Public

Terms of Service

Managed Services and Self-Managed Services

Last update: (see next page)
Owner: CEO
Author: Product Team

Classifications:
| Public: Okay to put on our website. **| Internal**: Elastisys use only.
| Confidential: As needed internally depending on working group **| Customer data:** Never shared

Last updated 2025-10-13.

Previous versions of the ToS are located at
https://github.com/elastisys/terms/commits/main/terms-of-service.md

Terms of Service

These Terms of Service set forth the terms between you ("**Customer**," "**you**," or "**your**") and Elastisys AB, org. no. 556873-6135, a company incorporated under the laws of Sweden, ("**Elastisys**," "**we**", or "**us**") and governs your access to and use of the Services, as defined below.

The terms are valid for the following Elastisys offers:

- **Managed Services**:
  - **Standard Plan**: Welkin and Additional Services, Managed by Elastisys 6-22
  - **Premium Plan**: Welkin and Additional Services, Managed by Elastisys 24/7
- **Enterprise Services**:
  - **Enterprise Plan**: Welkin and Additional Services, Managed by the Customer and Supported by Elastisys 8-17

The main part of these terms (clauses 1 to 20) applies to all offers. Each appendix applies to the Services specified in the title.

Links to external websites are for informational purposes only and are NOT incorporated by reference in these Terms of Service.

Unless otherwise specified, all times are stated in Central European Time (CET, UTC +01:00) or Central European Summer Time (CEST, UTC +02:00), as observed in Stockholm, Sweden.

1. Definitions

The following terms and expressions shall in this document, when capitalized, have the meanings assigned to them in this section.

APPLICABLE LEGISLATION means the GDPR and; any applicable supplementary legislation to the GDPR.

AUTHORIZED USER means Customer and Customer's employees, consultants, contractors, and agents (i) who are authorized by Customer to access and use the Services under the rights granted to Customer pursuant to the Agreement and (ii) for whom access to the Services has been purchased hereunder.

AGREEMENT means the Order, these Terms of Service (including all appendices), any Data Processing Agreement between the Customer and Elastisys, and any additional agreements, documents or terms which incorporate these Terms of Service by reference.

AUTOSCALING means a technical method to add or remove Nodes without human intervention either from the Customer's or Elastisys's side.

BUSINESS HOURS means the time between 8.00am to 17.00pm in the Europe/Stockholm timezone on working days. Working days are Monday to Friday except for:

- public holidays as defined in the Swedish Public Holidays Act (1989:253);
- Labour Day, which means May 1st;
- Midsummer's Eve (midsommarafton), which means the day before Midsummer's Day (midsommardagen);
- Christmas Eve (julafton), which means Dec 24th;
- New Year's Eve (nyårsafton), which means Dec 31st.

CHANGE ORDER refers to a written notification from the Customer to Elastisys to make changes in the Service(s), such as to change between Standard and Premium plan, etc.

CONTROLLER A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

CUSTOMER means the legal entity that has entered into the Agreement with Elastisys.

CUSTOMER APPLICATIONS refers to all of the Customer's application(s) which, from time to time, are deployed using the Services.

CUSTOMER DATA refers to all Data processed by the Customer Application inside an Environment. Examples include database definitions, data in databases, container images, messages in message queues, files on PersistentVolumeClaims, application logs. Platform-related Data, including alerts, platform audit logs, platform metrics are not Customer Data.

DATA means all the information, text drawings, diagrams, images or sounds (including and/or together with any databases made up of any of these) and other data which are embodied in any electronic, magnetic, optical or tangible media, and which:

- are owned by or relate to either Party's business;
- are supplied to one Party or on behalf of the other Party; or
- are generated, processed, stored or transmitted by a Party and/or a subcontractor, on behalf of the other Party pursuant to this Agreement.

DATA PROCESSING AGREEMENT INSTRUCTIONS means the written instructions from the Controller for how the Processor shall process the Personal Data. These instructions are provided in the Order.

DATA SUBJECT means a natural person whose personal data is processed.

DOCUMENTATION means Elastisys' user manuals, handbooks, and guides relating to the Services.

ELASTISYS IP means the Services, the Documentation, and all intellectual property provided to Customer or any other Authorized User in connection with the foregoing. For the avoidance of doubt, Elastisys IP does not include Data owned by the Customer.

ENVIRONMENT means one Welkin Service Instance, which might also include other Services as listed in the appendices to these Terms.

GDPR means Regulation (EU) 2016/679 of the European Parliament and the Council as amended, supplemented and/or varied from time to time.

INCIDENT levels are defined as follows:

- **CRITICAL INCIDENT**: Incidents that cause loss of service or continuous instability of mission-critical functionality and have no workaround. The

incident causes or may cause a material adverse effect on the Customer's business or material parts of the operational services are unavailable.
- **MAJOR INCIDENT**: Incidents that are impairing, but not causing loss of service or loss of mission-critical functionality. Intermittent issues that affect mission-critical functionality. The incident causes or may cause an adverse effect on the Customer's business or a critical function does not work, or work with response times that are inferior to the agreed-upon time.
- **MINOR INCIDENT**: All other incidents.

MANAGED SERVICES means delivery of Welkin and Additional Services operated by Elastisys. The Customer does NOT have administrative access to Environments. Managed Services are offered with two Plans: Standard Plan and Premium Plan.

NODE means a data plane (worker) Node in Kubernetes and may be either a virtual or a physical machine.

ORDER means the signed business contract between the Parties.

PARTIES refers to both Elastisys and the Customer, collectively.

PERSONAL DATA means the personal data as defined in Applicable Legislation.

PERSONAL DATA BREACH means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

PLAN means the combined uptime and support undertaking provided by Elastisys for one or more Environments as reflected in the Order. A Plan can either be a Standard Plan, Premium Plan or an Enterprise Plan.

PREVIEW FEATURE is a feature which is explicitly sold and marketed as "preview".

PROCESSOR means natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

PROFESSIONAL SERVICES means separately ordered consultancy services provided by Elastisys on hourly rates and basis.

SERVICE(S) means the Managed Service(s) or Enterprise Service(s) offered by Elastisys under the Agreement as described in the appendices to these Terms (including Welkin platform for running containerized applications and additional services).

SERVICE ENDPOINT(S) means the API or UI endpoints for the Service(s) made available to the Customer. The Service specific appendices set forth the Services Endpoints for each provided Service.

SERVICE FEE means the periodic fee for the Services (yearly or monthly) and the aggregated hourly fees for Professional Services, to be paid by the Customer to Elastisys.

SERVICE INSTANCE means one instance of a particular Service under a specific Plan. Customers may Order multiple Service Instances (for example multiple Welkin Service Instances). The Plan chosen for additional Services delivered in connection with one Welkin Service Instance (see appendices) must be the same as the associated Welkin Service Instance.

SERVICE RECIPIENT means a third-party company - other than the Customer - entitled to receive and use the Services.

SERVICE SIZE means a pre-defined Service package consisting of a pre-defined capacity -- e.g.CPU and memory -- of a Service Instance.

SERVICE START DATE means the date that the Services shall be available to the Customer and from which date Elastisys shall be entitled to charge the Service Fee. Service Start Date is specified in Order and if not, it shall be the date Elastisys announces that the Service is ready for use.

SUBPROCESSOR A natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the Processor, Processes Personal Data on behalf of the Controller.

SUPPORTED SERVICES means delivery of Welkin and Additional Services operated by the Customer. The Customer has administrative access to Environments. Elastisys supports the Customer with operations. Enterprise Services are offered with one Plans: Enterprise Plan.

TERMS means these Terms of Service with all appendices.

THIRD COUNTRY means a state that is not a member of the European Union (EU) or the European Economic Area (EEA).

2. Access and Use

2.1 Provision of Access

Subject to and conditioned on your payment of the Service Fee and compliance with the terms and conditions of the Agreement, Elastisys hereby grants you a revocable, non-exclusive, non-transferable,non-sublicensable, limited right to (i) access and use the Services during the Term and (ii) to use Documentation during the Term. Your use of the Services is at all times solely for your internal business operations by Authorized Users in accordance with the terms and conditions of the Agreement. Elastisys shall provide you with the necessary means of access to the Services.

2.2 Use Restrictions and Reservation of Rights

Customer shall not, and shall not permit any Authorized Users, to: (i) use the Services, (ii) use any software component of the Services, or (iii) use Documentation for any purposes beyond the scope of the access granted in the Agreement. Unless authorized in writing by Elastisys, Customer shall not at any time, directly or indirectly, permit any Authorized Users to: (i) copy, modify, or create derivative works of the Services, any software component of the Services, or Documentation, in whole or in part; (ii) rent, lease, lend, sell, license, sublicense, assign, distribute, publish, transfer, or otherwise make available the Services or Documentation except as expressly permitted; (iii) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of the Services, in whole or in part; (iv) remove any proprietary notices from the Services or Documentation; or (v) use the Services or Documentation in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person, or that violates any applicable law, regulation, or rule.

Elastisys reserves all rights not expressly granted to Customer. Except for the limited rights and licenses expressly granted under this Agreement, nothing in this Agreement grants, by implication, waiver, estoppel, or otherwise, to Customer or any third party, any intellectual property rights or other right, title, or interest in or to the Elastisys IP.

