ONE NET LIMITED

Service Level Agreement

Connectivity, IT & Cybersecurity Services

CONTENT SUMMARY

PART I: GENERAL PROVISIONS

1. Definitions

Terms not defined in this SLA have the meaning given in the One Net Standard Terms & Conditions. Unless otherwise expressly defined in this Agreement, any capitalized term or abbreviation used in this Agreement shall have the meaning attributed to it in the Terms & Conditions. In case of conflict, the Terms & Conditions prevail.

"Agent Software" means the system platform tools provided by One Net for the purpose of the Sentrify Service.

"Change" means a request to modify configuration, policy, or system settings.

"Critical Ticket" means a ticket type for a complete service outage, security incident, or issue with potential safety or significant commercial impact.

"Direct Support" means a support plan under which vessel crew and customer ICT personnel may contact One Net directly.

"Extended Support Hours" means Monday to Friday, 05:30 to 19:00 UTC.

"First Response" means the acknowledgement of a support ticket with confirmation of the next steps to be taken.

"Force Majeure" means events beyond the reasonable control of either party, including natural disasters, war, terrorism, and pandemics, as described in Clause 53 of the Term & Conditions.

"High Ticket" means a ticket type for significantly degraded service, multiple users affected, or major business impact.

"Incident Response Team (IRT)" means a specialised group of cybersecurity professionals designated to handle and manage security incidents, working in coordination with the SOC.

"Indirect Support" means a support plan under which vessel crew contacts the customer's ICT function, which in turn contacts One Net.

"Low Ticket" means a ticket type for system modifications, software updates, and third-party application changes.

"Normal Ticket" means a ticket type for degraded service affecting a single user, or a non-critical service where a workaround is available.

"On-Hold Time" means a period during which a support ticket cannot be progressed by One Net because it is awaiting customer feedback, information, or remote hands-on assistance. On-Hold Time is excluded from the measurement of First Response and response-time targets.

"Outage" means complete loss of service or functionality, as measured exclusively by One Net's monitoring systems.

"Resolution" means the point at which an issue has been resolved and normal service restored, or an agreed workaround has been implemented.

"Security Operations Center (SOC) / SOC Team" means a centralised team responsible for continuously monitoring, detecting, analysing, and responding to cybersecurity incidents on a 24/7 basis.

"Sentrify Managed" means the monitored and managed Sentrify plan under which One Net's SOC and IRT monitor and respond to cybersecurity incidents on the customer's behalf.

"Sentrify Self-Managed" means the Sentrify plan under which the customer's own team operates the service, with One Net providing the Agent Software platform and tiered support on escalation.

"Support Hours" means Monday to Friday, 05:30 to 17:00 UTC.

"Tier 1" means Customer Support: first-line troubleshooting, known issues, standard procedures, standard requests, and emergency hardware bypass for connectivity. Available 24/7.

"Tier 2" means Advanced Support: complex diagnostics, critical incidents, and vendor coordination. Available during Extended Support Hours.

"Tier 3" means Systems Administration: backend administration, IT policy, patch compliance, platform engineering, and change requests. Available during Support Hours.

2. Purpose & Scope

This Service Level Agreement (SLA) defines the support framework between One Net and its customers for the following services:

- Connectivity: VSAT, LTE, LEO
- abela IT: Toolkit, Tier 2 Support, Fully Managed
- Sentrify cybersecurity: Managed and Self-Managed

Technical Account Management and Professional Services agreements are not covered by this SLA.

This SLA applies to all vessels and shore-side contacts under active service agreements with One Net. It is subject to the One Net Standard Terms & Conditions.

3. Contact Methods

One Net's support channels are available 24/7, 365 days per year. Who may use each channel under the Connectivity & IT support plans is set out in Clause 6.

Contact Method	Availability	Applies To
Email: support@onenet.group	24/7	All services
Phone: +357 25 828999	24/7	All services
abela Pulse Instant Messaging	24/7	Connectivity & IT (vessel)
abela Pulse Direct Ticketing	24/7	Connectivity & IT (vessel)

4. Response Times

Response times are based on ticket type, not customer-assigned priority. Ticket types are defined in Clause 1. All tickets are logged and tracked in One Net's helpdesk system. First Response is measured from the moment a report is delivered to One Net's support mailbox or ticketing system; On-Hold Time is excluded from response-time measurement. Service-specific First Response targets are set out in Clause 7 (Connectivity & IT) and Clause 13 (Sentrify).

4.1 Resolution Commitment

Due to the nature of maritime IT and dependencies on third-party providers (satellite, ISP, hardware vendors), One Net does not commit to fixed resolution times. One Net commits to:

- Working all issues to resolution as quickly as possible
- Prioritising based on severity and business impact
- Providing regular status updates during active incidents
- Coordinating with third-party vendors on the customer's behalf

5. Customer Responsibilities — All Customers

- Provide and maintain accurate contact information for authorised support contacts
- Designate authorised persons for change request approval
- Respond to One Net requests for information within reasonable timeframes
- Provide remote access to systems when requested for troubleshooting
- Subscribe to service notifications at status.onenet.group
- Report incidents promptly to minimise service impact

PART II: CONNECTIVITY & IT

6. Support Plans

Support is assigned per vessel. A vessel has one support plan regardless of how many One Net services are installed.

