

## INTLAND TECHNICAL SUPPORT AGREEMENT

This Support Agreement ("Agreement") is a legal agreement between Intland Software GmbH ("Intland"; tax identification number: DE198055925) and the individual or entity ("End User") using and/or accessing the Intland codebeamer and Intland codebeamer X Softwares ("Intland products"). Intland shall provide Support Services in accordance with the terms of this agreement. Such terms may be amended from time to time by Intland Software.

### Scope of the Services

Intland provides technical support (Support) for customers under a valid Intland LICENSE AGREEMENT and SUPPORT AGREEMENT for the licensed Intland products.

### Supported Version of the Software

Intland provides Support for the selected set of versions that can be found on the website of Intland (under the following [link](#)). The list of the supported versions of the software is exclusive, Intland does not provide support services to other earlier released versions. The Software Release date is identical to the Software build date show on the Software.

### Support Service Options

Options	Standard	Silver
<a href="#">Knowledge Base</a> access	Yes	Yes
Online download access to the latest releases and patches, and upgrades	Yes	Yes
<a href="#">Customer Service Desk</a>	Yes	Yes
phone	Yes	Yes
live screen sharing	Yes	Yes
e-mail	-	Yes

Options		Standard	Silver
Number of users able to create incidents		2	4
Support language		English / German	English / German
Support hours		8x5	24x5 (for Critical)
Initial Response Time ( <sup>5</sup> ) for different Incident Severity Levels	Critical ( <sup>1</sup> )	8 Business hours	4 Business hours
	Major ( <sup>2</sup> )	2 Business days	1 Business day
	Medium ( <sup>3</sup> )	3 Business days	2 Business days
	Low ( <sup>4</sup> )	5 Business days	5 Business days
Information Security Incident Response (ISIR)		see Chapt. Information Security Incident	see Chapt. Information Security Incident
Dedicated support		Support Engineer	Sr. Support Engineer
Advice on installation		Yes	Yes
Log analysis		Yes	Yes
Upgrade Support		-	Yes
Remote upgrade		-	Yes
Remote assistance		-	Yes
Resource and Performance Monitoring		-	Yes
API support		-	Yes
Free staging server		-	Yes
Annual on-site visit		-	Yes
Price		20% of license list price	Please contact our sales team ( <a href="mailto:sales@intland.com">sales@intland.com</a> ) for a quote!

## Definitions of normal Incident Severity Levels

Intland will classify the normal incidents on their Severity Level according to the criteria below. Intland may re-classify Incidents if it believes that the original classification is incorrect. The Response Goal shall not apply if the Incident is caused by third party Software. Intland will not correct any Software Failure caused by modification or enhancement of the Software, or when the Failure is corrected by an existing Software release provided by Intland.

Severity	Definition	Response Goal
<b>(1) Critical</b>	The "Production system" is not available, substantially unavailable, or normal business operations are seriously disabled. The incident is preventing productive work on your production system, and it affects users performing a business-critical function. If Intland Software provides an acceptable workaround, the severity classification will drop to Medium or Low.	Intland will provide a response and begin to analyze the incident and verify the existence of the problem within the Initial Response Time <sup>(5)</sup> defined period. Intland will use commercially reasonable efforts to resolve Critical Incidents as soon as possible. The resolution will be delivered as a Workaround or Hotfix. If Intland provides an acceptable Workaround or Hotfix for the Incident, the severity classification will drop to Medium or Low.
<b>(2) Major</b>	The "Production system" is available but the incident has a business-critical impact on your production system; a function or functions are not available or are not working properly, preventing productive work, and affecting people performing a business-critical function.	Intland will provide a response and begin to analyze the Incident and verify the existence of the problem within the Initial Response Time <sup>(5)</sup> defined period. Intland will use commercially reasonable efforts to resolve Major Incidents as soon as possible or in the next Maintenance Release. If Intland provides an acceptable workaround for the Incident, the severity classification will drop to Medium or Low.
<b>(3) Medium</b>	The incident has a business impact on your "Production system", but does not prohibit the execution of productive work, or a reasonable workaround is available.	Intland will provide a response and begin to analyze the Incident and verify the existence of the problem within the Initial Response Time <sup>(5)</sup> defined period.
<b>(4) Low</b>	The incident is not production-critical, or it is detected on your non-production system. The incident has no impact on the "Production System" performance, quality or functionality and no impact on productive work.	Intland will provide a response to the Incident and verify the existence of the problem within the Initial Response Time <sup>(5)</sup> defined period. Intland does not guarantee a resolution time for Low Severity incidents.