2.3 Suspension

Notwithstanding anything to the contrary in the Agreement, Elastisys may temporarily suspend Customer's and any other Authorized User's access to any portion or all of the Services if: (i) Elastisys reasonably determines that (A) there is a threat or attack on any of the Elastisys IP; (B) Customer's or any other Authorized User's use of the Elastisys IP disrupts or poses a security risk to the Elastisys IP or to any other customer or vendor of Elastisys; (C) Customer or any other Authorized User is using the Elastisys IP for fraudulent or illegal activities; (D) subject to applicable law, Customer has ceased to continue its business in the ordinary course, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding; or (E) Elastisys' provision of the Services to Customer or any other Authorized User is prohibited by applicable law; (ii) any vendor of Elastisys has suspended or terminated Elastisys' access to or use of any third-party services or products required to enable Customer to access the Services; or (iii) in accordance with Section 6 (Service Fees and Terms of Payment) (any such suspension described in subclause (i), (ii), or (iii), a "**Service Suspension**"). Elastisys shall use commercially reasonable efforts to provide written notice of any Service Suspension to Customer and to provide updates regarding resumption of access to the Services following any Service Suspension. Elastisys shall use commercially reasonable efforts to resume providing access to the Services as soon as reasonably possible after the event giving rise to the Services Suspension is cured. Elastisys will have no liability for any damage, liabilities, losses (including any loss of or profits), or any other consequences that Customer or any other Authorized User may incur as a result of a Service Suspension.

3. Service Levels and Support

3.1 Availability

For Managed Services, Elastisys is responsible for uptime (see A2.1.1 Availability).

For Enterprise Services, the Customer is responsible for uptime in consultation with Elastisys (see A5.4 Division of responsibility).

3.2 Ways of Contact

The Customer may contact Elastisys by opening a support ticket, or calling the Elastisys' support number. The Customer may initiate an unlimited number of support tickets. A support ticket may only be submitted to Elastisys via Elastisys designated support channels as instructed from time to time by Elastisys. The Customer should not enter any sensitive information in a written support ticket. If such information needs to be provided, it should be done over the phone. If the customer has a shared Slack channel with Elastisys, this contact path is to be used for informal communication only.

3.3 Change Order(s)

The Customer may only submit Change Order(s) via support tickets. The submission of a Change Order(s) shall constitute an offer to buy the Services or an upgrade thereof, as applicable. Elastisys may accept that offer at its sole discretion (at which time both Parties are legally bound) by way of (i) responding to the service ticket thereby acknowledging receipt and acceptance of the Change Order; and/or (ii) delivery of the Services. When submitting a Change Order, the Customer agrees and acknowledges that Customer will be, or continue to be, bound by these Terms.

3.4 Incident Levels and Response Time

Incident levels are defined in 1. Definitions.

The Customer commits to help expedite resolution of an incident by:

- keeping an open communication line during and until the incident is resolved; and
- providing evidence that the incident is truly critical or major.

Otherwise, Elastisys reserves the right to downgrade the incident's level. This is needed in order to minimize unnecessary overtime and comply with the Swedish Working Hours Act (1982:673).

For Managed Services, Elastisys responds as stipulated in A2.1.2 Response Time.

For Enterprise Services, Elastisys responds as stipulated in A5.2 Response Time.

3.5 Updates and Upgrades

For all offers, Elastisys is responsible for producing Service updates and upgrades. For Managed Services, Elastisys is responsible for applying updates and upgrades (see A2.6 Updates and Upgrades). For Enterprise Services, the Customer is responsible for applying updates and upgrades in consultation with Elastisys (see A5.4 Division of responsibility).

3.6 Vulnerability Management

Elastisys makes commercially reasonable efforts to ensure that the provided Services are free from security vulnerabilities which are either publicly known or known to Elastisys, and which can put Customer systems and Customer Data at risk, inter alia:

- **Prepare**: Elastisys prepares for vulnerability management as follows:
  - control what software components are added to software used by Elastisys;
  - ensure software components are provisioned from vendors which have demonstrated good vulnerability management;
  - ensure the Software Bill of Materials (SBOM) is up-to-date;
  - subscribe to security announcements issued by vendors of software components used by Elastisys;
  - setup Elastisys vulnerability disclosure channels; information on how to report a vulnerability to Elastisys can be found at https://github.com/elastisys/compliantkubernetes-apps/blob/main/SECURITY.md;
  - ensure via its CNCF membership that open-source projects are sufficiently funded for good vulnerability management; evidence that Elastisys is a CNCF member can be found at https://landscape.cncf.io/?item=cncf-members--silver--elastisys-member;
- **Detect**: Elastisys will detect vulnerabilities as follows:
  - monitor security announcements issued by vendors of software components used by Elastisys;
  - monitor Elastisys vulnerability disclosure channels;
- **Respond**: Elastisys will respond to vulnerabilities without undue delay by determining if a vulnerability will put Customer systems and Customer Data at risk; and if so:
  - release and apply countermeasures – such as firewall rules or disable functionality – so as to limit the impact of the vulnerability;

    - work with vendors to ensure timely release of security patches for software components with are part of the Service;
    - release security patches for software included in the Services;
    - for Managed Services apply security patches for the software included in the Services;
    - for Enterprise Service inform the customer and help them apply security patches for software included in the Services;
- **Recover**: Elastisys will recover from vulnerabilities as follows:
    - identify opportunities to reduce the likelihood or impact of future vulnerabilities

Illustrative Example: Third-party security researcher reports a vulnerability to a vendor

A typical sequence of events is:

1. A third-party security researcher reports a vulnerability to the vendor, via the vendor's security disclosure channels. For example, for a vulnerability found in Kubernetes, the communication between the security researcher and the vendor proceeds as written in the Kubernetes Security and Disclosure Information page, located at https://kubernetes.io/docs/reference/issues-security/security/.
2. The vendor releases a security patch and announces it via its security announcement channels. For example, for a vulnerability found in Kubernetes, an email is sent to the kubernetes-security-announce@googlegroups.com mailing list.
3. Elastisys becomes aware of the security patch via the vendor's security announcement channels, because Elastisys is subscribed to all security announcement channels of the relevant software components.
4. Elastisys incorporates the security patch into Welkin and releases a new version of Welkin.
5. Elastisys informs Enterprise Service Customers via Slack and/or email that a new security patch was released for Welkin.
6. The Enterprise Service Customers in collaboration with Elastisys apply the newly released version of Welkin.
7. Elastisys applies the security patch for Managed Service Customers.

Illustrative Example: Third-party security researcher reports a vulnerability to Elastisys

A typical sequence of events is:

1. A third-party security researcher reports a vulnerability to Elastisys, via Elastisys's public security disclosure channel located at https://github.com/elastisys/compliantkubernetes-apps/blob/main/SECURITY.md.
2. Elastisys identifies the affected component and which vendor it belongs to.
3. Elastisys collaborates with the vendor, via their security disclosure channels. For example, for a vulnerability found in Kubernetes, the communication between the security researcher and the vendor proceeds as written in the Kubernetes Security and Disclosure Information page, located at https://kubernetes.io/docs/reference/issues-security/security/.
4. The vendor releases a security patch and announces it via its security announcement channels. For example, for a vulnerability found in Kubernetes, an email is sent to the kubernetes-security-announce@googlegroups.com mailing list.
5. Elastisys becomes aware of the security patch via the vendor's security announcement channels, because Elastisys is subscribed to all security announcement channels of the relevant software components.
6. Elastisys incorporates the security patch into Welkin and releases a new version of Welkin.
7. Elastisys informs Enterprise Service Customers via Slack and/or email that a new security patch was released for Welkin.
8. The Enterprise Service Customers in collaboration with Elastisys apply the newly released version of Welkin.
9. Elastisys applies the security patch for Managed Service Customers.

4. Elastisys Obligations

Elastisys shall, from the Service Start Date as reflected in the Order and for the duration of the Agreement, make the Service(s) available to the Customer.

Elastisys shall, during the term of this Agreement, use commercially reasonable efforts to hold and maintain appropriate insurance policies in relation to its obligations under this Agreement, which insurance policies should be from financially sound and reputable insurers.

5. Customer Obligations

5.1 Acceptable Use Policy

As follows from this Agreement, the Services may not be used unauthorized, which includes unlawful, fraudulent, offensive, or obscene activity. You will comply with all terms and conditions of this Agreement, all applicable laws, rules, and regulations, and all guidelines, standards, and relevant requirements listed on http://www.elastisys.io, that may be updated over time without notice.

You are responsible and liable for all uses of the Services and Documentation resulting from access provided by you, directly or indirectly, whether such access or use is permitted by or in violation of this Agreement. Without limiting the generality of the foregoing, you are responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by you will be deemed a breach of this Agreement by you. You shall use reasonable efforts to make all Authorized Users aware of this Agreement's provisions as applicable to such Authorized User's use of the Services and shall cause Authorized Users to comply with such provisions.

If you become aware of any unauthorized access, copying, modification, or use of the Services, the Customer must promptly provide Elastisys with all details.

5.2 Customer Applications

The Customer is solely responsible for Customer Applications and that it has the capability to receive the Services. The Customer shall, upon request, grant access to and provide Elastisys with information about the Customer Applications to the extent relevant and required to set up, maintain and perform the Services.

The Customer shall not interfere with or disrupt the security, stability, or performance of the Service.

The Customer allows Elastisys to use the Customer's logo on Elastisys' website for marketing purposes, unless agreed otherwise.

5.3 Deployment on Azure Marketplace

If the Service is deployed on Azure Marketplace, the Customer acknowledges that they may make certain modifications at the Azure subscription level. These modifications could impact the stability and security of the Service and are outside

the control of Elastisys. This includes, but is not limited to, the Customer enabling Microsoft Defender for Endpoint, which may introduce additional security scanning processes that could potentially impact the performance of the Service.

The Customer agrees to:

- take reasonable measures to avoid interference with the proper functioning of the Service;
- promptly inform Elastisys of any modifications at the subscription level which may affect Elastisys's ability to deliver the Service;
- not hold Elastisys responsible for any degradation of performance, security, or other adverse effects resulting from such modifications.

