HALOPV

SERVICE LEVEL AGREEMENT

FOR CUSTOMER

AGREED SERVICE LEVELS

Index of delivered services

The following list of service deliverables will be provided during the term of the Agreement

A.1 Customer support - Handling of incidents and service requests

A.2 Bi-annual upgrades and intermediate patching

A.3 Infrastructure management

A.4 User reviews and configuration reviews

A.5 Governance and meetings

The indexed items are further explained in the following;

A.1 Customer support – incidents and service requests

The following support services are issued for the customer:

Request Type	Response time	Resolution time	Description
Major incidents and Security incidents	< 2 hours	< 8 hours	The application or a critical part hereof is not useable, and no useable workaround exists. Security incidents are always handled as major incidents. Platform/System down incidents are covered by separate 24/7 agreement, see RPO/RTO section. Major incidents and Security Incidents are always prioritised at the highest and every event is sought resolved with minimum impact for the users
Minor incidents	< 6 hours	< 2 days	Incidents where non-critical areas are not working - or where a useable workaround exists
Standard Service Requests	< 6 hours	< 2 days	Pre-defined service requests / configuration updates as defined below: List values, workflow tasks and task actions and notifications. GDPR requests for backend extraction, physical deletion etc. User management, including new/delete user and user roles. (no limit of request volume)

			Tabular report and dashboard changes (max. 4 reports/dashboard updates per month) Standard service requests do not cover building new workflows or setting up fundamentally re-designed workflows, this is to be considered a Non-Standard Service Request.
Non-Standard service requests (Changes)	< 24 hours	[Assessed per change]	Within 24 hours an assessment and estimate or handling the change is provided. Resolution time depends on the change type (e.g. new validation requirements etc.) Non-standard service requests may lead to chargeable work, if outside the agreed services, i.e. as a Service Order
Time calculation			
Response (work on incident resolution initiated) and resolution times (resolution of the incident) is calculated as actual working hours since incident reporting.			
Time pending customer and non-business working hours (as defined in the SLA) is not included in the time calculation ("Stops the clock")			

Insife guarantees the following service levels in excess of 90% of incidents and service requests and strives for 100% of major and security incidents. The service delivery metrics will be maintained by Insife and provided to the Customer quarterly, timelines aligned with Governance and meetings section

A.2 Bi-annual upgrades and intermediate patching / security patching

Update type	Notice period	Description
Major upgrade	60 days before	Major upgrades are delivered two times per year. Typical upgrade schedule will be to release a new version in May and November. Release notes will be published no later than 45 days before release, i.e. 15 days after first notice together with a Customer-specific impact assessment that includes a traceability to changed user requirements and an overall risk assessment for the Customer environment. Specification, evidence of validation activities etc- will be provided at release time to the Customer, including the following list of validation deliverables: - Validation plan

		- Installation Qualification Combined Protocol/Report including test cases, test results and deviations - Operational Qualification Combined Protocol/Report including test cases, test results and deviations - Standard Configuration Item List - System Specification - User Requirement Specification - Tabular report specification - Automation specification - Validation report - Traceability Matrix - Customer-specific Configuration Item list(s)
Scheduled Maintenance of patch / security updates	10 days before*	Patch / security updates are delivered upon identified need. Patch updates may fix bugs or other technical issue and is defined by not impacting user requirements. Insife will conduct maintenance with due warning. Emails will be sent out by the Insife Service Desk confirming the scheduled outage. The email will contain high level information on the scheduled outage. Emails will also be sent out at the completion of the scheduled outage.
Emergency Maintenance of patch / security updates	*While standard notice period is 10 days, some security patches may be implemented with retrospective notice, as per the Insife hosting team's assessment of the patch	Emergency maintenance and any resulting HALOPV Web Site downtime, instability or insecurity will be communicated to Customer as the need for said maintenance is identified.

A.3 Infrastructure

Item	Description
High Availability, Disaster Avoidance and Disaster Recovery	Insife's HALOPV infrastructure environment is designed for high availability and disaster avoidance, by utilizing best-in-class infrastructure from AWS, configured to meet expectations of critical operations. Insife's Disaster and Recovery Plan shall contain disaster avoidance procedures designed to maintain the availability of the SaaS Services and to safeguard Customer Confidential Information and Customer Data. Insife shall perform disaster recovery testing at least once every twelve (12) months unless Customer determines testing is not necessary. The testing shall include, but not be limited to, testing of hardware, installation and operation of Insife's network, conversion of customer data, processing of data and generation of reports, and testing of telecommunications facilities. Insife will provide notice to Customer in the event any material changes are made to any of Insife's Disaster Avoidance or Disaster Recovery plans within seven (7) days of any such material change being implemented.
Operations Interruptions	In the event of any unplanned interruptions of the operations of the HALOPV application, Insife shall use its best efforts to restore the HALOPV customer to Customer as expeditiously as possible. Complete availability interruption shall be treated as a Major Incident.
Infrastructure, Layered Software and Operating System Management	Insife's hosting services includes the setup, maintenance, monitoring, service desk and logical security of the computing environment necessary to meet our obligations under this SLA including: • Infrastructure maintenance, monitoring and problem resolution • Operating system and layered software maintenance including patching, upgrading, monitoring and problem resolution • Keeping all operating systems, web servers, layered software databases and firmware used to support the provision of services at commercially reasonable patch levels for security. Lower patch levels, such as firmware, RDS service etc. are managed by AWS. Any patching performed by Insife shall follow notice periods as described in A.2