## Information Security Incidents Response

Any security events and information security weaknesses should be assessed immediately after the incident/event has been observed, and it should be decided if they are to be classified as information security incidents.

Information security events and weaknesses shall be classified under the below four severity levels:

1. Major (Security) Incident
2. Normal (Security) Incident

Security incidents need to be reported under the following links:

CB: <https://codebeamer.com/cb/tracker/16949942>

CBX : <https://codebeamer-x.com/x#/tracker/12613106/0>

Classification/Severity	Event description	Action	Reaction Time
1. Major (Security) Incident	<ul style="list-style-type: none"><li>- Organization has lost the ability to provide a critical service to a subset (or all) of system users.</li><li>- Personal or other sensitive data was compromised.</li></ul>	<ul style="list-style-type: none"><li>- Time to recover is long enough, and additional resources are needed.</li><li>- Escalation, internal and external communication.</li><li>- Additional resources should be made available.</li></ul>	4 working hours
2. Normal (Security) Incident	<ul style="list-style-type: none"><li>- The company can still provide all critical services to all users but has lost efficiency.</li><li>- No personal or other sensitive data was compromised.</li></ul>	<ul style="list-style-type: none"><li>- Time to recover is predictable with existing resources.</li><li>- Information Security Incident Response Team (ISIRT) can manage the whole incident handling process at its own discretion within a reasonable time frame.</li></ul>	8 working hours

Just for clarification: application security vulnerabilities are not considered as security but normal incidents, normal incidents are governed by Secure SDLC process as part of SOP 1 (Software Development and Operations).

## Standard Support

With Standard Support two members (or more members, but only if this is agreed in writing in advance, depending on the End-User's selected service package) of your team able to create an unlimited number of incidents on our Customer Service Desk, Standard Support includes support by phone, live screen sharing. Standard Support is available in both German and English, with a dedicated Support Engineer attending to your tickets 8 hours a day (9AM-5PM CET), 5 days a week (Mon-Fri).

## Silver Support

Silver Support includes a wide range of support services. This flexible support plan lets 4 members of your team submit an unlimited number of incidents either using the Customer Service Desk or via e-mail, based on which your team may receive help via phone, e-mail, or live screen sharing over the web. Silver Support is provided in both English and German and includes 24x5 (Mon-Fri) support for critical incidents by our dedicated senior Support Engineers.

## Business Hours

Intland Software's business hours are 9:00 AM to 17:00 PM CET (GMT +1), Monday through Friday, excluding German national holidays. For information on German public holidays see the following [link](#).

## What is covered by Inland's Support service?

- Root cause analysis, identifying and troubleshooting incidents
- Assistance on installation incidents
- Guidance on upgrade incidents
- Guidance on Inland's supported integrations (3<sup>rd</sup> party integrations are not covered)
- Analysis of SSO, LDAP/AD connection problems
- Incidents are usually resolved in newer releases, thus an upgrade may become necessary to benefit from fixes.

## What Inland's Support service does not cover?

- Technical Support for end of live versions (see [currently supported versions](#)).
- When the software is used on a non-recommended platform or in a non-recommended environment. Recommended platforms and environments are described in the [knowledge base](#).
- Customers without a valid software license, or a valid Support & Maintenance Agreement.
- Beta releases, release candidates, snapshots, and end-of-life releases, and for deprecated features.
- Customized product instances where the original source code was changed or extended.
- Programming-related or development related questions and requests.
- Product education questions.
- Professional services, including:
  - Installation and upgrade services (Support helps with advices)
  - Docker configuration issues
  - Customization
  - Performance tuning
  - Infrastructural problems, configuration of SSO, OpenID Connect, LDAP/AD configuration, Apache & web server, [Proxy and Firewall issues](#)
  - Database and clustering configuration
  - 3rd party integrations
- Failures caused by software for which Inland is not responsible

## Support Incident Reporting, Contact Methods

Tickets submitted using Incident Trackers are handled with the severity as entered, and Incidents can be entered by Authorized Contact(s). Authorized Contact(s) must have sufficient Software expertise and training. You can also contact us by emailing [support@intland.com](mailto:support@intland.com) or calling us.

