Coro Cybersecurity Support Service Level Agreement (SLA)

This is a Service Level Agreement (SLA) ("Agreement") between Coronet Cyber Security Ltd. ("Coro") and the individual or legal entity (hereinafter referred to as "You" or "Your"), outlining the services and commitments regarding technical support for the purchased Coro Cybersecurity products.

1. **Definitions**:

- "**Coro Cybersecurity**" refers to Coro, the party to this Agreement with the customer to whom a service form is issued under this Agreement.
- "**Level 1 Support**" means providing general pre- and post-sales product information, software configuration, collecting relevant technical problem identification information, performing base problem determination, providing basic support on the standard products, protocols, and features.
- "**Level 2 Support**" means providing Level 1 Support and the ability to resolve most misconfigurations, troubleshoot complex configuration and software problems, support problem isolation and determination of product specification defects, provide lab simulation and interoperability and compatibility testing for new software releases before being deployed into a customer production network, define an action plan, provide advanced support on all products, protocols and features, and analyze traces and diagnose problems remotely.
- "**Level 3 Support**" means providing Level 1 Support and Level 2 Support and the ability to provide software enhancements such as patches and hotfixes, fixing or generating workarounds that address software bugs, and troubleshooting bugs that were not diagnosed during Level 2 Support.
- "**Problem Resolution**" means the use of reasonable commercial efforts to resolve the reported problem, which may include (but are not limited to) configuration changes, patches that fix an issue, reinstalling the software, etc.
- "**Respond**" means addressing the initial request and taking ownership of the issue.
- "**Response Time**" means the time elapsed between the initial contact by the customer to Coro Cybersecurity support and the returned response to the customer by Coro Cybersecurity staff.
- "**Service Level Agreement (SLA)**" means the customer Service Level Agreement (SLA) that identifies the features and defines the processes involved with the delivery by Coro Cybersecurity of support functions to the customer, as presented by this document.
- "**Support**" means the technical support provided by Coro Cybersecurity directly to the customer as set forth in this Agreement.

2. **Coro Cybersecurity Support Obligations**:

2.1. Customers will be entitled to receive support according to the features and benefits provided under the applicable offering, subject to the terms and conditions of this Agreement. For customers covered under Coro Cybersecurity support offering, technical support will be provided pursuant to the terms of Section 4 (Technical Support), which includes providing access to product update releases, related documentation, and knowledge articles upon general commercial release, and access to support representatives who will work with the customer to diagnose issues and provide Problem Resolutions, including escalating the issue through Level 2 Support.

2.2. **Exclusions**:

The service commitment under this Agreement does not apply to any unavailability, suspension, performance issue or termination of the Coro Cybersecurity service caused by factors outside of Coro Cybersecurity's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of the Coro Cybersecurity service that result from any actions or inactions of the customer or any third party, that result from customer equipment, software, or other technology and/or third party equipment, software, or other technology (other than third-party equipment within Coro Cybersecurity's direct control), or arising from the suspension or termination of customer right to use the Coro Cybersecurity service.

3. **Designated Contacts**:

The customer agrees that contact with Coro Cybersecurity will be through the specified number of designated contacts. The customer is responsible for specifying and updating valid designated contacts in the Coro Cybersecurity control panel within admin users. The customer agrees that access to any Support deliverable, software subscription downloads and workspace will be through their registered designated contacts only.

4. **Technical Support**:

4.1. Web-based Support. Coro Cybersecurity web-based support available at URL: https://support. https://support.coro.net provides the customer access to:

(a) **Documentation**, containing product documentation, release notes, technical white papers about Coro Cybersecurity products, as releases become generally commercially available.

(b) **Agent Downloads**, the latest version of the agent software can be obtained through the control panel of the Coro Cybersecurity platform. The updated version can be accessed by navigating to the "Endpoint Devices" section and selecting "Agent Deployment." The downloading and installation of the latest version of the agent software shall be the responsibility of the customer.

Availability and accessibility of Support is in accordance with the specifications of this Agreement, subject to Section 2.2 above.

	Level 1	**Level 2**	**Level 3**
Support Availability For First Response	Up to 1 Hour (Business Hours)	Up to 2 Business Days	Up to 3 Business Days

4.2. **Technical Support Procedures**:

Coro Cybersecurity uses a multi-tier support model for problem resolution. When a customer makes initial contact with support, a technical representative or web service request tool will validate customer and contract information, workspace id, and gather details relevant to the issue. A unique ticket number will be assigned and delivered to the customer's designated contact via web request or email. This ticket number will be used to track the issue from initial contact to final problem resolution. If appropriate and technically possible, the issue will be reproduced in Coro Cybersecurity. Further investigation, including additional troubleshooting or debugging activity, may be required. Based on the investigation results, the issue may be resolved, or, if an anomaly is identified, elevated to the appropriate Coro Cybersecurity team for final problem resolution.

Coro Cybersecurity agrees to work with the customer to resolve an issue in accordance with the specifications of this Agreement using commercially reasonable efforts. If communication from the customer ceases without notice, Coro Cybersecurity may, upon notice, close a ticket due to inactivity on the part of the customer. A ticket may be reopened within ten (10) consecutive days of closure. Once a ticket is closed for ten (10) consecutive days, this issue will be considered permanently closed, and it cannot be reopened. If further work is necessary, a new ticket will be opened, and all pertinent materials may need to be resubmitted before work can continue.

4.3. **Escalation Process and Procedure**:

(a) Customer-initiated Escalation: When work items (especially those associated with critical situations) need to be expedited, the customer shall notify Coro Cybersecurity of the critical situation. If the support representative determines that sufficient information has been provided by the customer and the escalation is accepted, Coro Cybersecurity will work with the customer on providing the appropriate solution. The escalation begins in accordance with Coro Cybersecurity standard business practices. Upon request, Coro Cybersecurity may provide an action plan to the customer that may include (but is not limited to) the problem statement, next action items to resolve the issue, and time estimates on these action items.

(b) Coro Cybersecurity Internal Escalation Process: When a support representative determines that an issue needs internal escalation, the issue receives increasing levels of engineering expertise and managerial attention in accordance with Coro Cybersecurity standard business practices, except for the case of a customer-initiated escalation.

(c) Management Escalation: If an issue is not being resolved, or if it requires managerial attention, the customer can request the support representative to connect with the support manager, or contact the support manager directly using the contact information provided at the bottom of the ticket email. Regardless of the elapsed time of the outstanding ticket, escalation should be initiated at the support representative level, and then escalated to the support manager.