

XiltriX International B.V.

Service Level Agreement

XiltriX Resilience: service desk, incident handling, monitoring of the service, system availability and management of monitoring data.

In force from 1 September 2026.

Contents

1. Purpose and scope
2. Definitions
3. Service desk and availability
4. Priorities and response times
5. Monitoring of the service
6. Availability
7. Back-up and recovery
8. Change and version management
9. Data integrity and retention
10. Hosting, connectivity and security
11. Exit and destruction of data
12. Reporting and evaluation
13. Roles and responsibilities
14. Emergency procedure
15. Exclusions
16. Rates outside office hours
17. Calibrations
18. Order of precedence of documents

1. Purpose and scope

This service level agreement (SLA) describes the service levels that apply to customers with a valid agreement for the use of XiltriX Resilience (hereinafter: the system): the availability of the service desk, the handling of incidents, monitoring of the service, the availability of the system, and the management of monitoring data.

The services in this SLA are part of the XiltriX Resilience portfolio: monitoring, alarming and reporting fall under Intelligence; installation and commissioning, validation, maintenance, support and calibration fall under Care.

The service levels in this SLA apply from three months after delivery of the system. This stabilisation period gives the parties room to fine-tune settings, escalation paths and reporting procedures.

Customer-specific arrangements are recorded in an addendum to the agreement and take precedence over this SLA. The order of precedence of all contract documents is set out in article 18.

Boundary of responsibility: XiltriX detects deviations, raises alarms and escalates according to the agreed structure. The substantive assessment of monitoring data and the follow-up of alarms always remain the responsibility of the customer.

2. Definitions

- Agreement: the agreement concluded between the parties (the accepted proposal with addenda) of which this SLA forms part. Terms such as customer have the meaning given to them in the agreement.
- Office hours: Monday to Friday from 08:30 to 17:00 CET/CEST, excluding Dutch public holidays.
- System: XiltriX Resilience as installed at the customer and described in the agreement.
- Monitoring data: all data collected and processed by the system, including measured values, metadata and the audit trail.
- XiltriX engineer: an engineer directed and certified by XiltriX, regardless of whether they are employed by XiltriX or work for XiltriX as a partner.
- Incident: a fault or deviation in the operation of the system, reported by the customer or identified through monitoring of the service.
- Initial response time: the time between the reporting of an incident and the first response from XiltriX to the customer. This is a response time, not a resolution time.
- Exit: the termination of the agreement, whereby the customer is entitled to the transfer of the monitoring data and to its permanent destruction by XiltriX.
- Uptime: the availability of a service, expressed as a percentage of the available time relative to total time, measured per contract year, excluding a force majeure situation as described in article 13.6 of the XiltriX general terms and conditions and planned maintenance and outages in external systems and systems over which XiltriX cannot reasonably exercise control, including the customer's IT infrastructure and internet connections.
- Planned maintenance: work announced in advance by XiltriX that may cause temporary unavailability.
- RPO (recovery point objective): the maximum data loss in the event of a recovery action, expressed in time.
- RTO (recovery time objective): the maximum time within which a recovery action is completed.

3. Service desk and availability

- The service desk can be reached during office hours on +31 73 521 0040 and at support@xiltriX.com, for faults and technical questions.
- Outside office hours, the service desk can be reached by phone for urgent incidents.
- A numbered ticket is created for every report. The customer receives this ticket number and is kept informed of follow-up and handling through the ticket. On request, XiltriX provides an overview of all of the customer's tickets.
- Urgent incidents are put through directly to a XiltriX engineer. Non-urgent reports are picked up the next working day.

- Incidents are reported by authorised contact persons of the customer (a maximum of three, recorded in the agreement).

4. Priorities and response times

Incidents are classified into three priorities upon reporting. Incidents arising from monitoring of the service (article 5) follow the same classification and response times.