- US phone number: 866-468 5210.
- European phone number (+49) 711-2195-420.

Incidents should be reported on <https://intland.com/technical-support/>.

Incidents submitted via email or telephone are automatically assigned with low severity.

## Required Information on incidents

All incident reports must, if applicable, include the following:

- The Licensee's "account" which Intland shall provide to the Licensee on registration.
- The exact Version Number and the Platform that the Software is running.
- Before reporting an Incident, the Licensee must verify that the Incident is reproducible. The Licensee should provide a reproducible Test Case that demonstrates the specific usage that causes the Software Failure being reported.
- Log files, screenshots, trace files.
- Exact wording of all related error messages.

In case of reported Information Security Incidents the following data has to be provided:

- Name of the incident
- Summary of the incident (some evidence has to be provided, for example screen shot, alert notice etc.)
- Categorization

Please note that in this tracker Information Security incidents must be reported exclusively, not any feature request or improvement request can be submitted. If such a feature request or improvement request is included the incidents are going to be closed without further investigation.

Our Silver Support service covers remote upgrades & assistance, API support, a free staging server, and an annual on-site visit to your team by our experienced Support Engineers.

## API Support

- To analyze incidents reported against Rest- and/or OpenAPI (Swagger), a sample code that demonstrates the problem must be provided.
- API support does not include answering API related development questions.

## Incident Status and Workflow

The table below show each incident status and describes which actions are performed in each different st

Incident Status	Description
<b>New</b>	Every reported incident gets this status. Generally, only recently submitted incidents are in this status.
<b>Under Investigation</b>	Inland's Support Team is analyzing the incident.
<b>Pending</b>	Inland's Support Team requires (and is waiting) for further information about the incident. After receiving the required information, the incident should transition to the status <b>Under Investigation</b> . Items remaining in this status for 30 calendar days will be automatically closed.
<b>Short Term Target</b>	The reason of the incident is identified, and the fix is planned for next upcoming release.
<b>Medium Term Target</b>	The reason of the incident is identified, and the fix is planned for one of the upcoming releases.
<b>Long Term Target</b>	The reason of the incident is identified, and the fix is planned to be delivered in subsequent future releases later on.
<b>Resolved</b>	The incident is considered resolved. Items remaining in this status for 30 calendar days will be automatically closed.
<b>Closed</b>	The incident is closed, no further activity is available.

## Incident and Bug Fixing Policy

Inland Support helps with workarounds and advices to resolve specific product incidents.

### Bug Fixes

Fixes for non-critical, non-security bugs will be provided by Inland Software in the next maintenance release, with the conditions that:

- The fix is technically feasible, and
- The fix doesn't impact the quality or integrity of the Software.

Inland Software assesses and prioritizes bugs and schedules fixes for non-critical incidents based on internal considerations. Factors considered in the analysis and prioritization of bugs include, but are not limited to:

- How many customers are affected by the problem?
- Whether there is an effective workaround or patch to the incident
- How difficult the incident is to fix?
- Whether a fix is already available in a newer release
- Whether new features on our roadmap make the bug obsolete
- Internal factors within Inland's judgement.



## Hotfixes (patches)

In special cases Intland provides Hotfixes (patches) when the

- incident's Severity is classified by Intland as "Critical" or
- the incident is security related.

Critical Incidents are where the "Production system" is not available, substantially unavailable, or normal business operations are seriously disabled. The incident is preventing productive work on your production system, and it affects users performing a business-critical function.

Non-security Hotfixes are only available on a case by case, by user requested basis, and Intland reserves the right to charge for hotfixes based on custom quotes.

## Customization, Feature and Change Requests

Intland Software provides various extensions, templates, and other customization options with documentation and examples to support the customization of the Software.

In addition, Intland Professional Services provides help with answering questions regarding customization, configuration, add-ons, product development, performance tuning, clustering, and creating integrations with 3rd party tools.

Please contact [sales@intland.com](mailto:sales@intland.com) to request professional services.