6. Service Fees and Terms of Payment

6.1 Service Fee

The Customer shall pay the Services Fee stated in the Order or otherwise as stated in Elastisys' general price list. All Service Fees are exclusive of VAT and other taxes and/or duties. Customer is responsible for all sales, use, and excise taxes, and any other similar taxes, duties, and charges of any kind imposed by any governmental or regulatory authority on any amounts payable by Customer hereunder.

The Service Fee includes the cost of infrastructure required to run Service Instances and Customer Applications. Additional infrastructure used by Customer applications (such as storage for the application, external outbound/inbound network traffic, additional load-balancers, etc.) are added on top of Service Fee.

Similarly, the infrastructure needed for the platform's internal components, such as logging, monitoring, and vulnerability scanning, are sized to meet the demands of average applications. The average needs of applications are calculated based on years worth of data from dozens of production-grade environments. To avoid the risk of data loss, applications that have greater than average needs will require a larger infrastructure footprint for the platform's internal components. For the Managed Service and as per the responsibility model (see Appendix A2.8 Division of responsibility) Elastisys will scale up that infrastructure. The additional costs for this are added to the Service Fee.

Elastisys reserves the right to modify Service Fees for all Services with a notice period of 30 days. Updated Service Fees will override any original Service Fees stated in an Order.

For any overdue payments, Elastisys shall have the right to charge a monthly interest of 8 percent based on the outstanding overdue balance. If payment for Services is more than 60 days past due, Elastisys may, without any liability whatsoever, terminate or suspend providing the affected services to the Customer upon 10 days prior written notice to the Customer.

All Elastisys prices are in SEK. By default Elastisys invoices in SEK, customers can request to be invoiced in Euro (€).

6.2 Terms of Payment

The Service Fee is invoiced by Elastisys after each month of usage. Terms of payment are thirty (30) days from the date of invoice. The minimum billing period for any Service instance is one month. Change Orders that modify the cost of a Service Instance have a billing granularity of one day. Nodes which are provisioned with Autoscaling have a billing granularity of one hour.

The Service Fee for any agreed Professional Services shall be invoiced by Elastisys on a monthly basis in arrears. Terms of payment are thirty (30) days from the date of invoice.

Premium Plan Environments will be billed according to Premium Plan Service Fees from the day of the Service Start Date. However, Premium Plan Service Availability and any associated penalties will be enforced only after the Customer together with Elastisys have successfully completed a go-live checklist. The go-live checklist tests that the application can withstand maintenance windows and disaster recovery with acceptable downtime.

The go-live checklist is located at https://elastisys.io/welkin/user-guide/go-live/. Elastisys reserves the right to continuously, and without notice, update the go-live checklist.

7. Term and Termination

These Terms are effective from the Service Start Date and shall remain in force until terminated by either Party. The mutual termination notice period for termination without cause period is two (2) months unless otherwise agreed in writing by the Parties.

Either Party shall have the right to terminate the Agreement for cause without liability to the other Party, by written notice to the other Party, if;

1. the other Party goes into liquidation;
2. enters into composition proceedings with its creditors;
3. becomes insolvent or is unable to pay its major debts or the majority of its debts or fails or admits in writing its inability to pay its major debts or the majority of its debts as they become due;
4. makes a general assignment for the benefit of creditors or if a petition under bankruptcy or under any insolvency law is filed by or against the other Party and such petition filed by a third party is not dismissed within sixty (60) days (or such longer period agreed upon between the Parties) after it has been filed or a secured part takes possession of all or substantially all of its assets and such process is not dismissed or restrained within thirty (30) days.

Either Party shall have the right to terminate the Agreement forthwith without liability to the other Party, by written notice to the other Party, if the other Party commits a material breach of its obligations hereunder. However, in case such a material breach is capable of being cured, neither Party shall be entitled to terminate the Agreement unless and until the other Party has failed to cure the material breach within thirty (30) days after the failing Party has been served with a notice requiring it to cure such a breach and stating the sending Party's intention to terminate the Agreement if compliance with the notice to cure is not met.

The expiration or termination of this Agreement shall not affect or prejudice any provisions of the Agreement which are expressly or by implication provided to continue in effect after such expiration or termination.

Upon termination of this Agreement, the Customers access to the Services will cease and Elastisys will erase all of the Customer's Data. The Customer is responsible for downloading and/or copying all the Customer's data before the effective date of the termination.

8. Force Majeure

Neither Party shall be liable for non-performance or defective nor late performance of any of their obligations hereunder to the extent that such non-performance, defective or late performance is due to causes and/or conditions outside of the performing Party's reasonable control.

Causes and/or conditions outside of a Party's reasonable control shall include, but not be limited to, acts of terrorism, strikes, and other labor disputes, explosions, earthquakes, wars (whether declared or undeclared), government acts (including

failure to act) (de jure or de facto), sabotage or severe weather conditions which the Party claiming excuse could not have reasonably foreseen the effects of or made alternative arrangements for.

If conditions that fall under force majeure affect this agreement more than three consecutive months, both parties have the right to cancel this agreement with 30 days' notice.

9. Limitation of Liability

Elastisys shall not be liable for any non or late performance or defective Service if this has been caused by Customers' data or Customer Applications; non-compliance with the Customer's obligations; regular system maintenance activities announced by Elastisys in advance; or emergency system maintenance activities which could not reasonably have been foreseen by Elastisys or its third-party program product developers.

Elastisys shall not be liable to the Customer in connection with the Agreement for any indirect or consequential damages, including but not limited to loss of production, loss of data, loss of business, loss of investment, loss of revenue, and loss of goodwill. In the scope of the Agreement, Elastisys does not provide legal or compliance advice. Customers are responsible for making their own assessment of whether their use of the Services meets applicable legal and regulatory requirements.

Elastisys' aggregate and total liability in respect of any one or more events or series of events (whether connected or unconnected) occurring during the term of this Agreement shall per calendar year be limited to direct damages equal to fifty (50) percent of the Service Fees invoiced to the Customer during the calendar year preceding the year when the loss arose. If this Agreement has not been in force during an entire calendar year, the above mentioned amount shall be calculated over a twelve-month period on the basis of the Service Fees already invoiced to the Customer during the calendar year in question.

The limitations of liability set forth herein shall not apply to any liability arising from intent or gross negligence.

9.1 Preview Features

Upon request, Elastisys may offer Customers access to Preview Features. Preview Features are assessed to have a higher residual risk than commonly accepted by Customers. Preview Features are covered by DPAs, but not SLAs (Section 3).

Residual risks include, but are not limited to: (a) risk of downtime, (b) risk of the feature becoming unavailable in the future, (c) risk of data loss. The risks are usually due to novelty of the feature or uncertainties in the open-source ecosystem. By using Preview Features, the Customer accepts these additional risks.

10. Confidential Information

From time to time during the Term and for a period of five years after the Term has ended, Elastisys and Customer may not disclose or make available to third parties the other party's business affairs, products, confidential intellectual property, trade secrets, third-party confidential information, and other sensitive or proprietary information, whether orally or in written, electronic, or other form or media/in written or electronic form or media, whether or not marked, designated, or otherwise identified as "confidential" at the time of disclosure (collectively, "**Confidential Information**"). Confidential Information does not include information that at the time of disclosure is: (a) in the public domain; (b) known to the receiving party; (c) rightfully obtained by the receiving party on a non-confidential basis from a third party; or (d) independently developed by the receiving party. The receiving party shall not disclose the disclosing party's Confidential Information to any person or entity, except to the receiving party's employees, agents, or subcontractors who have a need to know the Confidential Information for the receiving party to exercise its rights or perform its obligations hereunder and who are required to protect the Confidential Information in a manner no less stringent than required under this Agreement. Notwithstanding the foregoing, each party may disclose ConfidentialInformation to the limited extent required (i) to comply with the order of a court or other governmental body, or as otherwise necessary to comply with applicable law, provided that the party making the disclosure pursuant to the order shall first have given written notice to the other party and made a reasonable effort to obtain a protective order; or (ii) to establish a party's rights under this Agreement, including to make required court filings. Each party's obligations of non-disclosure with regard to Confidential Information are effective as of the date such Confidential Information is first disclosed to the receiving party and will expire as set forth above; provided, however, with respect to any Confidential Information that constitutes a trade secret (as determined under applicable law), such obligations of non-disclosure will survive the termination or expiration of this Agreement for as long as such Confidential Information remains subject to trade secret protection under applicable law.

11. Intellectual Property Rights

Elastisys Data and Services, including but not limited to, any derivatives, developments or modifications (upgrades, updates, fixes etc.) thereof and the intellectual and industrial property rights therein, shall be and remain the exclusive property of Elastisys or its subcontractors. Any results of Professional Services created by Elastisys under and during the performance of this Agreement, including any intellectual property rights in relation thereto, which relate specifically to any software used by to deliver the Services shall be the exclusive property of Elastisys or have the option to be released as open source to benefit both the Customer and the wider community. Any results of Professional Services specifically carried out with regard to the Customer's own software shall be the Customer's exclusive property.

The Customer's data and Customer Applications, including but not limited to, any derivatives, developments, or modifications (upgrades, updates, fixes etc.) thereof and the intellectual and industrial property rights therein, shall be and remain the exclusive property of the Customer or its suppliers. The Customer grants Elastisys a non-exclusive, non-transferable, license to use the Customer's data and Customer Applications to perform the Services.

Each Party is responsible for obtaining, at its own cost, all consents and licenses which it requires in order to enable it to perform its rights and obligations in accordance with this Agreement. In particular, the Customer warrants, and is solely liable for ensuring, that it has any and all necessary rights, consents, and licenses to access and process any data provided to Elastisys under this Agreement. In particular, Elastisys warrants, and is solely liable for ensuring that it has any and all necessary rights, consents, and licenses to perform and provide any Services to the Customer under this Agreement.