6.1 Direct Support

Vessel crew and customer ICT can contact One Net directly.

Who can contact One Net:

- Vessel crew (Captain, officers, authorised users)
- Customer's shore-based ICT team

6.2 Indirect Support

Customer ICT contacts One Net. Vessel crew contacts customer ICT.

Who can contact One Net:

- Customer's shore-based ICT team

Vessel crew contact path:

- Crew contacts customer's in-house ICT/helpdesk
- Customer ICT triages and resolves where possible
- Customer ICT escalates to One Net when required

7. Response Targets — Connectivity & IT

First Response targets for Connectivity & IT services, measured in accordance with Clause 4:

Ticket Type	First Response
Critical (P1)	2 hours
High (P2)	4 hours
Normal (P3)	8 hours
Low (P4)	8 hours (Support Hours)
Change	8 hours (Support Hours)

8. Support Tiers

The scope and availability of each tier are defined in Clause 1 (Tier 1, Tier 2, Tier 3). The table below summarises tier availability.

Tier	Team	Availability
Tier 1	Customer Support	24/7 / 365
Tier 2	Advanced Support	Mon–Fri 05:30–19:00 UTC (Extended Support Hours)
Tier 3	Systems Administration	Mon–Fri 05:30–17:00 UTC (Support Hours)

8.1 Escalation

Tier 1 handles all incoming contacts and resolves where possible. Issues are escalated as follows:

- Tier 1 → Tier 2: Advanced troubleshooting, critical incidents, vendor coordination
- Tier 2 → Tier 3: Change requests, backend administration, platform-level issues
- Tier 3 → Management: Unresolved Critical (P1) incidents or issues requiring executive decision

8.2 Third-Party Coordination

Where issues involve third-party providers (satellite operators, ISPs, hardware vendors), One Net acts as the single point of contact on the customer's behalf. Vendor response times are outside One Net's control and are excluded from SLA measurement.

9. Availability Targets — Connectivity & IT

Availability is measured in accordance with Clause 16. The following monthly targets apply to Connectivity & IT services:

Service	Target Availability	Notes
abela Fully Managed	99.5% per month	Measured by One Net monitoring
abela Tier 2 Support	99.0% per month	Measured by One Net monitoring
abela Toolkit (Portal)	99.0% per month	Measured by One Net monitoring
Connectivity (VSAT/LTE/LEO)	Best endeavours	Third-party dependent — excluded from availability targets

10. Customer Responsibilities — Connectivity & IT

10.1 Direct Support Customers

- Ensure all authorised vessel contacts are aware of One Net's contact methods
- Provide accurate vessel name, location, and system details when raising tickets
- To avoid service disruption, contact One Net before making any changes to network equipment or configurations

10.2 Indirect Support Customers

- Operate a functional in-house ICT helpdesk or first-line support function
- Perform first-line triage before escalating to One Net
- Act as communication relay between One Net and vessel crew when required
- Provide One Net with relevant diagnostic information gathered during triage
- Ensure crew are aware of the correct escalation path through customer ICT

PART III: SENTRIFY

11. Sentrify Service Model

Sentrify is One Net's maritime cybersecurity service, delivered on a Managed Security or EndPoint Security basis as specified in the customer's Offer.

11.1 Managed Security

Security Operations Center (SOC) continuously monitors, detects, and analyses cybersecurity events on a 24/7 basis, and the Incident Response Team (IRT) investigates threats, contains breaches, mitigates damage, and implements corrective actions. One Net provides Customer Support to the customer's fleet.

11.2 EndPoint Security

The customer's own security team operates the service. One Net provides the Agent Software platform and abela.io dashboard.

11.3 Scope & Shared Responsibility

Managed Security covers monitoring, detection, analysis, and incident response only. Unless the customer also subscribes to abela IT Fully Managed, the customer remains solely responsible for patching, configuration, hardening, access policy, and all preventive maintenance of in-scope systems. Outside active incident containment, One Net has no obligation or authority to apply updates or to change system or policy configuration. Customers who wish One Net to assume these preventive responsibilities should subscribe to abela IT Fully Managed.

11.4 Service Limitations

Managed Security reduces risk but does not guarantee that every threat will be detected or prevented, particularly on systems One Net does not manage. Warranty terms are set out in the One Net Standard Terms and Conditions of Sale.

12. Alert Handling & Escalation

This clause applies to the Managed Security plan only. Under EndPoint Security, alert handling and escalation are performed by the customer's own security team. For Managed Security, Sentrify alerts reach One Net through two paths: standard, non-security tickets follow the tier structure in Clause 1; cybersecurity alerts follow the paths below. In both paths the SOC takes ownership of the investigation and maintains communication with the vessel.

12.1 Vessel-Initiated Alert

- The vessel contacts ONG Support Tier 1 (24/7) by phone or email (support@onenet.group).
- Tier 1 categorises the issue as cybersecurity and assigns it to the SOC.
- The SOC takes ownership, maintains vessel communication, and begins the investigation.

