VesselIQ

IMO MSC-428(98) Cyber Risk Management Compliance Statement

How VesselIQ supports vessel operators in meeting IMO cyber risk management obligations

Document ref: VIQ-CYBER-001 | Version 1.0 | Issued: 6 April 2026 | vesseliq.app

1. Purpose and Scope

This statement documents how the VesselIQ platform supports vessel operators, managers, and owners in discharging their cyber risk management obligations under IMO Resolution MSC-428(98) and the associated IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). It is intended for use by Designated Persons Ashore (DPAs), fleet managers, flag state auditors, and classification society surveyors.

VesselIQ is a cloud-based vessel systems documentation and crew handover platform. It is not itself a Safety Management System (SMS), nor a substitute for any SOLAS Chapter IX obligation; rather, it is a supporting tool that helps operators maintain accurate, accessible records of on-board systems as part of a broader SMS.

2. Regulatory Background

IMO Resolution MSC-428(98) (2017)

Requires that cyber risks be appropriately addressed in existing ISM Code Safety Management Systems no later than the first annual ISM audit after 1 January 2021.

IMO MSC-FAL.1/Circ.3 (2017)

Provides guidelines on maritime cyber risk management covering five functional elements: Identify, Protect, Detect, Respond, Recover.

BIMCO Cyber Security Guidelines (v4) (2023)

Industry-standard guidance endorsed by BIMCO, ICS, INTERCARGO, INTERTANKO and OCIMF, providing practical implementation guidance for ship operators.

IACS UR E26 / E27 (2024)

Unified Requirements for cyber resilience of ships and on-board systems, mandatory for newbuilds at classification societies including DNV, Lloyd's Register, Bureau Veritas.

UK MCA / Flag State Guidance (Ongoing)

MCA guidance aligns with IMO requirements; operators under UK flag must demonstrate cyber risk management within their ISM audits.

3. IMO Functional Elements — Compliance Matrix

The table below maps the five IMO cyber risk management functional elements (as elaborated in MSC-FAL.1/Circ.3 and the BIMCO Guidelines) to specific controls implemented within or supported by the VesselIQ platform.

IMO / BIMCO Requirement	VesselIQ Control	Status
Identify critical systems and data assets	Vessel systems registry with categorised assets and risk classification	✓ Supported
Protect systems from unauthorised access	Role-based access control, 2FA (TOTP), brute force lockout, session timeout	✓ Implemented
Detect anomalies and incidents	Immutable audit log capturing all user actions, resource access and changes	✓ Implemented
Respond to and manage cyber incidents	Documented incident response contact (security@vesseliq.app); audit trail supports investigation	✓ Supported
Recover and restore operations	Data hosted on Supabase (PostgreSQL) with automated backups; Vercel edge deployment with instant rollback	✓ Supported
Crew training and awareness	User guidance built into handover and documentation workflows; operator responsible for crew training	■ Operator responsibility
Third-party / supply chain risk management	Sub-processors documented in Privacy Policy; DPA-compliant agreements with Supabase, Vercel, Anthropic	✓ Documented

■ *items indicate areas where VesselIQ provides supporting capability but the primary obligation rests with the vessel operator as part of their SMS.*

4. Technical Security Controls

Access Control & Authentication

- Multi-factor authentication (TOTP) enforced at AAL2 level via Supabase MFA
- Role-based access control limiting data access to authorised users per vessel
- Brute force protection: account lockout after 5 failed attempts with 5-minute cooldown
- Automatic session timeout after 60 minutes of inactivity
- Minimum password length of 12 characters with complexity requirements (upper, lower, numeric, special)

Data Protection & Encryption

- All data encrypted in transit via TLS 1.2+ (enforced by Vercel edge network)
- Database encrypted at rest (AES-256) by Supabase/PostgreSQL
- File storage encrypted at rest with Row-Level Security (RLS) policies
- Signed URLs for media access with 30-day expiry

Audit Logging & Monitoring

- Immutable audit log table — PostgreSQL rules block UPDATE and DELETE operations
- All user actions (imports, media uploads, service log entries) recorded with IP address, user agent and timestamp
- Audit entries attributable to individual user accounts

Input Validation & Application Security

- Server-side rate limiting on all API endpoints (10–60 requests/minute by endpoint)
- Input sanitisation against XSS on all rich-text and document import pathways
- File type whitelisting and size limits on all upload endpoints
- CORS policy restricting cross-origin requests to authorised origins only

- UUID validation on all resource identifiers

Infrastructure & Supply Chain

- Hosted on Vercel (SOC 2 Type II certified) with global edge deployment
- Database on Supabase (SOC 2 Type II, ISO 27001 in progress)
- Automated dependency vulnerability scanning via GitHub Dependabot
- Transactional email via Resend with DKIM/SPF/DMARC authentication

5. Data Residency & Sub-processors

Sub-processor	Role	Data Location	Certification
Supabase Inc.	Database & Auth	AWS us-east-1	SOC 2 Type II
Vercel Inc.	Application hosting & CDN	Global edge / US primary	SOC 2 Type II
Anthropic PBC	AI features (Claude API)	US	SOC 2 Type II
Resend Inc.	Transactional email	US (us-east-1)	SOC 2 in progress
Cloudflare Inc.	DNS, DDoS protection, email routing	Global	ISO 27001, SOC 2

6. Operator Responsibilities

VesselIQ is a supporting tool within the operator's broader Safety Management System. The following responsibilities remain with the vessel operator, manager, or owner:

- Incorporating VesselIQ usage into the vessel's SMS cyber risk assessment
- Defining and maintaining user access levels appropriate to crew roles
- Ensuring crew are trained on the platform and aware of cyber hygiene obligations
- Conducting periodic review of audit logs for anomalous activity
- Reporting cyber incidents to the relevant flag state and, where applicable, to the DPA
- Maintaining offline backup procedures in the event of platform unavailability
- Ensuring that data entered into VesselIQ does not include classified or export-controlled information

7. Continuous Improvement & Certification Roadmap

Initiative	Target	Status
Cyber Essentials (UK NCSC)	Q3 2026	Planned
ISO 27001 Information Security Management	Q1 2027	Planned
SOC 2 Type II (Trust Services Criteria)	Q2 2027	Planned
Penetration testing (annual)	Q4 2026	Planned
BIMCO Cyber Security Guidelines v4 self-assessment	Q2 2026	In progress

8. Security Contact & Responsible Disclosure

VesselIQ operates a responsible disclosure programme. Security researchers and operators who identify vulnerabilities or have security concerns are encouraged to contact us before public disclosure to allow remediation.

Security reports	security@vesseliq.app
General enquiries	hello@vesseliq.app
Security policy	https://vesseliq.app/security-policy
security.txt	https://vesseliq.app/.well-known/security.txt

This document is provided for informational purposes and does not constitute legal, regulatory, or classification advice. Operators remain solely responsible for ensuring compliance with applicable flag state, port state, and classification society requirements. VesselIQ is not a certified Safety Management System and does not replace any obligation under SOLAS Chapter IX or the ISM Code.