Security policy

Last updated 07.02.24

SEA-FLUX
VESSEL MANAGEMENT SOFTWARE

This information security policy describes how Sea-Flux is committed to ensuring your information is secure.

Sea-Flux Application

Our commitment to your information security

We maintain a secure process for the collection, transmission, and storage of your personal information.
Sea-Flux suggests that all users keep their browsers up to date to ensure a high level of security is maintained. Old browsers could make it difficult to use modern websites, or could allow malicious websites to read your files, steal passwords, and infect your computer.

Protecting personal information

The Sea-Flux application is designed to hold some personal information, both of registered users, and individuals such as crew (should these modules of Sea-Flux be used by you).

This information, when collected, is held securely using Google Firebase Cloud based platform. Cloud based architecture generally offers better redundancy, availability, and scalability.

What platforms are Sea-Flux available on?

Web, iOS app, Android app for both tablet and mobile.

What Hosting service does Sea-Flux use?

The web client (which is just static HTML5), is hosted using Netlify.

What technology is Sea-Flux built with?

The code base is written in typescript using the React framework and Ionic. The iOS & Android App bridge to native functionality using Ionic Capacitor. Server side functions are built using Google's Firebase Cloud Based Platform.

How often is the data backed up?

Data is backed up at 3am every day.

How is the Authentication and data managed?

1. User Authentication is handled using Firebase Authentication.
The only method allowed is email and password. No passwords are stored in the Sea-Flux database.

2. Data is managed using Cloud Firestore.
To access or change data in Sea-Flux, the user must be authenticated and have the appropriate credentials such as being part of the Licensee account in question and having the specific user permissions required.

Where is the database located?

Sea-Flux data is primarily handled by Google's data centre in Southeast Australia (Sydney).
1. Files are stored using Cloud Storage for Firebase.

2. Other functions such as regularly scheduled jobs, functions triggered from data changes and a few other specialised requests are handled by Cloud Functions for Firebase.

All four of these services provided have been certified under major privacy and security standards including:
ISO 27001, see: https://firebase.google.com/static/downloads/gdpr/NOV2022_Firebase_ISO_27001.pdf

ISO 27017, see: https://cloud.google.com/security/compliance/iso-27017

ISO 27018, see: https://cloud.google.com/security/compliance/iso-27018

SOC 1, see: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report

SOC 2, see: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

SOC 3, see https://firebase.google.com/static/downloads/gdpr/JUNE2022_Firebase_SOC3_Report.pdf

All requests to load or save data are made over secure connections (HTTPS).
In addition to this, the four services listed above also encrypt their data at ReST.

For more information see: https://firebase.google.com/support/privacy

Logging In

You can save your login details on your browser, only if your computer is secure, and only ever used by you, and you alone. If this is not the case you MUST use your unique login details that have been provided to you by Sea-Flux, or your allocated administrator – each time you log into the Sea Flux application.

Security enforcement

You must tell us immediately about any unauthorised access or use of the Sea-Flux web service or information collected and maintained by us.

We will investigate any violation of the security of your personal information that we're told about and if necessary, take action to prevent any further violations.

In the unlikely event that we believe the security of your personal information in our possession or control may have been compromised, we will immediately do all things necessary to contain and manage the potential breach.

Personal Devices

Use of personal devices such as tablets and mobile phones used to access the Sea-Flux application are the responsibility of the customer, and use thereof is governed by the security policies of that organisation.

Contact us

If you are concerned that this information security policy may have been breached or the security of your personal information has been compromised, please email us immediately at safety@sea-flux.com or call customer services on +64223080209

More information about our policies for protecting your personal information can be found in our Terms of Use and our privacy policy.

Updated	Changes made	Changes made by
13.10.23	General review, updated Google links	Tai
07.02.24	Full review and minor edits including, update to third party software providers.	Tai