (VISR)

1. Confirm certificate number and vessel identifiers against the internal issuance register.
2. Validate issuance date, authorized signatory status, and registry status at the time of issuance.
3. Validate any QR code or verification link resolves only to VISR-authorized channels.
4. Confirm current registry status (registered / deleted / suspended) and applicable restrictions.
5. Issue a written authenticity response with an internal reference number and audit trail.

7.3 Red Flags

The following indicators trigger High Suspicion and require escalation:

- QR code or verification link resolves to a non-official domain.
- Document purports to be issued after deletion or suspension.
- Mismatch in vessel particulars, tonnage, owner/operator details, or signatory information.
- Unusual validity periods, wording, or formatting inconsistent with VISR templates.
- Sender email spoofing or look-alike domains.
- Requests for secrecy or urgent validation for “port clearance” outside normal procedures.

8. Incident Response Procedure

8.1 Intake and Logging

All incidents must be recorded in the Forgery Incident Register with date/time, reporter details, vessel identifiers, document identifiers, suspected domain/QR link, and an initial risk classification.

8.2 Severity Levels

- Critical: active false flag claims, suspected sanctions evasion, PSC involvement, insurance/banking reliance risk, or widespread circulation.
- High: forged certificates detected or impersonation infrastructure active with material stakeholder exposure.
- Medium: suspicious document requiring verification with limited exposure.
- Low: look-alike domains without evidence of document fraud.

8.3 Evidence Preservation

VISR will preserve (as applicable):

- Original files (PDFs) and metadata;
- Email transmissions, including full headers;
- Screenshots of websites and QR destinations;
- WHOIS and DNS records;
- Internal verification logs and registry status confirmations;
- Correspondence with registrars/hosts and any takedown confirmations.

8.4 Containment and Notification

- Issue warnings/circulars where required to protect stakeholders.
- Notify relevant partners (ROs, agents, insurers/P&I, banks) when there is reliance risk.
- Apply compliance holds and restrict registry access where an agent or counterparty is implicated.
- Coordinate messaging with competent authorities where national interest or reputational risk exists.

8.5 Takedown and International Cooperation

- Notify registrar abuse contacts and request immediate suspension of impersonation domains; request preservation of registration data.
- Notify hosting provider(s) and request preservation of logs and customer/payment records.
- Where voluntary disclosure is refused, refer the matter to law enforcement and pursue international cooperation channels (including Interpol) to compel disclosure.

9. Enforcement Measures and Penalty Pathways

9.1 Administrative Measures

- Refusal, suspension, or deletion of registration services as permitted by law and policy.
- Blacklisting of implicated vessels and associated beneficial owners/entities.
- Suspension or revocation of recognized agent status and termination of access to VISR systems.
- Notification to relevant authorities and stakeholders where required to protect the public interest.

9.2 Monetary Penalties and Legal Liability

Where empowered under applicable law and delegated authority, administrative monetary penalties may be pursued. Where criminal conduct is indicated, VISR will refer matters for investigation and prosecution. VISR's policy position is to seek the highest penalties available under law where forgery involves false flag representation, commercial reliance, or sanctions evasion risk.

10. Records, Audit and Training

- Maintain a Forgery Incident Register and evidence archive with chain-of-custody notes.
- Retain issuance logs, signatory lists, and template control records for audit readiness.
- Conduct periodic staff/agent awareness training on verification, red flags, and reporting obligations.
- Review this Policy after any High/Critical incident and at least annually.

11. Review and Revision Control

This Policy is reviewed at least annually and may be updated to reflect legislative amendments, IMO/ILO developments, risk trends, and audit findings. Superseded versions must be archived and marked obsolete.

Approval

Issued by authority of:

Saade Makhlouf
Maritime Administrator, VISR
And in the exercise of delegated powers as Deputy Commissioner / Assistant Commissioner of Maritime Affairs
Republic of Vanuatu