Priority	Description	Response time
Priority 1 (critical)	Immediate data loss, or no access to the application for the entire organisation	30 minutes, 24/7
Priority 2 (medium)	Fault in parts of the application or the data storage	4 hours
Priority 3 (low)	Minor impact or urgency, for example a workable workaround is available	16 hours

- The target for the initial response time is 30 minutes. XiltriX monitors this response time. XiltriX will make every effort to meet each response time within the stated norm. However, due to specific circumstances it may happen that certain response times are not always met. Other response times, by contrast, will often be met well ahead of target. We therefore measure this on an annual basis as service levels, in line with the annual operational review described in article 12.
- Incidents are resolved remotely wherever possible. XiltriX has a secure connection to the system that allows the XiltriX engineer to view it directly, so that a diagnosis can be made quickly.
- If an incident cannot be resolved remotely, a XiltriX engineer will intervene on site. The response time for an on-site intervention is, on average, a maximum of 12 working hours after the report, measured retrospectively over a contract year.
- On-site support is provided between 08:00 and 21:30, seven days a week, taking travel time into account.
- For non-serious incidents, no on-site deployment takes place outside office hours. An incident is not serious as long as measurement data continues to be processed and stored and alarms continue to be reported, for example if a single door sensor fails while temperature logging continues.
- A XiltriX engineer is at all times accompanied on site by the customer, in particular outside office hours.

5. Monitoring of the service

- For systems hosted by XiltriX, continuous monitoring of the critical infrastructure is included as standard. The purpose of this monitoring service is to ensure that a fault does not go unnoticed.
- If a disruption of the monitoring modules lasts longer than 20 minutes, it is escalated internally and a XiltriX engineer is engaged to resolve the incident remotely. If the incident cannot be resolved without the customer's cooperation, the XiltriX engineer will contact the customer. Disruptions resolved by XiltriX itself are reported to the customer afterwards by e-mail.
- Alarm delivery time: a validated deviation is sent as a first notification to the designated user within 60 seconds of being established.
- For as long as a technical fault or a threshold breach persists, a repeat alarm is sent to the designated user at least once every 15 minutes.

6. Availability

- The processing and storage of measurement data is continuously available with an uptime of 99.9% per contract year (a maximum of 8.76 hours of unavailability per year). Planned maintenance and outages in external systems, including the customer's IT infrastructure and internet connections, do not count towards the uptime calculation.

- The user interface of the application is continuously available with an uptime of 95% per contract year. Planned maintenance and outages in external systems, including the customer's IT infrastructure and internet connections, do not count towards the uptime calculation.
- The availability achieved is demonstrated in the annual service management report (article 12).

7. Back-up and recovery

- XiltriX uses multiple environments and back-ups so that, in the event of an outage, the system is restored in accordance with the RPO and RTO set out below.
- A recovery action results in the loss of a maximum of 30 minutes of data (RPO).
- A recovery action is completed within 24 hours of a disaster or a request for recovery (RTO).

8. Change and version management

- XiltriX classifies every change on the basis of a risk and impact analysis. The release method is determined on that basis.
- Release documentation consists of: release notes, risk classification and validation documentation.
- Updates to the application and the system are installed remotely within an announced maintenance window. XiltriX announces a maintenance window at least two working days in advance; the customer's consent is not required for this.
- For changes with a high (security) impact, XiltriX reserves the right to roll these out immediately without prior notice. The customer is informed immediately afterwards.
- Historical monitoring data remains readable and viewable in the application under new software versions. A change in functionality never means that previously recorded data becomes inaccessible.

9. Data integrity and retention

- Stored monitoring data is read-only and cannot be altered, not even by employees of the customer, XiltriX or the hosting provider.
- Where changes do nevertheless take place at data level, an audit trail is maintained in which individual users are traceable.
- The audit trail is accessible to the user; a specific change can be located within 10 minutes.
- Reported electronic data is archived in a protected location and remains readable and accessible via the user interface for the duration of the data's lifecycle, for a minimum of ten years.
- The data is at all times located within the European Economic Area.

10. Hosting, connectivity and security

- The system runs on AWS in the eu-central-1 region (Frankfurt am Main). The hosting provider is ISO 9001 and ISO 27001 certified. Should a fallback region be required, an AWS location within Europe will be selected.
- Where XiltriX provides connectivity, this includes a 4G connection as a fallback alongside the primary internet connection.
- WhatsApp is used as standard for notifications of deviations. If a customer opts for SMS/RCS, separate arrangements will be made for this in view of the higher costs.
- Fair use 4G: the system may run on 4G as the primary connection for a maximum of one month per contract year. In the event of structurally higher usage, XiltriX reserves the right to charge the additional costs, after prior notice to the customer.
- The data centre has facilities for uninterrupted service, including emergency power, redundant data traffic, physical and digital security, and climate control.

