CYBER. STATEMENT. SEATRADE.

This Cyber Security Statement ("Statement") is applied by the Seatrade Group of companies. Seatrade deems it important that its Suppliers provide a solid service to the vessels owned and or managed by Seatrade. Amongst others, it is of utmost importance that the risk of any cyber security breach is prevented. By means of this Statement, the Seatrade Group implements part of its program to prevent Cyber Security Incidents.

In this Statement the following terms shall mean:

"Cyber Security Incident" is the loss or unauthorised destruction, alteration, disclosure of, access to, or control of a Digital Environment.

"Digital Environment" are Seatrade's information technology systems, operational technology systems, network, internet-enabled applications or devices and the data contained within such systems, technology systems controlling hardware such as engines and other devises controlled by information technology used to operate and control ships.

"Service Provider": shall mean the party which is providing delivering products and/or rendering services to Seatrade.

"Seatrade" shall mean any company falling under the Seatrade Group of Companies, such as but not liminted to: Seatrade Group N.V., Seatrade Groningen B.V., Seatrade Shipmanagement B.V. and/or any of the Vessels which they have in management to which the Service Provider is rendering services or deliverring products.

Cyber Security Incident prevention:

I) When delivering products and/or rendering services to Seatrade, the Service Provider is to make sure that its products and or services and any devices used by Service Provider to deliver such products or render such services, shall be free from malware, bugs, virusses and any other potential defects which could result into a Cyber Security Incident on board of one of Seatrade's vessels or to Seatrade's systems used ashore.

II) The Service Provider shall at al times have the appropriate systems and procedures in place to avoid any potential Cyber Security Incident and will maintain such systems during the lifespan of the products delivered and or for the duration of the services rendered to Seatrade.

III) Prior to delivering products or rendering services to Seatrade, Service Provider will make sure that the working area where such products are to be delivered or services to be rendered is safe. This safety check includes a torough investigation of the technology systems which Seatrade is using, this to avoid that the systems of Seatrade will cause any harm to the systems or devices of Service Provider.

IV) Should the Service Provider become aware of a breach of any of its systems which could harm the Digitial Environment of Seatrade, it will immediately inform Seatrade of such event and will render all necessary cooperation and assitance so that a Cyber Security Incident can be avoided or rectified.

Cyber Security Incident rectification

I) Should a Cyber Security Incident have occurred, the Service Provider shall promptly render all necessary assistance and cooperation to rectify same.

II) The Service Provider is to reimburse Seatrade for any and all of its losses connected with or caused by the Cyber Security Incident, unless those losses have been proven to have been caused by Seatrade's own negligence.