If the Customer or any of the Customer's employees, contractors, or agents sends or transmits any communications or materials to Elastisys by mail, email, telephone, or otherwise, suggesting or recommending changes to the Services, including without limitation, new features or functionality relating thereto, or any comments, questions, suggestions, or the like ("**Feedback**"), then Elastisys are free to use such Feedback irrespective of any other obligation or limitation between you and Elastisys governing such Feedback. All Feedback is and will be treated as non-confidential. Customer hereby assigns to Elastisys on Customer's behalf, and shall cause its employees, contractors, and agents to assign, all right, title, and interest in, and Elastisys is free to use, without any attribution or compensation to you or

any third party, any ideas, know-how, concepts, techniques, or other intellectual property rights contained in the Feedback, for any purpose whatsoever, although Elastisys is not required to use any Feedback.

12. Indemnity

Elastisys shall at its sole cost defend, indemnify and hold the Customer harmless from and against any and all damages, costs, and expenses incurred as a result of any claim, suits, proceedings or litigation of any kind (actual or threatened) brought against the Customer based on the allegation that the access or use of the Services in accordance with the terms of this Agreement constitutes an infringement of any intellectual and industrial property rights of such third party, subject to Elastisys being authorized to manage and settle the claim, suit or proceeding or other right of action at its own discretion.

The Customer shall, at its sole cost, defend, indemnify and hold Elastisys harmless from and against any and all damages, cost, and expenses incurred as a result of any claims, suits or proceedings or litigation of any kind (actual or threatened) brought against Elastisys based on the allegation that the access to or use of the Customer's data or Customer Applications in accordance with the terms of this Agreement constitutes an infringement of any intellectual and industrial property rights of any third party.

The intellectual property indemnities as set out in this section, shall not apply to the degree and to the extent:

- the claim arises out of breach of this Agreement by the Party entitled to be indemnified;
- the claim arises directly out of compliance by the indemnifying Party with a specification or instructions provided by the Party entitled to be indemnified; or
- the Party entitled to be indemnified has caused or materially and/or substantially contributed to the events which gave rise to the claim under the indemnity.

If such a third-party claim is made or either party reasonably anticipates such a third-party claim will be made, Customer agrees to permit Elastisys, at Elastisys' sole discretion, to (A) modify or replace the Services, or component or part thereof, to make it non-infringing, or (B) obtain the right for Customer to continue use. If Elastisys determines that neither alternative is reasonably available, Elastisys may terminate this Agreement, in its entirety or with respect to the affected component or part, effective immediately on written notice to Customer. This Section sets forth

the Customer's sole remedies and our sole liability and obligation for any actual, threatened, or alleged third-party claim that the Services infringe, misappropriate, or otherwise violate any intellectual property rights of any third party. This Section does not apply to the extent that any such third-party claim arises from Customer Applications, the Customer's Data, or products provided by third-party.

13. Data Protection

In the performance of this Agreement, Elastisys may process personal data on behalf of the Customer, as described in Appendix 1.

14. Subcontracting

Elastisys may use subcontractors for the performance of its obligations under this Agreement. Elastisys is fully responsible and liable for all acts (including omissions) of its subcontractors and shall cause each of its subcontractors to fully abide with all applicable obligations, terms and conditions of the Agreement. Elastisys will not use subcontractors for processing of Customer data that are outside the jurisdiction of European law.

15. Assignment

The Agreement shall accrue to the benefit of and be binding upon the Parties hereto and any successor entity into which either Party shall have been merged or consolidated or to which either Party shall have sold or transferred all or substantially all its assets, but it shall not be otherwise assigned by either Party without the prior written consent of the other Party. The Parties agree that any consent to a requested assignment shall not be unreasonably withheld or delayed. Elastisys shall be entitled to assign this Agreement to any company affiliated with Elastisys, including subsidiaries.

16. No Waiver

The failure of either Party to insist, in one or more instances, upon the performance of any of the terms or conditions of the Agreement, or to exercise any right hereunder, shall not be construed as a waiver or relinquishment of the future performance of any such terms or conditions or the future exercise of such right, and the obligation of Elastisys or the Customer with respect to such future performance shall continue in full force and effect.

17. Notice

Any notice required or permitted to be given by either Party under this Agreement shall be in writing and may be delivered by hand, by courier, sent by registered airmail letter, or electronic mail. Any notice shall be deemed to have been received when actually delivered or

- when left at the address of the recipient, receipt confirmed;
- five (5) days after the date of posting it with ordinary mail; or
- where sent by email, on the day following receipt by the sender of an email confirmation, generated by the machine (or computer) from which the notice was sent, indicating that the notice was sent in its entirety to the recipient's email address, as applicable.

All notices shall be sent to the contact details specified in the Agreement. The notice requirement in this Section 17 does not include support tickets from the Customer to Elastisys.

18. Severability

Each provision of the Agreement is construed in such a manner as to be effective and valid under the substantive laws of Sweden. Should, however, any provision notwithstanding this, by action of law or for any other reason, be held to be prohibited or invalid, the remaining provisions of the Agreement shall, provided that the contractual state of equilibrium between the Parties is not materially distorted as a result of such prohibition or invalidity, remain in full force and effect.

Should the contractual state of equilibrium between the Parties not be materially distorted as a result of a prohibition or invalidity of any provision of this Agreement, the Parties shall promptly agree upon an alternative provision having an effect as similar as possible to the effect of the prohibited or invalid provision.

Should the contractual state of equilibrium between the Parties be materially distorted as a result of the prohibition or invalidity of any provision of the Agreement, the Party not favored by such prohibition or invalidity shall have the right to terminate this Agreement with immediate effect.

19. Entire Agreement and Modifications

This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all previous negotiations, proposals, commitments, writings, oral statements, and understanding of any nature whatsoever.

Customer acknowledge and agree that Elastisys has the right, in its sole discretion, to modify this Agreement and its appendices (including fees) from time to time, and that modified terms become effective on posting. You will be notified of modifications through notifications or posts on Elastisys' website or direct email communication from Elastisys. You are responsible for reviewing and becoming familiar with any such modifications. Your continued use of the Services after the effective date of the modifications will be deemed acceptance of the modified terms. Elastisys will provide at least 90 days' advance notice of changes to any service level that Elastisys reasonably anticipates may result in a material reduction in quality or services. If the Customer chooses not to accept the modification, Customer has the right to terminate the Agreement within 30 days from Elastisys notification of the modification.

20. Governing Law and Dispute

The Agreement shall be governed by and construed in accordance with the laws of Sweden.

Any dispute, controversy or claim arising out of, or in connection with, the Agreement, or the breach, termination or invalidity of the Agreement shall be finally and exclusively settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (the "**SCC**").

The Rules for Expedited Arbitrations shall apply, unless the SCC in its discretion determines, taking into account the complexity of the case, the amount in dispute and other circumstances, that the Arbitration Rules shall apply. In the latter case, the SCC shall also decide whether the Arbitral Tribunal shall be composed of one or three arbitrators.

The place of the arbitration proceedings shall be Stockholm, and the language of the proceeding shall be English, unless both Parties are Swedish entities. In such case, the language of the proceeding shall be Swedish.

Appendix 1 Data Processing Agreement [All Services]

This Appendix applies to both Managed Services and Enterprise Services.

This Data Processing Agreement (the "DPA") between the Customer (below, the "**Processor**") and **Elastisys AB** (below, the **"Sub-processor**") constitutes a part of the Agreement, under which the Sub-processor will process personal data on behalf of the Processor when supplying the Service (including any Professional Services).

A1.1 Instructions

A1.1.1 The Sub-processor shall process the Personal Data in accordance with this Data Processing Agreement as well as with the Processor's written instructions set forth in the Order.

A1.1.2 The Sub-processor may not process the Personal Data for any other purposes or in any other way than as instructed by the Processor from time to time. The Parties shall update Data Processing Instructions in the event of new or amended instructions.

A1.1.3 Notwithstanding the above, the Sub-processor may undertake reasonable day-to-day actions with the Personal Data without having received specific written instructions from the Processor, provided that the Sub-processor acts for and within the scope of the purposes stated in the Data Processing Instructions.

A1.1.4 In the event that the Sub-processor considers that any instruction violates Applicable Legislation, the Sub-processor shall refrain from acting on such instructions and shall promptly notify the Controller and await amended instructions.

A1.1.5 The Processor is responsible to, in writing, give the Sub-processor an up to date list of the categories of Personal Data and categories of data subjects being processed under this agreement. Any changes to the categories of Personal Data or categories of data subjects being processed under this agreement shall be notified to the Sub-processor without delay.

A1.2 The Controller's responsibilities

A1.2.1 The Controller is responsible to ensure that a legal ground recognized under Applicable Legislation applies for processing of the Personal Data. The Controller is also responsible to take other necessary actions to meet all other obligations of a controller under Applicable Legislation.

A1.2.2 The Controller has the sole responsibility for the accuracy, quality, and legality of the Personal Data and the means by which it acquired the Personal Data. The DPA between the Processor and the Controller shall state that the Controller is responsible for informing data subjects of the data processing, and to safeguard the rights of data subjects in accordance with the Applicable Legislation.

A1.2.3 The Processor undertakes to inform the Sub-processor without undue delay of any changes in the processing that may affect the Sub-processor's obligations pursuant to the Data Protection Legislation.

A1.3 Security measures

A1.3.1 The Sub-processor shall maintain adequate security measures to ensure that the Personal Data is protected against destruction, modification and proliferation. The Sub-processor shall further ensure that Personal Data is protected against unauthorized access and that access events are logged and traceable.

