CYBERSECURITY BASELINE EXPECTATIONS FOR SUPPLIERS

DeepOcean is committed to protecting its employees, partners, suppliers and operations from cybersecurity threats. As part of this commitment, we aim to establish a secure environment across our entire supply chain, ensuring the confidentiality, integrity, and availability of information shared with suppliers.

By complying with these expectations, suppliers play a crucial role in enhancing our collective resilience, protecting mutual interests, and maintaining the trust and confidence of all stakeholders. These cybersecurity expectations are an integral part of the agreement between DeepOcean and its suppliers for the provision of goods or services. Additional obligations may apply, as determined through audits conducted by DeepOcean.

1. General Expectations

DeepOcean expects suppliers to apply their own internal cybersecurity frameworks such as policies, systems, and procedures, provided these meets or exceed DeepOcean's cybersecurity standards. If a supplier's framework does not meet these standards, it must be adjusted to ensure full compliance.

Additionally, suppliers performing work at DeepOcean sites or aboard vessels must follow all relevant DeepOcean guidelines and procedures.

1.1. Definitions

- **DeepOcean Information/Data**: Any information shared by DeepOcean with the supplier, including but not limited to personal data and proprietary data.
- **HSE**: Health, Safety, Security, Social Responsibility, and Environment.
- **Site**: The location where work is being performed.
- **Sub-suppliers**: Any third parties performing part of the work for the supplier, including all levels in the supply chain.

1.2. Cybersecurity Management System

Suppliers must have or demonstrate compliance with a cybersecurity management system aligned with internationally recognized standards, covering all activities relevant to the contract's execution.

At a minimum, this system must include:

1. **Risk and Vulnerability Management**: Identification, assessment, treatment, and reporting of risks and vulnerabilities, with timely remediation aligned with global best practices.

2. **Protective Controls**: Measures to secure systems and information used by both the supplier and DeepOcean.
3. **Incident Response**: Preparedness for cybersecurity incidents, recovery and reporting.
4. **Holistic Security**: Comprehensive protection across people, processes and technology.
5. **Human and Third-Party Risks**: Management of actions by supplier personnel, sub-suppliers, or third parties that could harm DeepOcean's operations, personnel, or reputation.

To demonstrate compliance, suppliers may present certification or alignment with recognized standards given in Section 1.6.

1.3. Continuous Improvement

DeepOcean reserves the right to review the supplier's cybersecurity activities periodically to ensure compliance. These expectations may be updated in response to evolving cybersecurity threats or incidents.

Suppliers are responsible for continuously assessing and addressing cybersecurity risks in their operations and within their role as a supplier to DeepOcean. If risks are identified, the supplier must adjust its controls accordingly.

The supplier must also manage DeepOcean's information in accordance with DeepOcean's sensitivity classifications and implement additional safeguards as required.

1.4. Information Management

Any platforms used for exchanging information must prevent unauthorized access, loss, or exposure. Upon request or at the end of the contract, the supplier must return all DeepOcean information or securely destroy it and provide certificates of destruction.

If required by legal or regulatory obligations, the supplier must retain and protect DeepOcean information for the mandated period before securely destroying it.

1.5. Personnel Management

Access to DeepOcean information granted to supplier personnel or sub-suppliers must follow DeepOcean's procedures. The supplier must verify the identity and qualifications of all personnel involved in compliance with applicable laws.

The supplier must designate a point of contact for cybersecurity communications and ensure sub-suppliers do the same. Additionally, the supplier is responsible for ensuring all personnel receive required cybersecurity training.

1.6. Cybersecurity Compliance

Suppliers must provide evidence of compliance with recognized cybersecurity standards upon request. Acceptable evidence includes valid certificates or documented assessments.

Relevant standards include, but are not limited to:

- ISO/IEC 27001
- Cyber Essentials
- NIST CSF
- ISF Standard of Good Practice

The latest versions of these standards should be referenced, and any provided certifications must be valid with clear expiration dates.

2. Data Breach & Incident Notification

In the event of a data breach or cybersecurity incident that affects the supplier's ability to fulfill the contract, the supplier must notify DeepOcean within 48 hours of identification. Where legal or regulatory obligations apply, the supplier must notify DeepOcean and relevant authorities within the prescribed timeframes.

Notifications must be made through the agreed channels or by contacting the DeepOcean IT Duty Phone at +47 52 70 04 40. Notifications should include the responsible DeepOcean representative's name and sufficient information to enable DeepOcean to meet reporting obligations.

The supplier must fully cooperate with DeepOcean and take necessary actions to support investigation, containment, and resolution.

2.1. Emergency Situations and Serious Incidents

The supplier must maintain an emergency response organization as outlined in the agreement and must not disclose information regarding DeepOcean's assets or data to the media, external parties, or unauthorized individuals without DeepOcean's prior written consent.

3. Audit and Verification Activities

DeepOcean reserves the right to conduct cybersecurity audits and verifications of the supplier, its sub-suppliers, and related third parties during the contract's term. These audits do not relieve the supplier of its responsibility to meet contractual obligations.

Following any audit, the supplier must submit an action plan to address the findings. All issues must be resolved with corrective actions, and resolution must be documented to DeepOcean's satisfaction.