SERVICE LEVEL AGREEMENT (SLA)

1. GENERAL

This SLA is part of the cooperation between the Supplier and the Customer. It describes the agreed services and service level in the operational phase. If any significant defects occur which limit the Customer's use of the Solution, the Customer must be informed immediately.

The Supplier has subcontracted Hostnordic A/S to host the backend. The Supplier has dedicated servers at Hostnordic.

The agreement between Hostnordic and the Supplier includes a document similar to the present one which describes the agreed service level. The Supplier undertakes to keep the Customer informed about IT security issues that could significantly affect the agreement.

2. BASIC ASSUMPTIONS

The Supplier shall be responsible for delivering the agreed IT services at the agreed quality within the agreed timeframes.

In order for the Supplier to be able to deliver the agreed service, it is necessary that the users/Customer provide sufficient information, e.g. about bugs and errors, so the Supplier can detect and correct all errors. The following will therefore be prerequisites for the Supplier's ability to deliver the services at the specified levels:

- When an error is detected, it must be described to the Supplier as specifically as possible, e.g. stating the specific module, login details, customer number and as much relevant data as possible. If possible, the description should be supplemented with a screen shot.
- If more information is needed, the Supplier will contact the Customer directly. If the Customer is not available, the Supplier will inform the Customer that the case is registered as pending.
- After three unsuccessful attempts to contact the Customer over at least three days, the file will be closed in the helpdesk.

In order for the Supplier to be able to provide IT services (e.g. error correction) within the agreed timeframes, the Customer's representatives or stand-ins must be available to the Supplier. If this is not the case, the error-correction process will be extended.

When the Agreement is signed, the Customer must, in cooperation with the Supplier, appoint a super user who will be the Supplier's primary contact and communicate information from the Supplier to the Customer's users.

This super user should as far as possible serve as the liaison between the Customer's users and the Supplier.

3. SUPPORT

All questions from the Customer's users concerning the use and understanding of the Solution, as well as requests and error messages, should initially be directed to the Customer's super user, who will then if necessary contact InsuBiz Support (**IB Support**). However, all users may contact IB Support directly to report errors.

IB Support will register all enquiries and prioritise them according to the impact they have on the Customer.

In general, enquiries to **IB Support** should be made via email to support@insu.biz. Messages can be sent 24/7 but will only be responded to and processed during office hours. **IB Support** can also be contacted by telephone on +45 3699 0190 on weekdays from 9:00 to 15:00. In the case of error situations in which the response times set out in Section 6 must be observed, the above times may be ignored.

The Supplier's office hours are weekdays from 9:00 to 16:00 (GMT +1). 5 June, 24 December and 31 December are considered holidays.

The Supplier is not obliged to provide support for older versions. If the Customer does not follow the Supplier's request on upgrading administration programs when prompted, the Supplier will not accept responsibility or liability for the performance and operation of the system.

4. Change Management and development policy

The Supplier manages changes via a workflow that requires all changes to be approved before they are implemented.

The approval ensures that:

- all changes are done in the right way
- all changes are documented and can be traced back to their origin
- all changes are tested and approved
- the implementation disturbs users as little as possible, and
- there is a plan for quickly restoring normal operation if a problem occurs.

As a rule, the Supplier shall collect the changes and implement them in the set release periods, which typically take place 2 – 3 times per year. Before each period, a meeting shall be held to plan the coming period's tasks. Mid-period planning meetings shall also be held to assess the reported errors and requests.

