Veson Nautical LLC Hosted System Outline and Boundaries

Outline of System

Veson's services and features are provided by a set of services running in Amazon Web Services, currently hosted in data centers in three independent regions: Northern Virginia (*us-east-1*), Ireland (*eu-west-1*) and Singapore (*ap-southeast-1*). AWS regions are designed to be completely isolated from other regions to achieve the greatest possible fault tolerance and stability.

The processes and controls managed by Amazon Web Services, as part of their "Shared Responsibility Model", are not elaborated in this document but are available at the AWS Compliance Internet website.

Application node types include, but are not limited to, authentication; Veslink Voyage Reporting; Veslink API; Veslink IMOS Platform web session proxies; and Veslink IMOS Platform user session hosts.

Infrastructure

Infrastructure associated with Veson's client-facing system varies depending on the specific offerings as determined in the Client Agreement; user-initiated connections are available using IPv4 addresses via TCP ports 443 (HTTPS), 80 (HTTP) or 229 (VXP). (VXP is a Veson-developed extension of TCP that adds publish and subscription notification functionality, and is used to provide Veslink Voyage Reporting.)

All unencrypted HTTP connections are redirected to an equivalent HTTPS endpoint where applicable, otherwise HTTP connections are blocked. For clients whose networks restrict outbound connections to port 229, VXP connectivity is also available and encouraged over port 443 via the Websockets protocol.

Within the Veson-designed Virtual Private Cloud (VPC), client-specific data is stored in relational databases (currently Microsoft SQL Server) that are hosted on Amazon EC2 instances whose internal access is limited to application nodes and management servers. Confidential client data is segregated into isolated databases, and further logical barriers are enforced by the system. Data may also be stored in ephemeral cache services, such as Elasticsearch; such data is subject to logical access barriers enforced by the system.

User-initiated requests accessing the system using a web browser via HTTPS, excepting "Veslink Voyage Reporting" and "Veslink API" functionality, will be distributed amongst application nodes based on the client's operational database region. These requests are proxied, as necessary and via Amazon Web Services maintained load balancer(s), to a cluster of stateful application nodes. If a load balancer is present, TLS/SSL is terminated at this tier, and subsequent internal traffic is protected by the isolation provided by the Amazon VPC services and hypervisor.

User-initiated requests accessing the system using a remote access client (e.g., “IMOSlive”) are currently handled by a client-dedicated instance hosted in Amazon EC2, using Remote Desktop Protocol (RDP) tunneled using an HTTPS channel on TCP port 443.

User requests may be redirected to Amazon S3 for content uploads or routed through external third-party services such as CloudFlare to improve connectivity.

Users can configure the system to send notifications to third-party systems and providers. Traffic initiated from the system in such a manner originates from consistent IP addresses within the Veson-managed AWS accounts (e.g., IP addresses assigned to long-running instances and/or IP addresses assigned to AWS Network Address Translation egress-only Gateways).

Boundaries and Responsibility Model

While Veson is responsible for the security in the cloud and AWS is responsible for the security of the cloud, the client is responsible for application security and the data uploaded into any of Veson’s SaaS solutions.

Veson is responsible for:

- Server-side encryption, dependent on client offering(s)
- Endpoint and network traffic protection
- Backups of operational client databases and other system functionality
- Operating system and application maintenance on Veson-managed server instances

Clients are responsible for:

- Applying logical access security controls within the system, including:
  - User account management
  - Logical role and permission models
  - User role assignment
- Security of third-party integrations with the Veson system
- Data classification within the system, including which data should be shared with other clients

For further details on client responsibilities, see the Veson Nautical Website Terms and Conditions document available on the public Veson website.