A1.3.2 The Sub-processor shall ensure

- that all employees comply with this Agreement and the Instructions, and are informed about relevant legislation,
- that only authorized employees have access to the Personal Data,
- that the authorized employees process the Personal Data only in accordance with this DPA and the Processor's instructions and
- that each authorized employee is bound by a confidentiality undertaking towards the Processor in relation to the Personal Data.

A1.3.3 The Sub-processor shall notify the Processor without undue delay and in no case later than 24 hours after becoming aware of a personal data breach. Such notification shall, where possible, at least contain the information described in Article 33.3 of the GDPR.

A1.4 The sub-processor's obligations to assist

A1.4.1 The Sub-processor shall assist the Processor with the fulfillment of the Processor's obligation under Applicable Legislation by ensuring appropriate technical and organizational measures.

A1.4.2 The Sub-processor shall take measures to protect the Personal Data against all kinds of processing that is not in compliance with this Agreement, the Instructions, and the Data Protection Legislation.

A1.4.3 The Sub-processor shall assist the Processor in relation to the Processor's obligations under Articles 32-36 of the GDPR.

A1.4.4 In the event that the Sub-processor finds the Instructions to be unclear, in violation of the Data Protection Legislation or non-existent, and the Sub-processor is of the opinion that new or supplementary Instructions are necessary in order to fulfill its undertakings, the Sub-processor shall inform the Processor of this without delay.

A1.4.5 In the event the Controller provided the Processor or the Sub-processor with new or amended Instructions, the Sub-processor shall inform the Processor, without undue delay after receiving them, whether the implementation of the new Instructions will entail any changed costs for the Sub-processor.

A1.5 Sub-processors

A1.5.1 The Sub-processor may engage third parties to process the Personal Data or any part thereof on its behalf ("sub-processors"). Where the Sub-processor intends to engage a new sub-processor, the Processor must be informed thereof in writing. The new sub-processor may process the Personal Data if the Processor has not objected in writing 30 days after such information was provided. Approved sub-processors are listed in the Order.

A1.5.2 The Sub-processor shall enter into a written agreement with every sub-processor, in which each sub-processor undertakes obligations at least reflecting those undertaken by the Sub-processor under this DPA. The Sub-processor is responsible towards the Controller for its sub-processors' acts and omissions as for its own.

A1.5.3 In the event the Processor objects to any new sub-processor in accordance with Section A1.5.11, the Sub-processor shall refrain from using such Sub-processor. If that is not practically or commercially reasonable according to the

Sub-processor, both Parties shall at its discretion be entitled either to

- upon prior approval from Sub-processor receive compensation from the Processor for any additional costs incurred by it due to such objection, or,
- terminate the DPA on 45 days' notice.

A1.5.4 The Processor is hereby informed that the Sub-processor made the following assessment: The colocation providers hosting hardware which processes Personal Data are NOT sub-processors. The Sub-processor performed this assessment based on guidance from the Danish Data Protection Authority (Datatilsynet), periodic audits and periodic on-site visits to colocation providers. The Sub-processor closely monitors both the legal landscape and approved sub-processors, and will inform the Processor if said assessment changes.

A1.6 Transfers to third countries

A1.6.1 The Sub-processor shall ensure that the Personal Data will be handled and stored within the EU/EEA by a natural or legal person who is established in the EU/EEA. The location(s) of the Processing of Personal Data (are) is set out in the Order.

A1.6.2 The Parties are aware that changes in legislation, changes in practices and/or other events (such as Public authorities requests) may occur during the term of the Agreement. As a result, it may be necessary to re-assess whether measures taken need to be adjusted or measures need to be taken. To ensure that the Processor is at all times able to (re-)assess whether amended and/or additional measures are required to comply with the EU level of protection of Personal Data, the Sub-Processor shall keep itself informed of all developments concerning changes in the third country's legislation and practices and all relevant requests of public authorities that may lead to its inability to comply with its contractual obligations and to ensure a level of protection, equivalent to the GDPR. The Sub-Processor shall inform the Processor promptly of any such changes and/or events.

A1.6.3 The Sub-Processor shall inform the Processor about additional technical and/or organizational measures that are required to ensure a level of protection, equivalent to the GDPR.

A1.6.4 If, in the Sub-processor's reasonable opinion, no measures can ensure an essentially equivalent level of protection and an alternative solution is not available, the transfer should be suspended with immediate effect. If, as a result, the Sub-Processor is no longer able to perform the Agreement, Parties shall be entitled to terminate the Agreement without any penalties.

A1.7 Audit

A1.7.1 Upon the Controller's request or Processor's request, the Sub-processor will provide the information necessary to demonstrate the Sub-processor's compliance with its obligations under Applicable Legislation and this DPA.

A1.7.2 If the Processor, despite receiving the information set out in Section A1.7.1 above, has a legitimate reason to suspect that the Sub-processor does not fulfill its obligations under Applicable Legislation and this DPA, the Processor shall be entitled on 30 days' written notice to carry out an audit of the Sub-processor's processing of the Personal Data and information relevant in that respect. The Sub-processor shall assist the Processor and disclose any information necessary in order for the Processor to carry out such an audit. The Processor shall ensure that the personnel carrying out the inspection are subject to secrecy or duty of confidentiality pursuant to law or contract. The Processor shall carry the costs for such an audit.

A1.7.3 If a data protection authority carries out an audit of the Sub-processor which may involve the processing of Personal Data, the Sub-processor shall promptly notify the Processor thereof.

A1.8 Costs

A1.8.1 The Sub-processor shall be entitled to remuneration for any time spent to comply with Section A1.4 in accordance with the Services Fee for Professional Services as set out in the Service Order or otherwise as stated in the Sub-processor's general price list for consultancy services. The Processor shall further bear all costs incurred by the Sub-processor due to any altered or additional instructions issued by the Processor regarding the processing of the Personal Data.

A1.9 Limitation of liability

A1.9.1 In the event that compensation for damages in relation to Processing is payable to the Data Subject, through a legally binding judgment or settlement, due to a violation of the Agreement, Instructions and/or applicable provision of the Data Protection Legislation, Article 82 of GDPR is applicable.

A1.9.2 Fines in accordance with Article 83 of GDPR or Chapter 6, Section 2 of the Data Protection Act (2018:218) shall be paid by the party to this Agreement that has been levied such a fee.

A1.9.3 If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimize the damage or loss.

A1.10 Confidentiality

A1.10.1 The Sub-processor undertakes not to disclose or provide any Personal Data, or any information related to the Personal Data, to any third party. For the avoidance of doubt, any sub-processor shall not be considered a third party for the purposes of this Section A1.10. This confidentiality obligation will continue to apply also after the termination of this DPA without limitation in time.

A1.10.2 Notwithstanding Section **A1.10.1** above, the Sub-processor may disclose such information if the Sub-processor is obliged herein by law, judgment by court, or by decision by a competent authority. The Sub-processor shall not be entitled to represent or act on behalf of the Processor or the Controller vis-à-vis supervisory authorities in matters relating to the processing. When such an obligation arises, the Sub-processor shall promptly notify the Processor in writing before disclosure, unless restricted from doing so under Applicable Legislation.

A1.11 Return and deletion of data

A1.11.1 The Processor shall upon termination of the Agreement or this DPA instruct the Sub-processor in writing whether or not to transfer the Personal Data to the Processor (such transfer to be made in a common machine readable format). The Sub-processor will erase the Personal Data from its systems no earlier than 30 days and no later than 40 days after the effective date of termination of the Agreement.

In certain cases, the Processor has access to self-service Service Instance deletion, e.g., by using the Delete Managed application feature in Azure portal. If the Customer self-service deletes a Service Instance, then the Personal Data will be erased immediately, including its backups.

A1.12 Terms

A1.12.1 This DPA shall, notwithstanding the terms of the Agreement, enter into effect when the Sub-processor commences to process Personal Data on behalf of the Processor and shall terminate when the Sub-processor has erased the Personal Data in accordance with Section A1.11 above.

Appendix 2 Managed Welkin Service Specification [Managed Services only]

This Appendix applies only to Managed Services.

A2.1 Service specification

Welkin is a platform for running containerized applications and additional services -- e.g., databases, message queues, and key-value caches -- as required to comply with data protection regulations. Besides the ability to run containerized applications, Welkin comes with out-of-the-box security and observability.

Welkin can be integrated with the customer's Identity Provider to facilitate compliance with Customer's access control policy.

Welkin documentation can be found at https://elastisys.io/welkin/.

Managed Welkin is Welkin offered by Elastisys as a managed service.

A2.1.1 Availability

Subject of the terms and conditions of the Agreement, Elastisys shall use commercially reasonable efforts to make the Service(s) available 24 hours a day, 7 days a week, with the service availability specified below ("**Service Availability**"), except for:

- Planned downtime and maintenance events;
- Force Majeure Events;
- Failures or malfunctions in any Customer equipment or technology; and/or Customer Applications:
    - Downtime due to Node replacement (Customer Applications are expected to tolerate worker Node replacement, one Node at a time); and/or
    - Downtime due to Service Endpoint failover as can happen during maintenance or failures. (Customer Applications are expected to

tolerate Service Endpoint failover, by reconnecting to the newly promoted Service Endpoint).

Availability (uptime) is measured every minute for every Service Endpoint, from external network location whenever possible. Managed Additional Services are measured from internal locations.

