OSPREY TRIPADMIN SYSTEM SECURITY

This Policy covers the security and use of the Osprey TripAdmin system. The main objective of this Policy is to define

- the general security principles for the Osprey TripAdmin software
- data management and privacy principles for the information stored, processed and transmitted by the system
- responsibilities with regards to system security and data management and privacy

1. About the System

The TripAdmin system is a proprietary software solution for the marine insurance industry, developed and owned by Osprey Solutions AS, Norway. The solution provides international marine insurers and shipowners with a shared platform for digitization of reporting processes related to vessel trade in high risk areas. The system allows for full process-automation through ingestion of vessel position data from AIS or GPS tracking sources.

Access to the TripAdmin is provided as a Software-as-a-Service (SaaS) via the Internet. The TripAdmin is supported by all major browsers.

2. Secure architecture and design

Osprey Solutions has prioritized security and privacy throughout every part of the design and development process for the TripAdmin. Architecture and controls in TripAdmin are designed to enhance productivity, so that users can focus on using data to meet their business goals and not worry about unintentional data access.

- Platform

The TripAdmin is hosted on the DigitalOcean cloud infrastructure, a leading developer platform with one of the highest uptime standards in the industry. DigitalOcean is certified on multiple international standards, including SOC 1 Type II, SOC 2 Type II, ISO/IEC 27001, and PCI-DSS in the international standard ISO/IEC 27001:2013 for information security controls. All DigitalOcean regional data centers are independently audited, and many are certified by internationally recognized attestation and certification compliance standards.

- Access control

a) ID and authentication

The TripAdmin uses the secure login infrastructure service Auth0 to authenticate and authorize users. When a user initiates their login on the TripAdmin, the system redirects them to the Auth0's service for authentication. Once authenticated by Auth0, the user is redirected back to the TripAdmin with an access-token that is valid for 10 hours. After 10 hrs, or if the user has been inactive for 120 minutes or closes their browser, they will need to re-authenticate with Auth0.

The standard rules for authentication are set by Osprey in Auth0 to meet the highest security standards including

- 2 Factor Authentication through Google Authenticator
- Highest/excellent password strength according to prevalent Auth0 recommendations
- Password not included in list of world’s 10,000 most used passwords
- No re-use of previous password

b) Roles and permissions

Applicable user roles and permissions are configured on the Management site in the TripAdmin. Once authenticated by Auth0, the system will login the user with the pre-defined access rights and permissions for the role the administrator has assigned them.

Administrators can manage, update, change or delete registered users through the Management site in TripAdmin, in accordance with the company’s own policies and procedures for user management. In addition to overviews of registered users, roles and permissions, the Management site of the TripAdmin also provides a detailed log to monitor activity and identify potential unauthorized use.

- Backup

The TripAdmin uses a managed database cluster service that includes daily backups with 7-day history and point-in-time recovery. Static assets are stored on a S3-compatible object storage service built with Ceph. Ceph is built for redundancy so the loss of a single drive, server, or even an entire data center rack does not compromise data integrity or availability. Standby database nodes with automated failover will automatically start up in case one of the other database nodes should fail. The application itself is load balanced.

- Secure infrastructure

TripAdmin uses the CloudFlare security platform as a reverse proxy to mitigate DDoS attacks, WAF and similar cyber threats. By using CloudFlare the IP addresses of the TripAdmin application servers are hidden from public for increased server security.

Antivirus and root kit/vulnerability scanners are installed on all the application servers, and 3rd party monitoring solution Snyk.io is used to protect the TripAdmin code repository against deployment of malicious or vulnerable code.

- Monitoring and log

The TripAdmin logs all activity with a time stamp and information on who triggered the action in the application. The log files can be viewed by administrators.

3. Data management and privacy

- Data ownership

Data processed through the TripAdmin solution is protected as the property of the customer. Access to company data is controlled by the customer who sets access rights for each user. Data required by Osprey to analyse system performance and improve general system functionality is managed according to contract terms for such use.

- Personal data protection

The TripAdmin is designed and developed based on cyber security and privacy principles imposed by Norwegian data protection laws, and the EU General Data Protection Regulation ("GDPR").

Personal data is defined as any information relating to an individual that can be directly or indirectly identified. The main purpose of the TripAdmin is to manage vessel activities in high risk areas, and there is only a minimum of personal data processed by the system (email and IP address of users).

The TripAdmin application is hosted on DigitalOcean datacenters in Amsterdam, Netherlands, which are certified and audited according to GDPR.

4. Development and change management process

The development process for our SaaS platform follows an agile methodology and is based on the following principles:

- Privacy by design for software changes
- Security requirements are documented as part of development process
- Software changes are subject to change control procedures
- Only authorized individuals are permitted to deploy software changes

5. Responsibilities

Security and compliant data management is the responsibility of all employees and contractors of Osprey involved in the development, management, deployment or maintenance of the TripAdmin.

The ultimate responsibility resides with the Board of Directors and Executive Management of Osprey. This responsibility cascades down through a series of designated roles who define and manage the TripAdmin roadmap, development and change management process.

All contracts with external contractors that allow access to system must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

Version	Policy Owner	Effective Date	Last revised
1.1	Osprey Solutions (Analytics) AS	1.2.2021	1.10.2020