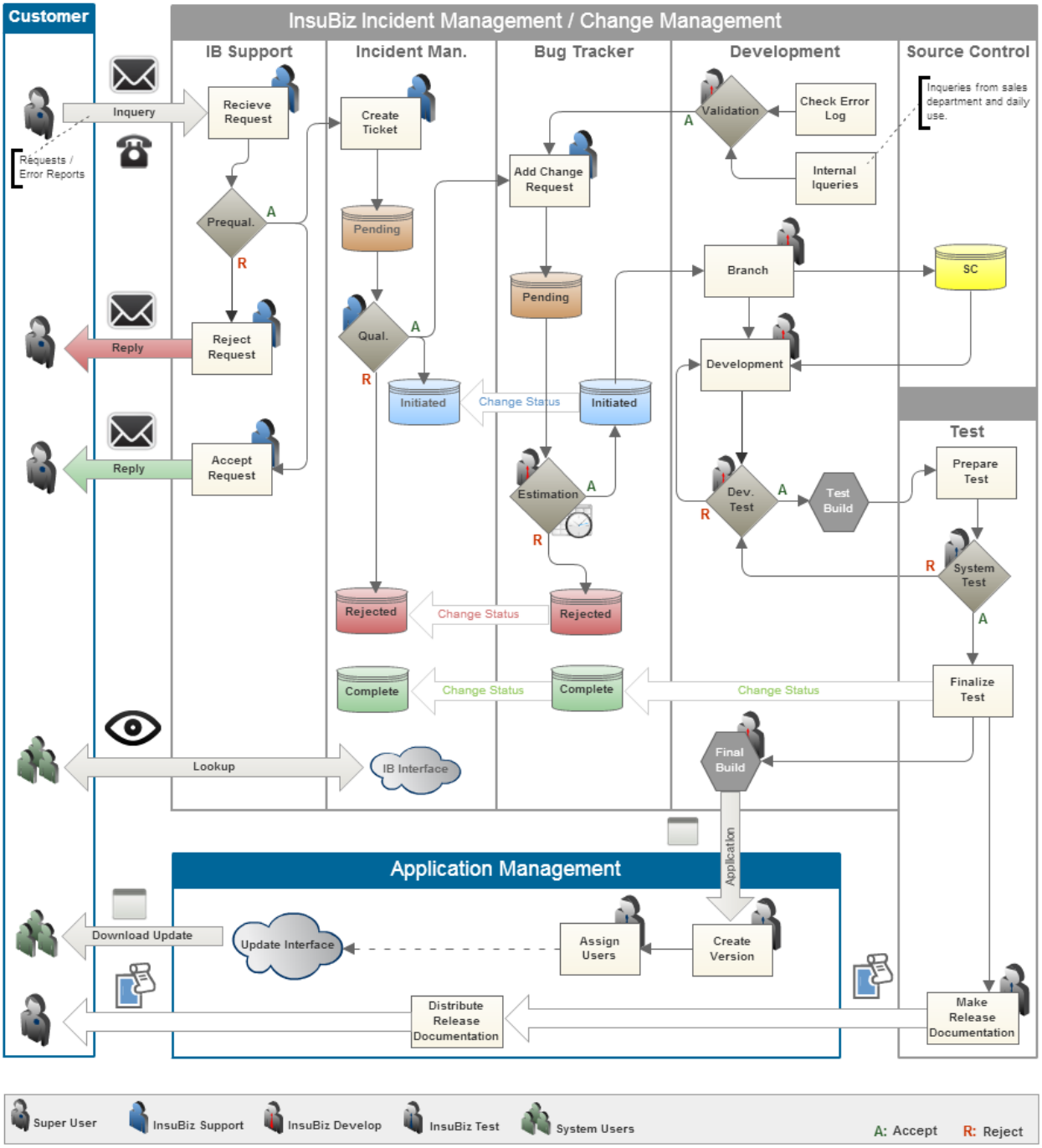
Information about significant system changes and releases shall be sent to the Customer per email.

4.1. CRITICAL CORRECTIONS

Critical corrections that are necessary for the Solution to continue to function or for the Supplier to comply with new rules or procedures may be made outside the prescribed intervals. As a rule, critical corrections shall only be made when there is a substantial reason why the change cannot wait until the next release.

The change-management procedures shall apply to all changes, error corrections, optimisations, critical corrections etc. that will affect the administration programs/web applications.

The following chart describes the change-management procedure in InsuBiz:



4.2. DEVELOPMENT POLICY AND UPDATES OF THE SOLUTION

The Supplier's development policy includes a policy on the continuous development of the Solution and the setup in which the administration programs run. The Supplier's main rule is that it does not develop customer-specific functions. A given function **must** be relevant to other customers, so that the Supplier can continue to maintain a single overall solution for all customers.

4.3. THE PRACTICAL PROCESS OF UPDATING THE INSUBIZ SOLUTION

The administration programs are updated through a central application manager. This ensures that the Customer has the correct applications in the latest versions. Installing and updating takes place through a transfer of encrypted zip files via an SSL-encrypted channel.

4.4. HARDWARE CHANGES

If the Supplier needs to upgrade the servers at Hostnordic and the system will not be available for a short period as a result, the Customer shall be informed in due time. The Supplier undertakes to schedule such upgrades at times when the system is least busy, typically on Friday afternoons and weekends outside normal working hours.

4.5. SERVICE WINDOWS AND PATCH MANAGEMENT

Service windows and patch management can affect the accessibility of the InsuBiz systems. InsuBiz will do the outmost to keep this inaccessibility to a minimum.

4.5.1. PLANNED SERVICE WINDOWS

InsuBiz has the right to effectuate planned service windows in connection with changes, updates and maintenance of hardware and systems on weekdays between 23:00 and 06:00 CET. InsuBiz will inform the customers main contact person about the planned service window via e-mail. A notice will be given 6 days before.