Elastisys shall follow industry best practices to ensure Service Availability. In particular, Elastisys shall adjust the size of Service Instances and replication of Service Instances, as required to maintain Service Availability. Elastisys guarantees Availability of each Service according to the following:

	Premium Plan	**Standard Plan**
Service Availability	99.9% 99.95%* (geo-redundant deployment)	Best effort
Service downtime allowed per month	44 minutes **	N/A
Penalty ***	Calculation is based on total monthly fee for the Service Instance Less than 99.9%: 10% credit Less than 99.0%: 25% credit Less than 95.0%: 50% credit	No penalties apply

* 99.95% Service Availability for Premium Plan services deployed in geo-redundant setups that tolerate data center outages.

** 44 minutes (43m 49s) is the maximum allowed downtime in a month (30 days or 43 200 minutes).

*** Upon customer request.

A2.1.2 Response Time

	Premium Plan**		Standard Plan	
Priority level	**Response time***	**Solution target time**	**Response time***	**Solution target time**
Critical Incident	60 min	4 h	60 min **6am to 22pm**	4 h **6am to 22pm**
Major Incident	2 h †	12 h †	2 h †	12 h †
Minor Incident	9 h †	N/A	9 h †	N/A
Change Order	9 h †	9 h †	9 h †	N/A

For General Questions, Elastisys will make commercially reasonable effort to answer within 1 official Swedish business day.

* Response time from a qualified engineer measured from incident start or notification by the Customer

** Environments with the Premium Plan are required to go through a go-live checklist before any uptime service levels are enforced. The go-live checklist tests whether the application can withstand maintenance windows and disaster recovery with acceptable downtime. The go-live checklist is located at https://elastisys.io/welkin/user-guide/go-live/.

† Response time and target solutions times only applies during Business Hours. This is needed in order to minimize unnecessary overtime and comply with the Swedish Working Hours Act (1982:673).

A2.2 Retention for logs and metrics

Standard retention time:

- Application logs are stored for a time period of 30 days.
- Audit logs are stored for a time period of 30 days.
- Metrics are stored for a time period of 90 days. Downsampled metrics may be stored for longer time periods for capacity management purposes.

The retention period for application, audit logs, and metrics can be modified after discussion with the customer. Upon request, Elastisys can help the Customer set up long-term cold storage for both application and audit logs, including off-site replication.

Documentation regarding application logs, audit logs, metrics, as well as long-term retention can be found at:

- https://elastisys.io/welkin/user-guide/logs/
- https://elastisys.io/welkin/ciso-guide/audit-logs/
- https://elastisys.io/welkin/user-guide/metrics/
- https://elastisys.io/welkin/user-guide/long-term-log-retention/

A2.3 Safeguards

Elastisys reserves the right to enforce reasonable and proportionate safeguards to ensure the security and uptime of the platform. These Safeguards are important to enforce in order to stay true to our Data Processing Agreement (DPA) and to keep our customers' data safe. In particular, the Customer does not receive elevated privileges, such as access to underlying VMs, running containers as root, and cluster-admin Kubernetes permissions.

The list of safeguards is located at https://elastisys.io/welkin/user-guide/safeguards/.

Should the Customer require more permissions, this will be granted only after Elastisys determined that such a request does not pose a risk to the security and stability of the platform. How Elastisys conducts such an assessment is located at https://elastisys.io/welkin/user-guide/demarcation/.

A2.3.1 IP Allowlisting

IP allowlisting -- also called network-based access control -- adds an additional layer of security by only allowing access from a trusted set of IP addresses. Elastisys strongly recommends it as a complement to identity-based access control.

As a bare minimum, the Customer should configure IP allowlisting on Welkin Service Endpoints, such as the Kubernetes API. The Customer can easily request such IP allowlisting by filing a service ticket.

The Customer can configure IP allowlisting on applications hosted inside a Welkin environment. The exact steps to follow are located at https://elastisys.io/welkin/user-guide/network-model/.

Upon request, Elastisys can support the customer in configuring IP allowlisting for external IT systems. Said external IT systems run outside Welkin, but need to be accessed by Customer Applications running inside Welkin. The implementation may include manual approaches, such as careful coordination via email, or automated approaches. The Customer and Elastisys jointly decide on the exact implementation, taking into account the following decision drivers:

- Elastisys wants to minimize added risk to the Environment stability and security;
- Elastisys wants to reduce the human overhead to supporting the Customer with IP allowlisting;
- Customer wants to reduce the number of IP addresses trusted by the external IT system;
- Customer wants to reduce the human overhead in (re)configuring IP allowlisting.

A2.4 Backup and disaster recovery

The backup scope includes:

- All data and configuration required to fully restore an Environment and make all relevant Service(s) available through their Service Endpoints.
- For Customer Kubernetes, this includes resources in Customer owned namespaces, such as Pods, Deployments, StatefulSets, DaemonSets, CronJobs, Services, Horizontal Pod Autoscalers, Pod Disruption Budgets, ConfigMaps, Secrets, NetworkPolicies, ServiceAccounts, Roles, RoleBindings, Ingresses, PersistentVolumeClaims, and any additional custom resources added upon service requests.
- Customer Data stored on PersistentVolumes.
- Backups are enabled by default. Customers can opt-out from all backups.
- Customers are responsible to backup any kind of user and application data beyond what is covered by the Welkin resources listed above.

Documentation on how the Customer can configure backups is located at https://elastisys.io/welkin/user-guide/backup/.

Recovery Time Objective:

Recovery from Disasters are handled according to response and solution target times for Critical incidents, see Section 3. Some Customer Applications may need manual intervention after a recovery in order to become fully operational, e.g. Customer Applications that require specific initialization or depend on other components being available.

Recovery Point Objective:

- Backup frequency: once per day, to be performed between 0:00am and 3:00am UTC.
- Backup retention is 30 days, unless otherwise agreed.
- Long-term backup schemes can be enabled after discussion with the customer.

Documentation on how Elastisys protects backups is located at https://elastisys.io/welkin/user-guide/backup/#protection-of-backups.

A2.5 Resizing of platform infrastructure

For robustness and availability, Elastisys reserves the right to increase the infrastructure footprint of the Environment in case the capacity limit has been exceeded. Elastisys will leave headroom as required to ensure a healthy working environment for our on-call engineers, but without causing waste.

More details about how Elastisys performs Capacity Management is located at https://elastisys.io/welkin/operator-manual/capacity-management/.

A2.6 Updates and upgrades

Elastisys uses maintenance windows to take proactive measures for maintaining the stability and security of the Services. Maintenance windows are scheduled together with the customer according to the time frames below.

Type	Definition	Time frame	Frequency
Critical security patches	Patches to fix known vulnerabilities that Elastisys assessed as posing immediate risk to Customer Data.	Immediately	Immediately
Non-critical security patches	Patches to fix known vulnerabilities that Elastisys assessed as posing a security risk, but no data is at immediate risk.	22-05	At most daily
Minor updates	Updates that bring new features and improvements, without requiring careful coordination with the Customer. Minor updates are expected to be backwards compatible and incur negligible risk of downtime.	08-17	At most monthly
Major updates	Updates that bring new features and improvements, but require careful coordination with the customer. Major updates are not expected to be backwards compatible and may require active actions from the Customer.	08-17	Service specific, see appendices

For Major updates, the Customer will be informed and provided a changelog upon Elastisys releases of new versions of Services. Elastisys installs the new release during the next maintenance window. The Customer can only postpone the release by filing a service ticket at least 1 business day before the day of the next maintenance window. This is useful if the Customer needs additional time to verify that any changes to Customer-facing APIs are compatible with the Customer's Applications. Without an explicit written agreement with Elastisys, the Customer cannot postpone a release for more than the Service version lifecycle (see appendices for version lifecycle of each Service).

If the Customer has multiple Environments, and one or more have been designated by the Customer to be non-production Environments, Elastisys will apply major and minor updates to the Customer's non-production Environment(s) at least five working days before applying said update to the Customer's production Environment(s).

Should the Customer want to test upgrades in an additional environment, Elastisys can, subject to a Change Order, create a new Service Instance with the next major version.

Elastisys performs all maintenance according to best practices and will take all commercially reasonable efforts to avoid downtime for Customers during maintenance. Customers are recommended to implement robust applications that tolerate the above maintenance, such as node replacements and Service(s) restart, e.g., as per the go live checklist, which is located at https://elastisys.io/welkin/user-guide/go-live/. Any caused downtime during maintenance is not counted against the Service Availability, as detailed in the above section about Availability.

For Welkin, major upgrades are foreseen approximately 3 times per year, as per Kubernetes release cycle documentation located at https://kubernetes.io/releases/release/.

A2.7 Change Order

The Customer may issue a Change Order to request changes to an Environment, including but not limited to:

- Provision a new Environment.
  - Target resolution time 2 weeks.
  - Service Start Date to be confirmed with the Customer account manager.
- Scale Environment out or in by adding or removing Nodes.
  - Target resolution time 1 business day.
- Scale Environment up or down by resizing Nodes.
  - Target resolution time 1 business day.
- Increase retention for logs or metrics.
  - Target resolution time 1 business day.
- Change backup configuration, e.g., retention.
  - Target resolution time 1 business day.
- Decommission Environment.
  - Target resolution time: 1 week.

A2.8 Division of responsibility

Responsibility assignment matrix; Responsible, Accountable, Consulted, Informed (RACI).