Service Vulnerability Assessment	Customer reserves the right to conduct website vulnerability assessments against the specific systems presenting Customer's data, within seven business days advance notification and coordination with Insife network operations personnel. Material vulnerabilities that can reasonably be repaired or mitigated will be done so by Insife personnel at no cost to Customer. Insife shall not permit unauthorized persons or entities to access any Insife computing systems or networks utilized to provide services to Customer hereunder without Customer's express written authorization, and any such actual access will be undertaken solely in conformance with such authorization.
System Usage	System capacity and resources will be maintained and monitored for registered users of the system. Insife will monitor System Performance and Uptime and review at least monthly.
Response Time and Performance	Insife will provision the necessary infrastructure to deliver performance for the licensed number of users, in accordance with this SLA. The following performance levels will be adhered to: • HALOPV front page will load within 5 seconds • HALOPV dashboard page will load within 5 seconds • HALOPV forms will load within 5 seconds • HALOPV reports will load within 30 seconds General network issues and other issues not related to the HALOPV application are outside of the responsibility of Insife. Performance incidents are investigated and actions are brought to Customer as per A.5 Governance and meetings
Database and Infrastructure Availability and Monthly System Uptime	The system will be available 24 hours a day, 7 days a week with the exception of scheduled maintenance and downtime. The Monthly Uptime SLA is 99.5%. This will be reported to Customer quarterly, in alignment with A.5 Governance and meetings Monthly Uptime is calculated (scheduled minutes – unscheduled minutes) ÷ scheduled minutes * 100
System capacity management	Planning and monitoring the growth of the system and maintaining performance levels in SLA. Analysis and actions are brought to Customer as per A.5 Governance and meetings

Backup/Recovery Point Objective	A full backup of the data is performed at least nightly every twenty-four (24) hours. The backup data is stored within the AWS RDS service, in Frankfurt, Germany Backups are retained for 45 days. The Recovery Point Objective (RPO) SLA for this SLA is six (6) hours. The database solution is furthermore mirrored, leading to an expected performance of no data loss.
Recovery Time Objective	In the event of a disaster, Insife will recover the Hosted Services within a 6-hour period (RTO). Customer Content will be recovered from the latest nightly backup that is available / or from mirrored database service.
Audit Logging	Insife will monitor and log all logins to the Hosted Services and periodically review the underlying audit trail (at least monthly). The audit trail for log ins and login attempts is available for any Customer user with Application Management role.

A.4 User reviews and configuration reviews

If agreed in the SoW (optional service), Insife will conduct User reviews and configuration reviews for the Customer on an annual basis. The reviews will contain the following information at a minimum:

Item	Description
User Review Report	- Comparison of user accesses granted / revoked in the Customer user administration tool or log, with the HALO user accesses granted / revoked. Any discrepancies will be accounted for - Specific section on privileged accounts - Concluding on the effectiveness of the user management process for the application - The report will be delivered in accordance with Customer's QMS requirements and will be provided every January

Configuration review report	- Verification of the configuration items as per system CIL in order to obtain confidence of the system's configuration control state - Concluding on the effectiveness of change controls - The report will be provided every January

A.5 Governance and meetings

The following meetings are offered by Insife:

Meeting	Timeframe	Objectives	Participants
Executive Committee (SC)	As needed	▪ Overall Account Status ▪ Manage risks and escalations ▪ Future roadmaps	▪ Customer Data Owner ▪ Customer System Manager ▪ Insife Account Manager ▪ Insife Service Delivery Manager
Service Management Meeting	Quarterly	SLA metrics: ▪ Incident / Service request Trend analysis ▪ Incident / Service request prioritization ▪ High priority Incident / Service request review ▪ Findings from System usage (capacity, availability) and audit logging reviews (as relevant)	▪ Customer System Manager ▪ Insife Service Delivery Manager ▪ Insife Account Manager

Operational	Ad hoc	▪ Discussion on specific tickets if needed	▪ Customer System Manager ▪ Insife Service Delivery Manager / representative

Escalation Paths

The following escalation paths have been agreed:

Level	Customer Representative	Insife Representative	Categories
1	Customer System Manager	Insife Service Delivery Manager	▪ Support incidents ▪ Change Request prioritization
2	Customer System Manager	Insife Service Delivery Manager	▪ Process Deviations and non-compliance ▪ Support incidents not resolved
3	Customer Data Owner	Insife Account Manager	▪ Unresolved major incidents ▪ Business Performance issues ▪ Items requiring stakeholder involvement