



This Security as a Service by ALCiT Sub-Agreement (“Sub-Agreement”) is governed by the Master Service Agreement between ALCiT and CUSTOMER. This Sub-Agreement supersedes all prior discussions, communications, representations or agreements, including any digital, electronic or Internet-based agreements, between them, oral or written, between ALCiT and CUSTOMER concerning security as a service.

This Sub-Agreement shall consist of these terms:

1. **Activities:** ALCiT will ensure that the reports listed in Agreement are created and reviewed as per the table.

2. Process:

- (a) Each report will be automatically created by their originating system and forwarded to CUSTOMER’s service desk to create a ticket.
- (b) As per the specified frequency in the table below, the ticket will be opened and the report it contains will be reviewed by ALCiT.
- (c) If no action(s) is/are required, ALCiT will close the ticket with a comment stating that no action(s) were required.
- (d) If action(s) is/are required, ALCiT will add a note to the ticket summarize the required action(s). If said action(s) is/are covered by another service performed by ALCiT, ALCiT will perform the action(s), update the ticket and close it. If the action(s) is/are not covered by another service, the ticket will be assigned to CUSTOMER for execution.
- (e) ALCiT will review the events sent for analysis and filter out unnecessary events in an effort to reduce the EPS rate.

3. Schedule:

- (a) Daily reports are created every day
- (b) Weekly reports are created on Fridays
- (c) Monthly reports are created on the first day of the month or the first Business Day after the first of the month
- (d) Quarterly reports are created on the first day of the month or the first Business Day after the first of the month for the months of January, April, July and October
- (e) Semi-Annual reports are created on the first day of the month or the first Business Day after the first of the month for the months of January and July
- (f) Annual reports are created on the first day of the month or the first Business Day after the first of the month for the months of January

4. Cyber Security Incident Response:

- (a) ALCiT will respond to Cyber Security Incidents as per Service Details section below
- (b) Definitions:
 - i. **False Positive Suppression:** ALCiT will review alerts received from the platform and confirm the alert is a probable Cyber Security Incident.
 - ii. **Playbook or Scripted Responses:** ALCiT will leverage a pre-approved (jointly by ALCiT and Customer) playbook of actions to respond to the Cyber Security Incident.
 - iii. **Response via Infrastructure Management:** ALCiT will leverage the tools in the environment as per or in conjunction with the guidance of the Customer incident response team lead.
 - iv. **Digital forensic analysis:** A subset of forensic science that examines system data, user activity, and other pieces of digital evidence to determine if an attack is in progress and who may be behind the activity.
 - v. **Ransomware negotiations:** Engaging with the attacker in an effort to minimize or eliminate the ransom request.
 - vi. **Incident Commander:** The person responsible for all aspects of an emergency response; including quickly developing incident objectives, managing all incident operations, application of resources as well as responsibility for all persons involved.
 - vii. **Participation in war room:** Having ALCiT listen or participate in an ongoing war room and or/call about a Cyber Incidents.
 - viii. **Deep/dark web analysis:** Conduct reviews and/or investigations on the dark/deep web for insights on Cyber Security Incidents.
 - ix. **Cyber Security Incidents legal advice:** Provide legal advices in regards of a Cyber Security Incidents.
 - x. **Cyber Security Incidents public communications:** Create and/or execute communications with people outside the organization.
 - xi. **Incident recovery:** The effort and/or tools to recover from a Cyber Incident.

5. Service Details:

| Key | Label | Definition |
|----------|----------------------------|---|
| H | Help or Assist | The designated party (ALCiT / CUSTOMER) will provide assistance to enable the identified performing party (ALCiT / CUSTOMER) to complete the designated service. |
| P | Perform | The designated party (ALCiT / CUSTOMER) has the obligation and responsibility for performing the designated service. |
| A | Approve | The performance of the service is subject to the designated party's (ALCiT / CUSTOMER) written approval |
| V | Review | The designated party (ALCiT / CUSTOMER) will review the designated documents and provide feedback to the other party. |
| M | Make Available | Make the service or platform available to the designated party (ALCiT / CUSTOMER) |
| U | Use | The designated party (ALCiT / CUSTOMER) uses or leverage the service or platform. |
| ON | Ongoing | Service will be performed as required |
| D | Daily | Service will be performed once a day |
| W | Weekly | Service will be performed once a week |
| M | Monthly | Service will be performed once a month |
| Q | Quarterly | Service will be performed once a quarter |
| SN | Semi-Annually | Service will be performed twice a year |
| AN | Annually | Service will be performed once a year |
| AD | Ad Hoc | Service will be performed as requested |
| S | Semi-Annual | Service will be performed twice a year |
| I | Included | Included in unit price |
| TI | Ticket/IMAC | Work will be billed according to the Ticket and IMAC Rate Card |
| TR | Time and Material Regular | Work will be billed according to the Rate Card using the Regular rates. |
| TU | Time and Material Urgent | Work will be billed according to the Rate Card using the Urgent rates. |
| TC | Time and Material Critical | Work will be billed according to the Rate Card using the Critical rates. |
| TR/TU/TC | Time and Material | Regular work will be billed according to the Rate Card using the Regular Rates, Urgent work will be billed according to the Rate Card using the Urgent Rates and Critical work will be billed according to the Rate Card using the Critical Rates |
| OP | Optional | Additional cost as per Rate Card |