Setup and contributions

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Definition of Welkin Architecture				X	X	X		
Contribution of all related software components needed to run Welkin					X	X		
Contribution of all related software licenses needed to run Welkin					X	X		
Installation and configuration of all related Welkin components: • Setup of virtual machines and related infrastructure on the infrastructure provider • Setup of Welkin • Setup of related networking configuration (accessible on public Internet IP) • Setup of initial user privileges Notes: Customer selects Environment dimensioning as well as identity provider for installation.		X			X			

Maintenance and operations

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Administration of relevant user privileges Notes: Connection to external identity provider is the Customer's responsibility			X	X	X	X		
Planned major updates and unplanned updates			X	X	X	X		
Updating Customer Kubernetes objects (resources) that are part of their Applications as required for major updates.	X	X					X	
Planned minor upgrades				X	X	X		
Monitoring of key metrics (CPU, RAM, disk space)				X	X	X		
Adding/deleting/starting/stopping compute Nodes during maintenance					X	X		
Performing maintenance work in maintenance window			X	X	X	X		
Backup			X	X	X	X		
Recovery		X			X			
Responsibility for any kind of Customer Application	X	X						
Aggregation of all container and audit logs					X	X		
Ensure that Customer Applications tolerates Node replacement	X	X					X	

Decommissioning

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Extraction of Customer data and Customer Application	X	X						
Shutdown and removal of Welkin application elements including data and infrastructure		X			X			

Performance management

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Collecting Service(s) performance metrics					X	X		
Collecting Customer Application(s) performance metrics		X	X					
Performing configuration changes that affects Environment capacity, including: • Scale Environment up or down • Scale Environment in or out • Modify storage capacity for logs increase (i.e. switch to larger Node, or increase storage for logs)		X			X	X*		
Performance of Customer Application(s)	X	X						

* Elastisys accountable for minimum capacity

Incident management

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Classification of incidents	X	X*					X	
Investigation of incidents		X			X			
Performing configuration changes			X		X	X		
Setup and maintenance of ticketing system				X	X	X		
Documentation of performed recovery actions				X	X	X		

* Elastisys reserves the right to downgrade the incident's level. See 3.4 Incident Levels and Response Time.

A2.8 Pricing

The Customer is charged for:

- **change orders** and **incident management** on the basis of a monthly subscription;
- **proactive security and stability improvements** on the basis of a monthly subscription;

- **consultancy** on a time-and-material basis;
- **training** on an as-needed basis.

A2.8.1 Change Orders and Incident Management

This covers handling support tickets within the scope of the platform, such as:

- creating and terminating Environments or Additional Services;
- resizing Environments and Additional Services;
- help with troubleshooting;
- disaster recovery.

These activities are covered by the stipulated response times.

A2.8.2 Proactive Security and Stability Improvements

This covers activities such as:

- applying monthly platform updates;
- applying security patches as needed;
- proactive monitoring to ensure platform stability and security.

Premium Plan further includes:

- 1 yearly go-live exercises, which includes a disaster recovery drill.

The go-live checklist is located at https://elastisys.io/welkin/user-guide/go-live/.

A2.8.3 Consultancy

Consultancy on a T&M basis, such as:

- migration assessment;
- help with adapting the application to conform to Kubernetes and security best practices;
- security review;
- handling any other support ticket outside the scope of the platform.

A2.8.4 Training

Training on an as-needed basis, such as:

- training the application team on effectively using the platform.

Appendix 3 Managed Additional Service Specification [Managed Services only]

This Appendix applies only to Managed Services.

A3.1 Service Specification

Elastisys can manage the following Additional Services within an environment:

- Databases: PostgreSQL versions 13, 14, 15 or 16.
- Low-latency in-memory caches: Ephemeral Valkey (Redis version 7.2 compatible)
- Message queues: RabbitMQ version 3
- Time-series database: TimescaleDB Community (only open-source features are included)
- Continuous delivery: Argo CD 2 (only namespace-level, non-admin and non-beta features are included)

Documentation regarding Additional Services is located at https://elastisys.io/welkin/user-guide/additional-services/.

For fault-tolerance, Additional Services are replicated as follows:

- PostgreSQL Premium Plan: 3 dedicated Nodes
- Ephemeral Valkey: 3 dedicated Nodes
- RabbitMQ: 3 dedicated Nodes
- TimescaleDB Premium Plan: 3 dedicated Nodes
- PostgreSQL Standard Plan: 2 dedicated Nodes
- TimescaleDB Standard Plan: 2 dedicated Nodes
- Argo CD: not replicated, but guaranteed to fail-over within 5 minutes

A3.2 Retention for logs and metrics

Additional services feature the following monitoring capabilities:

- Service-specific logs, as produced by PostgreSQL, Ephemeral Valkey, and RabbitMQ, respectively.
- Audit logs contain which Authorized User accessed which Service and when, and also any changes to Service configuration. Audit logs for the database (PostgreSQL), e.g., which query was executed by which user when, can be enabled upon request.
- Metrics, e.g., synchronization latency, number of requests per second, CPU usage, memory usage, disk I/O, and network I/O.

The Customers can view monitoring data through the monitoring endpoints of Welkin.

Retention times of additional services are the same as the Welkin environment that hosts them. See A1.2.

A3.3 Customer access

Out-of-cluster Authorized User access is performed via OpenID and RBACs, covered by audit logs (included in Welkin). In addition, NetworkPolicies can be used to control access to Additional Services from selected microservices of the Customer Application.

For PostgreSQL and RabbitMQ, the Customer is given user access with privileges to delegate access to other Authorized Users and Customer Applications, as required. For Valkey, access is controlled via NetworkPolicies only, i.e., no usernames and passwords.

For Argo CD, the Customer only has self-service access to user (non-admin) features. Other features of Argo CD -- in particular those requiring admin access or cluster-wide mode -- might not be available or might only be available via service tickets. These safeguards are needed to maintain platform stability and security, in line with A2.3 Safeguards.

A3.3b Application access

By default, additional managed services are only accessible for applications running within the respective Kubernetes environment. Customer can request out-of-cluster access if Customer accepts the added security risks.

A3.4 Backup and disaster recovery

The backup scope includes:

- For PostgreSQL: user definitions, data definitions, and the data per-se.
- For RabbitMQ: user definitions, vhost definitions, topology definitions.
- For Argo CD: resources that can be created by application developers, such as: ApplicationSets; Applications; AppProjects; Secrets and ConfigMaps as needed to store configuration on repositories and notifications.

The backup does NOT include:

- For RabbitMQ: messages -- RabbitMQ core contributors discourage this.
- Ephemeral Valkey -- data cached in Valkey should be ephemeral with the source of truth stored in a database or user device.

Recovery Time Objective:

- Recovery from Disasters are handled according to response and solution target times for Critical incidents, see A2.1.2 Response Time.

Recovery Point Objective:

- A full backup of PostgreSQL, RabbitMQ definitions and Argo CD is taken every day between 0:00 am and 6:00 am UTC. The backup retention period is 30 days unless otherwise requested by the customer.
- For PostgreSQL, point-in-time recovery is provided for the last 7 days with a recovery point objective of 5 minutes.
- Long-term backup schemes can be enabled after discussion with the customer.

Documentation on how Elastisys protects backups is located at https://elastisys.io/welkin/user-guide/backup/#protection-of-backups.

A3.5 Capacity Management

The Customer is responsible for ensuring that the Size of the additional Service matches the demand of the application.

The Size of the additional Service needs to take into account overhead due to various data protection-related platform components, e.g., intrusion detection, log collection, and metrics collection.

Load testing is recommended for Standard Plan Environments and is mandatory for Premium Plan Environments to ensure additional Services are properly sized. Documentation on how to perform load testing is located at https://elastisys.io/welkin/user-guide/go-live/.

A3.6 Updates and upgrades

For PostgreSQL, major upgrades are foreseen approximately 1 times per year, as per PostgreSQL release cycle located at https://www.postgresql.org/support/versioning/.

For RabbitMQ, major upgrades will be available depending on upstream releases and Elastisys's risk assessment on the stability and security of the new major releases.

For Valkey, major upgrades will be available depending on upstream releases and Elastisys's risk assessment on the stability and security of the new major releases. Valkey upstream release cadence is located at https://valkey.io/topics/releases/.

For Argo CD, minor upgrades will be available depending on upstream releases and Elastisys's risk assessment on the stability and security of those releases. Argo CD upstream Release Process and Cadence is located at https://argo-cd.readthedocs.io/en/stable/developer-guide/release-process-and-cadence/.

Minor upgrades for Additional services are performed as specified in Section A2.6.

A3.7 Change Order

The Customer may issue a Change Order to request changes to an Environment, including but not limited to:

- Provision a new instance of a Service.
  - Target resolution time 1 week.
- Changing the Size of a Service.
  - Target resolution time 1 business day.
- Changing the storage capacity (disk) of a Service.
  - Target resolution time 1 business day.
- Change backup configuration, e.g., retention.
  - Target resolution time 1 business day.
- Decommission a Service.
  - Target resolution time 1 business day.

- The Customer is responsible for saving any data stored in the Service before issuing the Change Order.

A3.8 Division of responsibility

Responsibility assignment matrix; Responsible, Accountable, Consulted, Informed (RACI).

Setup and contributions

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Definition of Architecture				X	X	X		
Contribution of all related software components needed to run additional services					X	X		
Contribution of all related software licenses needed to run additional services					X	X		
Installation and configuration of all related components: • Setup of virtual machines and related infrastructure on the infrastructure provider • Setup of additional services • Setup of related networking configuration (accessible within an Environment) • Setup of superuser privileges		X			X			
Provision a new Service instance		X			X			
Decommission a Service instance		X			X			

Maintenance and operations

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Administration of relevant user privileges	X	X						
Network segregation		X			X			
Planned major updates and unplanned updates			X	X	X	X		
Planned minor upgrades				X	X	X		
Monitoring of key metrics (CPU, RAM, disk space)				X	X	X		
Performing monthly maintenance work in maintenance window				X	X	X		
Backup				X	X	X		
Recovery		X			X			

Decommissioning

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Extraction of customer data	X	X						
Shutdown and removal of additional services components, data, and related infrastructure		X			X			

Performance management

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Collecting performance metrics					X	X		
Migrate to a larger (or smaller) Service size (change plan) Notes: Performance configuration changes only performed upon request by customer via Change Orders. The customer is responsible to ensure sufficient capacity upon change to a smaller plan. Data migration between Database instances is also the responsibility of the Customer.		X			X			

Incident management

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Investigation and classification of incidents			X		X	X		
Setup and maintenance of ticketing system				X	X	X		
Documentation of performed recovery actions				X	X	X		

A3.9 Pricing

Pricing of Additional Services is performed as for the Welkin environment that hosts them. See A2.8 Pricing.