12.2 SOC-Generated Alert

- The SOC detects a potential threat from vessel monitoring systems and raises a ticket.
- The ticket is assigned to the SOC.
- The SOC reviews its findings, takes ownership, and begins the threat investigation, notifying the vessel.

12.3 Escalation

When the SOC takes ownership of a security incident, a two-hour escalation timer starts. If the incident is not contained or resolved within that window, or where it constitutes a major incident, it is escalated to the Incident Response Team (IRT), which is available on-call. Matters requiring executive decision are escalated to management.

13. Response Targets — Sentrify

First Response targets for Sentrify, measured in accordance with Clause 4. These targets apply to the Managed Security plan only. Under EndPoint Security, incident detection and response are handled by the customer's own security team, and these targets do not apply.

Ticket Type	First Response
Critical (P1)	30 Minutes
High (P2)	2 hours
Normal (P3)	12 hours
Low (P4)	12 hours
Change	8 hours (Support Hours)

Custom subscription response times, where agreed, are specified in the customer's Offer.

13.1 Incident Handling

One Net begins remediation by phone and email. Where an incident cannot be resolved remotely, One Net coordinates a technician to attend the vessel; onboard work is carried out by One Net or an approved partner.

14. Customer Responsibilities — Sentrify

- Ensure the Agent Software is installed and maintained on in-scope systems
- Ensure only authorised users have access to systems and Equipment
- Provide One Net with the access required for security monitoring and incident response
- Comply with One Net directives to modify, vary, or shut down a service where required to contain an incident
- For Self-Managed customers, operate a functional in-house security function and perform first-line triage before escalating to One Net

PART IV: COMMON TERMS

15. Customer Delay and Directive Non-Compliance

Where One Net issues a remediation, containment, or troubleshooting directive, or requests information or access, and the customer does not act within the timeframe reasonably specified, the affected period counts as On-Hold Time and One Net's First Response and escalation commitments for that incident are suspended for its duration. This applies to all services under this SLA.

16. Availability Measurement

Service availability is measured monthly as the percentage of contracted service time the service is operational. For Connectivity & IT services this is measured by One Net's monitoring systems; for Sentrify it is measured by the Agent Software. One Net's measurement is the sole measurement tool. Service-specific targets are set out in Clause 9.

The following are excluded from downtime calculations:

- Scheduled and emergency maintenance windows
- Force majeure events
- Third-party satellite or ISP provider outages
- Customer-caused outages or unauthorised changes

17. Maintenance

One Net performs scheduled maintenance to ensure system reliability and security. All maintenance is published at status.onenet.group. Customers are responsible for subscribing to receive notifications.

Type	Notice Period	SLA Impact
Planned maintenance	Minimum 5 business days	Excluded from downtime
Critical security patches	Minimum 24 hours	Excluded from downtime
Emergency maintenance	Best effort notification	Excluded from downtime

18. Exclusions

This SLA does not cover:

Exclusion	Description
Force majeure	Natural disasters, war, terrorism, pandemics, or events beyond either party's reasonable control
Third-party failures	Outages or degraded performance from satellite providers, ISPs, or other third-party vendors
Unsupported systems	Hardware or software not supplied or managed by One Net, or systems at end-of-life
Unauthorised changes	Modifications to systems or configurations made without One Net approval
Customer negligence	Failure to apply security updates, sharing credentials, or disregarding One Net recommendations
Physical hardware	Repairs requiring physical access onboard — remote diagnostic support is available
Scheduled maintenance	Pre-notified maintenance windows per Clause 17
Data loss	Data backup and recovery unless explicitly contracted
Connectivity services	VSAT, LTE, and LEO — performance depends on third-party satellite and ISP providers
Unprotected or inaccessible systems	Incidents on systems lacking installed and current Agent Software, or where the customer has not provided the access One Net requires, are outside Managed Security scope and excluded from all response targets.

19. Service Credits

Service credits are governed by the One Net Standard Terms & Conditions: abela IT services under Clause 15, Sentrify under Clause 24, and Connectivity under Clause 28. The availability targets in this SLA are service targets and do not themselves create a credit entitlement.

20. Review

One Net may review this SLA periodically. The stated Review Date is administrative only and does not cause this SLA to expire, renew or change automatically.

One Net may update this SLA on written notice to reflect changes in service delivery, technology, suppliers, security requirements, applicable law or operational processes. Administrative, clarifying or non-material changes may take effect on the date specified in the notice.

A change that materially reduces the contracted service levels will take effect on not less than thirty (30) days' notice, unless the change is reasonably required sooner by law, a regulator, an urgent security risk, a third-party supplier or circumstances beyond One Net's reasonable control.

Continued use of the affected service after the effective date constitutes acceptance of the updated SLA to the extent permitted by applicable law and the Terms & Conditions. If the Terms & Conditions provide a specific variation or termination procedure, that procedure prevails.

A Customer request to review this SLA does not require One Net to agree to any amendment. No amendment proposed by a Customer is effective unless expressly accepted in writing by an authorised representative of One Net.

Service levels applicable to a particular Customer may be varied only in the Customer's Offer or a written amendment that expressly identifies the provision being varied.