## Appendix

### Definitions

- a) **Production System** means the Software that is being used as a regular part of actual day to day business operations.
- b) **Services** refers to the Support Services listed in this document.
- c) **Version Number** is a three-part version number in the form of A.BB.CCC which identifies Releases of Intland products.
- d) **Incident** means bug or failure reported to Intland as a result of a reproducible operational deviation of the Software from the Software specifications.
- e) **Business Hours** are 9:00 AM to 17:00 PM CET (GMT +1), Monday through Friday, excluding German national holidays. For information on German public holidays, see the following [link](#).
- f) **Workaround** means a Hotfix or other method used to avoid Software Failure.
- g) **Releases of codebeamer** refers to any new version of Intland Software's products that delivers extended functionality, performance and usability improvements, and bug fixes. In some cases, Intland Software may consolidate features due to global system improvement, resulting in the removal of certain features.
- h) **LTS – Long term supported release**, is numbered with the abbreviation of "LTS"
- i) **Codebeamer releases on the roadmap or under development** are named by English women' names calendar- eg.: A(lice), B(etty), C(armen), D(orothy), E(mma) etc.- until its finally released and published.
- j) **Codebeamer releases published** are identified by the release date – eg. November 2020 is 20.11. For Example: \* CB 20.11 LTS\*\*\*
- k) **Service Packs are numbered** by 1...n and abbreviated as "SP". Service packs for certain releases are identified as eg.: CB 20.11 LTS - SP1
- l) **TÜV Validation:** versions validated by TÜV Nord and further related information can be found on the Intland webpage under the following [link](#).
- m) **Releases of codebeamer X** refers to any new version of Intland Software's products that delivers extended functionality, performance and usability improvements, and bug fixes with Angular frontend. In some cases, Intland Software may consolidate features due to global system improvement, resulting in the removal of certain features.
- n) **Codebeamer X is numbered** by 1...n and one decimal 1...n. eg: CB X 4.0, CBX 4.1.  
Change in the first number means significant new features or changes in the next release eg. CBX 3.0 to CBX 4.0...4.1.  
Change in the first decimal means minor improvements, usability development, bug fixing.

## Hosting services SLA

Intland defined Hosting Policies for AWS and MS Azure platforms. They are available under <https://intland.com/technicalsupport/>.

## General

This License will be governed by and construed in accordance with the laws of the Federal Republic of Germany and shall insure to the benefit of Intland and End-User and their successors, assigns and legal representatives.

If any provision of this License is held by a court of competent jurisdiction to be invalid or unenforceable to any extent under applicable law, that provision will be enforced to the maximum extent permissible and the remaining provisions of this License will remain in full force and effect. Any notices or other communications to be sent to Licensor must be mailed first class, postage prepaid, to Intland.

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and all prior proposals, agreements, representations, statements and undertakings are hereby expressly cancelled and superseded.

This Agreement may not be changed or amended except by a written instrument executed by a duly authorized officer of the Licensor.

## Notice

The Intland codeBeamer and Intland codebeamer X products are Copyrighted © by Intland Software GmbH. Intland, Intland codebeamer and Intland codebeamer X are trademarks of Intland Software.

The Software is available for use by end users according to the License Agreement. Any reproduction or redistribution of the Software not in accordance with the License Agreement is expressly prohibited by law and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent possible.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT

THE WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE LICENSEE ASSUMES ALL RISK AS TO THE SUITABILITY, QUALITY, AND PERFORMANCE OF THE SOFTWARE. IN NO EVENT WILL LICENSOR, OR ITS DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES, BE LIABLE TO THE LICENSEE FOR ANY CONSEQUENTIAL INCIDENTAL, INDIRECT, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA OR BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR ACCOMPANYING WRITTEN MATERIALS, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

LICENSOR'S LIABILITY TO THE LICENSEE (IF ANY) FOR ACTUAL DIRECT DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO, AND IN NO EVENT SHALL EXCEED, THE AMOUNT ORIGINALLY PAID TO LICENSOR FOR THE LICENSE OF THE SOFTWARE.

IN NO EVENT SHALL LICENSOR'S OR ITS DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES TOTAL CUMULATIVE LIABILITY TO ANY USER OR OTHER PARTY UNDER THESE TERMS OF SERVICE OR OTHERWISE EXCEED THE AMOUNT ORIGINALLY PAID TO LICENSOR FOR THE LICENSE OR SERVICE.