Appendix 4 Privacy Policy for Authorized Users [All Services]

This Appendix applies to both Managed Services and Enterprise Services.

A4.1 Introduction

Elastisys prides itself with being a data protection and privacy front-runner. Therefore, we take the privacy of Authorized Users seriously. As part of our service, we process personal data of Authorized Users for change management and auditing purposes, in accordance with GDPR, Swedish Patient Data, and other applicable laws and regulations.

Note that, this privacy policy **only** applies to Authorized Users. Customer Data is processed according to Appendix 1 Data Protection Agreement.

A4.2 Purpose

We collect personal data of Authorized uses for the following purposes:

- managing access to Services;
- executing Change Orders and complying with our change management policy;
- keeping an audit log.

A4.3 Personal Data We Process

The personal data we process includes contact information, such as IP addresses, first name, last name, business email, and business phone.

A4.4 Legal Basis

We process personal data of Authorized Users based on legitimate interest.

The three-part Legitimate Interest Assessment (LIA) is as follows:

- Purpose test: We need to be able to demonstrate that we properly executed Change Orders.
- Necessity test: As an ISO 27001-certified supplier, we are expected to keep audit logs. Only personal data of Authorized Users which is relevant for the Change Orders is stored.
- Balancing test: Only personal data of Authorized Users is processed. Art. 32 GDPR has been interpreted as requiring storing audit logs.

A4.5 Retention

By default, audit logs are stored the personal data of Authorized Users for at least 30 days.

Change Orders are stored for as long as we have a business relationship plus 30 days.

A4.6 Protection of personal data

We protect personal data of Authorized Users as following:

- Encryption: Personal data is encrypted in-transit. If supported by the underlying subprocessor, personal data is also encrypted at-rest.
- Data minimization: We only process necessary personal data of Authorized Users.
- Access minimization: Access to personal data of Authorized Users is only permitted to Elastisys employees needing it.

A4.7 Rights of Authorized Users

Authorized Users have the right to:

- access their personal data;
- request rectification or erasure of their personal data;
- object to the processing of their personal data;
- withdraw their consent to the processing of their personal data at any time;
- file a complaint with the Swedish Authority for Privacy Protection (IMY), whose website is located at https://imy.se.

A4.8 Processors and Third Countries

We use the following Processors for processing personal data of Authorized Users:

Name of Subprocessor	Description of Processing	Location of Processing	Corporate Location	DPA
Atlassian (JIRA)	service ticket handling	Global	US	DPA
Google Workspace (GMail, Drive)	Email communication, storing contact information	Global	US	DPA
Telavox AB	Phone communication, storing contact information	Sweden	Sweden	DPA is stored internally

Certain audit logs, such as Kubernetes API accesses, are stored within your Environment and hence use the Subprocessor which you chose when you ordered the creation of the Environment.

As of 2023-05-31, the US is a third country. See what this means on IMY's website: EN SE.

According to our experience, these services are ubiquitously used and appreciated by Authorized Users. Therefore, we assessed that their usage does not add risk to the privacy of Authorized Users.

A4.9 Contact information

If you have any questions or concerns about our privacy policy, please contact us at dpo@elastisys.com.

Name and contact details of the Data Controller:

```
Elastisys AB Org.nummer 556873-6135 Kuratorvägen 2A, 907 36 Umeå, Sweden
```

A4.10 IT Systems Outside the Scope of this Privacy Policy

As part of our Service, Authorized Users may choose to communicate with Elastisys over a shared Slack channel. Within the scope of that communication, the Slack Privacy Policy applies, which is located at https://slack.com/trust/privacy/privacy-policy.

Elastisys uses a self-hosted Yopass instance to secure share secrets. IP addresses are only processed as much as technically required. We do not retain personal data in Yopass. We advise customers to access Yopass from their corporate network, so their IP addresses do not constitute personal data.

Appendix 5 Enterprise Service Specification [Enterprise Services only]

This Appendix applies only to Enterprise Services.

A5.1 Service specification

Welkin is a platform for running containerized applications and additional services -- e.g., databases, message queues, and key-value caches -- as required to comply with data protection regulations. Besides the ability to run containerized applications, Welkin comes with out-of-the-box security and observability.

Welkin can be integrated with the customer's Identity Provider to facilitate compliance with Customer's access control policy.

Welkin documentation can be found at https://elastisys.io/welkin/.

Enterprise Services -- such as Welkin and Additional Services -- are operated by the Customer with support from Elastisys. Elastisys does not have access to Customer Environments, unless otherwise agreed.

Enterprise Services give the Customer access to experienced, motivated, highly skilled, and knowledgeable technical support engineers, within the response times stipulated below.

The Customer benefits with peace of mind and cost savings by:

- not having to develop an in-house Kubernetes-based platform;
- not having to hire an expensive in-house team of Kubernetes and Cloud Native experts;
- not having to "scramble" to find Kubernetes and Cloud Native experts to help deal with incidents and disasters.

Elastisys trains the Customer's in-house operations team as required for them to handle first-line operations. Elastisys virtually extends the Customer's on-call team with second-line operational support.

A5.2 Response Time

	Enterprise Plan (8am to 17pm)	
Priority level	**Response time***	**Solution target time**
Critical Incident	60 min †	4 h †
Major Incident	2 h †	12 h †
Minor Incident	9 h †	N/A
Change Order	9 h †	N/A

For General Questions, Elastisys will make commercially reasonable effort to answer within 1 official Swedish business day.

* Response time from a qualified engineer measured from incident start or notification by the Customer

† Response time and target solutions times only applies during Business Hours. This is needed in order to minimize unnecessary overtime and comply with the Swedish Working Hours Act (1982:673).

A5.3 As a whole, for the intended use-case

We optimized our product management, architecture design, development and quality assurance processes for the intended use-case of running a secure platform for containerized applications. Therefore, we can only provide support for Welkin as a whole for said use-case.

We are aware that it is technically possible to split Welkin and use some of its components in isolation. We are also aware that some or all of said components can be used for other use-cases. However, such use has unknown consequences and is untested by Elastisys. Therefore, such use is not within the scope of the Enterprise Plan.

A5.4 Division of responsibility

Unless otherwise agreed, responsibilities between the Customer and Elastisys are divided according to the Responsibility assignment matrix -- Responsible, Accountable, Consulted, Informed (RACI) -- below.

Note that, the Customer is overall responsible to ensure Customer Data confidentiality, availability and integrity.

Platform Development

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Definition of Welkin Architecture				X	X	X		
Releasing Welkin security patches				X	X	X		
Keeping Troubleshooting documentation up-to-date				X	X	X		

Application Development and Operations

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Ensure the application conforms to good containerization practices, both for security and stability	X	X					X*	

* Elastisys is a Kubernetes Training Partner and can provide experienced consultants integrated with the Customer's application team. This enables the application team and their application to use the Welkin platform in the best possible way. More information can be found at https://elastisys.com/training/.

Platform Operations

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Audit the underlying infrastructure to ensure its suitability given the Customer's security and stability goals	X	X					X*	
Installing Welkin	X	X					X*	
Configuring Welkin	X	X					X*	
Monitoring uptime of Welkin endpoints	X	X					X*	
Troubleshooting Welkin	X	X					X*	
Applying updates and security patches	X	X					X*	
Monitor and adjust capacity as needed	X	X					X*	
Periodically perform disaster recovery drills	X	X					X*	
Monitor and ensure stability of the underlying infrastructure	X	X						

* With a basis in the Welkin public documentation located at https://elastisys.io/welkin/operator-manual/, Elastisys supports the customer in finding, understanding and also performing the necessary steps to achieve platform-related administration.

Incident management

Activity	Customer				Elastisys			
	R	A	C	I	R	A	C	I
Classification of incidents	X	X*					X	
Investigation of incidents	X	X					X	
Performing configuration changes	X	X					X	
Setup and maintenance of ticketing system				X	X	X		
Documentation of performed recovery actions	X	X						X

* Elastisys reserves the right to downgrade the incident's level. See 3.4 Incident Levels and Response Time.

A5.5 Pricing

The Customer is charged for:

- **support** on the basis of a monthly subscription;
- **consultancy** on a time-and-material basis;
- **training** on an as-needed basis.

A5.5.1 Support

Support covers handling support tickets within the scope of the platform, such as:

- help with creating and terminating Environments or Additional Services;
- help with applying platform upgrades and security patches;
- help with troubleshooting;
- help with disaster recovery training and execution (maximum 2 times per year).

These activities are covered by the stipulated response times.

A5.5.2 Consultancy

Consultancy on a T&M basis, such as:

- activities required for configuring systems and applications owned by the Customer as needed to run the platform, such as:
  - infrastructure audits;
  - devising the architecture of the infrastructure upon which an Environment shall be deployed;
  - helping out the Customer configure their Identity Provider (IdP);
  - helping out the Customer configure their infrastructure;
  - test that the infrastructure and IdP were configured as needed;
  - alert tuning;
  - initial disaster recovery and business continuity testing;
  - help with adapting the application to conform to Kubernetes and security best practices;
- handling any other support ticket outside the scope of the platform.

A5.5.3 Training

Training on an as-needed basis, such as:

- training the application team on effectively using the platform;
- training the in-house on-call team.