4.5.2. PLANNED PATCH MANAGEMENT

InsuBiz performs planned patching of approved updates for OS and server software every Thursday within the period from 03:00 to 06:00 CET. A separate notice will not be given for these updates.

5. DEFINITION OF ERRORS

Errors are broadly defined as faults in the Solution or other conditions that lead to a lack of access, with the result that the Customer cannot use the Supplier's administration programs/web applications for the intended purpose.

A distinction is made between:

1) **Errors caused by the Customer's circumstances or circumstances for which the Customer is responsible.**
   a) Lack of connection from the Supplier's administration programs/web applications to the Supplier's servers due to local conditions in the Customer's network or on the Customer's computers (e.g. firewalls, antivirus or other security software/hardware).

b) The Customer's hardware or software in the form of an operating system or other software components that the Supplier's administration programs/web applications rely on do not meet the system requirements specified by the Supplier.

c) The transmission speed between the Customer's computers and the Supplier's servers do not meet the system requirements specified by the Supplier due to conditions in the Customer's network or the Customer's internet connection.

d) The Customer's administration programs cannot obtain the necessary file permissions on the Customer's computer because the Customer's computer does not meet the system requirements specified by the Supplier.

e) Improper use of the Supplier's administration programs/web applications, leading to errors and possible derivative errors.

2) Errors entirely or partly due to conditions in the administration programs/web applications, backend or the parts of the data communication for which the Supplier is responsible.

a) Lack of connection from the Supplier's administration programs/web applications to the Supplier's servers due to conditions in the Supplier's network or on the Supplier's servers.

b) Error in the backend on the Supplier's/subcontractors' servers.

c) Error in hardware for which the Supplier is responsible, including hardware located at the Supplier's subcontractor(s).

d) The transmission speed between the Customer's computers and the Supplier's servers do not meet the system requirements specified by the Supplier due to conditions in the Supplier's network or the Supplier's internet connection.

e) Errors introduced in administration programs/web applications for which the Supplier is responsible.

General guidelines for the Supplier's handling of errors:

Re 1): The Supplier shall make itself available as much as possible to help remedy these errors. This work shall be paid pursuant to the applicable pricing agreement for support work.

Re 2): The Supplier shall be responsible for the correction of these errors within the response times defined in Section 6.

6. RESPONSE TIMES

Level	Description	Action	Response time	Solution time
1 Critical	Business-critical situation – none of the employees can do their work through administration programs / web applications. The Solution is not available or cannot be used. There is no possibility of a workaround.	Error report within the Supplier's normal working hours from 09:00 to 16:00 (GMT +1). Two-hour response time. Either a solution must be found within four hours or an action plan must be presented with agreed solution times. As long as there are users who are prevented from doing their work, remedying must proceed without undue delay, including outside normal working hours, until a solution is found or an action plan can be presented. If the error is reported outside the Supplier's normal working hours the Supplier must start solving the problem the following day.	2 hours	4 hours
2 Medium	Business-critical parts of the Solution cannot be used (e.g. the ability to report or process claims or carry out interface transactions).	Reporting in the Supplier's normal working hours from 09:00 to 16:00 (GMT +1). Eight-hour response time. Either a solution must be found within 12 hours or an action plan must be presented with agreed solution times. If the error is reported outside the Supplier's normal working hours the Supplier must start solving the problem the following day.	8 hours	12 hours
3 Low	Limited or minimal defect that does not affect critical business processes.	Standard management of error corrections and improvements.		The next update

7. CAPACITY MANAGEMENT/OPERATION MONITORING

Hostnordic shall be responsible for monitoring the operation and capacity of all system resources. If an overall capacity upgrade should become necessary and the system will not be available during the upgrade, all super users shall be informed in due time. The Supplier undertakes to attempt to perform such updates outside normal working hours.

8. CONTINGENCY PLAN

The Supplier shall be responsible for the development and maintenance of the Solution, while Hostnordic shall handle the operation of the Solution at a separate location. In case of critical incidents at Hostnordic, Hostnordic shall take the necessary operational measures to restore the servers and their connection to the internet according to Hostnordic's own contingency plan[1]. Other business-critical components of the system shall be dealt with by the Supplier according to the Supplier's plan.

The Supplier's contingency plan identifies a number of scenarios (critical incidents) that would affect the operation of the business-critical components and describes the procedures in light of these scenarios. It also contains a list of the employees in the crisis unit and a detailed description of their responsibilities and duties.