5.1 Essential Service (24/7)

| ID | Description | ALCiT | CUSTOMER | FREQUENCY | CHARGE |
|----|---|-------|----------|-----------|--------|
| 1 | Ensure that all the reports in the Daily section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | D | I |
| 2 | Ensure that all the reports in the Weekly section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | W | I |
| 3 | Ensure that all the reports in the Monthly section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | M | I |
| 4 | Ensure that all the reports in the Quarterly section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | Q | I |
| 5 | Ensure that all the reports in the Semi-Annually section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | SN | I |
| 6 | Ensure that all the reports in the Annually section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | AN | I |
| 7 | Review Daily Report service desk ticket(s) and add note validating review and next steps within one (1) Business Day. | P | | D | I |
| 8 | Review Weekly Report service desk ticket(s) and add note validating review and next steps within two (2) Business Day. | P | | W | I |
| 9 | Review Monthly Report service desk ticket(s) and add note validating review and next steps within three (3) Business Day. | P | | M | I |



| ID | Description | ALCiT | CUSTOMER | FREQUENCY | CHARGE |
|----|--|-------|----------|-----------|-------------------|
| 10 | Review Quarterly Report service desk ticket(s) and add note validating review and next steps within five (5) Business Day . | P | | Q | I |
| 11 | Review Semi Annual Report service desk ticket(s) and add note validating review and next steps within five (5) Business Day. | P | | SN | I |
| 12 | Review Annual Report service desk ticket(s) and add note validating review and next steps within ten (10) Business Day. | P | | AN | I |
| 13 | Investigate unusual activity | P | A | AD | TR/TU/TC |
| 14 | Remediate vulnerability.* | P | A | AD | TR/TU/TC |
| 15 | Document vulnerability. | P | A | AD | TR/TU/TC |
| 16 | Participate in meetings. | P | A | AD | TR/TU/TC |
| 17 | Fill third party cyber security questionnaires on behalf of Customer (the first three (3) per year). | P | A | AD | I (3 per Year) |
| 18 | Fill third party cyber security questionnaires on behalf of Customer (after the first three). | P | A | AD | TR |
| 19 | False Positive Suppression | P | | AD | I |
| 20 | Playbook or Scripted Responses | P | A | AD | TR/TU/TC |
| 21 | Response via Infrastructure Management* | P | A | AD | TR/TU/TC |
| 22 | Digital forensic analysis | | P | | N/A |
| 23 | Ransomware negotiations | | P | | N/A |
| 24 | Incident Commander | | P | | N/A |
| 25 | Participation in war room | P | A | AD | TR/TU/TC |
| 26 | Deep/dark web analysis | | P | | N/A |
| 27 | Cyber Security Incidents legal advice | | P | | N/A |
| 28 | Cyber Security Incidents public communications | | P | | N/A |
| 29 | Incident recovery | P | A | AD | TR/TU/TC |
| 30 | Tools required to create the in scope reports | M / U | | ON | I |
| 31 | Tools required to analyze logs | M / U | | ON | I |

* Customer may include this service through ALCiT Infrastructure Management services.



5.2 Core Service (24/7)

| ID | Description | ALCiT | CUSTOMER | FREQUENCY | CHARGE |
|----|---|-------|----------|-----------|--------|
| 1 | Ensure that all the reports in the Daily section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | D | I |
| 2 | Ensure that all the reports in the Weekly section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | W | I |
| 3 | Ensure that all the reports in the Monthly section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | M | I |
| 4 | Ensure that all the reports in the Quarterly section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | Q | I |
| 5 | Ensure that all the reports in the Semi-Annually section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | SN | I |
| 6 | Ensure that all the reports in the Annually section in the SECaaS Report Schedule are created and available for review in CUSTOMER's service desk. | P | | AN | I |
| 7 | Review Daily Report service desk ticket(s) and add note validating review and next steps within one (1) Business Day. | P | | D | I |
| 8 | Review Weekly Report service desk ticket(s) and add note validating review and next steps within two (2) Business Day. | P | | W | I |
| 9 | Review Monthly Report service desk ticket(s) and add note validating review and next steps within three (3) Business Day. | P | | M | I |



| ID | Description | ALCiT | CUSTOMER | FREQUENCY | CHARGE |
|----|--|-------|----------|-----------|-------------------|
| 10 | Review Quarterly Report service desk ticket(s) and add note validating review and next steps within five (5) Business Day . | P | | Q | I |
| 11 | Review Semi Annual Report service desk ticket(s) and add note validating review and next steps within five (5) Business Day. | P | | SN | I |
| 12 | Review Annual Report service desk ticket(s) and add note validating review and next steps within ten (10) Business Day. | P | | AN | I |
| 13 | Investigate unusual activity | P | A | AD | TR/TU/TC |
| 14 | Remediate vulnerability*. | P | A | AD | TR/TU/TC |
| 15 | Document vulnerability. | P | A | AD | TR/TU/TC |
| 16 | Participate in meetings. | P | A | AD | TR/TU/TC |
| 17 | Fill third party cyber security questionnaires on behalf of Customer (the first five (5) per year). | P | A | AD | I (5 per Year) |
| 18 | Fill third party cyber security questionnaires on behalf of Customer (after the first five). | P | A | AD | TR |
| 19 | False Positive Suppression | P | | AD | I |
| 20 | Playbook or Scripted Responses | P | | AD | I |
| 21 | Response via Infrastructure Management* | P | A | AD | TR/TU/TC |
| 22 | Digital forensic analysis | | P | | N/A |
| 23 | Ransomware negotiations | | P | | N/A |
| 24 | Incident Commander | | P | | N/A |
| 25 | Participation in war room | P | A | AD | TR/TU/TC |
| 26 | Deep/dark web analysis | | P | | N/A |
| 27 | Cyber Security Incidents legal advice | | P | | N/A |
| 28 | Cyber Security Incidents public communications | | P | | N/A |
| 29 | Incident recovery | P | A | AD | TR/TU/TC |
| 30 | Tools required to create the in scope reports | M / U | | ON | I |
| 31 | Tools required to analyze logs | M / U | | ON | I |

*Customer may include this service through ALCiT Infrastructure Management services.