9. UPTIME GUARANTEE – REDUCTION OF THE ANNUAL OPERATION FEE

If the accessibility to the Customer's data throughout a calendar month is less than 99% Guaranteed accessibility measured over the whole calendar month, the Customer shall be entitled to receive a penalty payment as set out below, provided that the reduced accessibility is due to circumstances that are within the Supplier's control or for which the Supplier is responsible. Lack of access due to planned and necessary maintenance performed outside the Customer's normal business hours will neither be deducted from the Guaranteed nor the Actual accessibility in the statement. Outside interference (electrical outages, failure of third party/public data networks, etc.) resulting in non-accessibility in spite of the Supplier's and the Supplier's subcontractors' preparedness and compliance with their obligations pursuant to the Agreement, shall not be deducted from the Actual accessibility.

The Solution is considered inaccessible if it is subject to a level 1 or 2 error; cf. Section 6. The inaccessibility is calculated from the time the Supplier receives an error message from the Customer until there is no longer an error situation that can be categorised within Level 1 or 2. For each time the response time and/or solution time (cf. Section 6) is exceeded, the Calculated accessibility percentage shall be written down by an additional 0.5%.

The Supplier is required to register all known events that can be categorised within Level 1 and 2 (cf. Section 6) if these incidents are ongoing for more than 15 minutes, and to record all enquiries from the Customer regarding inaccessibility. Based on these records, after each quarter the Customer may request a statement of the quarter's events that have resulted in inaccessibility for the Customer. The Calculated accessibility shall be summed up and a possible penalty fixed.

The Customer is obliged to help rectify errors by participating either through representatives or deputies. When an error situation arises, the parties shall agree on the extent to which the Customer must be available. If an agreement is made and the Customer is not available for a period of time, and this is necessary for the error to be corrected, the Calculated accessibility rate shall be revalued by 0.5%.

[1] Hostnordic's contingency plan is available to read by personal enquiry at Hostnordic's head office.

The conditions for payment of penalties shall be set out in the Agreement between the Customer and the Supplier. If such conditions have not been defined, the Customer may claim a reduction in a future renewal of the Agreement in accordance with the following guide to the calculation of penalties. If the Agreement has been terminated, the penalty will be paid when the Agreement ceases.

Penalties shall be calculated according to the following formula:

The Calculated accessibility is calculated as follows: Actual accessibility/Guaranteed accessibility x 100. Then X% is subtracted for overrunning the response/solution time (see above). Then Y% is added for the lack of customer accessibility (see above).

For each percentage point or part of a percentage point that the Calculated accessibility lies below the Guaranteed accessibility, a penalty of 10% of the month's license fee shall be paid (total system costs per year divided by 12). A month's penalty may not exceed that month's license fee.

Example:

A customer pays DKK 100,000 per year, i.e. DKK 8,333.33 per month, and in one month an Actual accessibility of 96% is provided, the response time is exceeded once in two cases, and the Customer is unavailable in one case.

Estimated accessibility: (96/99 x 100) – (0.5 + 0.5) + (0.5) = 96.46%

This is three percentage points lower than 99.

The penalty can be calculated as follows: 3 x 8,333.33 / 10 = DKK 2,499.99

10. AUDIT REQUIREMENTS

As part of the operation documentation, the Supplier shall submit an annual assurance report prepared by an approved auditor auditing the IT general controls which are relevant to the service provided to the Customer. The controls must be planned, carried out and reported in accordance with ISAE 3402.

Audits at the Supplier must be extensive enough to allow the auditor to make conclusions in the certification about the overall security of the system, data and operation in relation to the Supplier's services to the Customer. The IT general controls are divided into the following categories:

1. Outsourcing, including security backups, physical security, external agreements and operation and capacity monitoring
2. Information security policy
3. User training
4. Telecommuting
5. Physical access control
6. User administration
7. Logical access control
8. Management of input and output data
9. Data communication

10. Logging
11. Change management
12. Termination/expiry of employee contracts
13. Incident management
14. Contingency plan

The audit shall be based on the partial-auditing method in relation to those parts of the IT services that the Supplier has outsourced to the Subcontractor that hosts the Solution. Thus the assurance report shall not include the Subcontractor's controls, but only the controls at the Supplier which monitor the Subcontractor's functionalities, including its ISAE 3402 assurance report.

The audit shall not include aspects relating to security and the control environment that the Customer maintains and manages itself.

The Supplier's audit period follows the calendar year. The Supplier's ISAE 3402 report must be submitted no later than 31 January in the following calendar year (Danish version). An English version follows in February. The Supplier's assurance report must include the Subcontractor's ISAE 3402 report for the period from 1 December to 30 November and a statement by the Subcontractor's management for December. These must be included in the report according to the partial-auditing method described above.

Upon request, the Customer may obtain a draft (only in Danish) of the Supplier's ISAE 3402 assurance report in mid-December.

11. SECURITY POLICIES

The Supplier's information security policy is a fixed part of this Agreement, but can only be obtained on request.