- Users of the customer and of XiltriX log in with a business but personal account. The audit trail in the application is switched on.
- Administrators of the hosting provider cannot make changes to the stored data.
- A log is kept of work carried out by XiltriX and the hosting provider on the application, database and system, making all work traceable.
- The customer may carry out an information security audit. Cooperation with regard to the hosting provider is limited to public documentation on certifications and mitigating measures; the data centres themselves are not subject to audit. In the case of such an audit, the customer must notify XiltriX in good time and, if necessary, provide the appropriate documentation demonstrating that (i) the auditor's independence is safeguarded, (ii) the auditor acts confidentially in line with XiltriX's wishes, and (iii) the auditor will not include in the report any information that XiltriX considers confidential, partly in view of (other) XiltriX customers and the protection of confidentiality in that regard. The audit must in all cases remain limited to what is strictly necessary, and XiltriX must verify the report before the auditor is authorised to provide it to the customer. Any costs associated with the audit, including the work XiltriX is required to perform, are for the account of the customer.
- For work carried out on site, the customer provides safe access to the installation, the materials needed to comply with applicable safety regulations, and access to the areas where the equipment is located.

11. Exit and destruction of data

- Upon exit, operational and archived monitoring data can easily be extracted from the application, in a format that is readable and usable without the application.
- The data is transferred in this format within 30 days of a request from the customer.
- After termination of the contract and after the customer has confirmed acceptance of the received data, all data, including back-ups, is permanently destroyed within 30 days. XiltriX provides proof of destruction.
- Permanent destruction after the retention period takes place only at the customer's request, subject to statutory retention periods, in accordance with the XiltriX Information Retention Policy (part of the ISO 27001 management system).
- Without prejudice to the provisions of this article, XiltriX retains the right to use and commercialise aggregated and anonymous or anonymised monitoring data for the purposes of innovation and the further development of its own products and services, provided that after exit this data can no longer be traced back to the customer or individual users, and in line with the mandatory statutory obligations that apply in this regard.

12. Reporting and evaluation

- A service management report is prepared annually, containing: serious disruptions with explanation, availability achieved with explanation, an overview of support tickets, and the changes carried out. In the event of major disruptions or incidents, an interim report follows.
- The parties maintain a consultation structure at three levels: operational (service desk, incidents and changes), tactical (account management, reports and service levels) and strategic (escalation and long-term development).
- The service levels are evaluated annually in the annual operational review, unless the parties agree on a different frequency.

13. Roles and responsibilities

Party	Responsibilities
XiltriX	Supply and maintenance of XiltriX Infrastructure (hardware such as monitoring stations, sensors and gateways, connectivity including 4G fallback connection), XiltriX Intelligence (data storage and application, updates to the application and system, monitoring of the service, back-ups of monitoring data and snapshots of the system).

Party	Responsibilities
Hosting provider	Infrastructure and system of the data centre, physical and technical security, emergency facilities.
Customer	Network connections and power supply on site. Internet access in accordance with the agreement. Access to rooms and equipment. Substantive assessment of the monitoring data and follow-up of alarms. Having and maintaining an up-to-date emergency procedure.

14. Emergency procedure

XiltriX makes every effort to resolve every incident as quickly as possible. For the exceptional situation in which this is not immediately possible, every customer has its own emergency procedure. To be able to provide adequate support during a disaster, XiltriX is informed of this emergency procedure.

15. Exclusions

The following matters fall outside the scope of the agreement. Costs arising from these are for the account of the customer.

- Cosmetic maintenance (cleaning).
- Recalibration and revalidation, unless included in the agreement.
- Preventive and corrective maintenance of components not supplied by XiltriX.
- Waiting hours outside XiltriX's sphere of influence.
- Deployment of a cherry picker or other non-standard equipment.
- Work involved in the airlock entry, exit or cleaning of goods (cleanroom procedures) required to be able to carry out the work.

16. Rates outside office hours

- For work carried out outside office hours on working days, a surcharge of 150% applies to the prevailing hourly and call-out rates of €176 and €350 respectively.
- On weekends and public holidays, a surcharge of 200% applies.

17. Calibrations

- Calibrations of the system are carried out exclusively by certified XiltriX engineers or by partners certified by XiltriX. The costs of certifying external parties are for the account of the customer.
- The customer makes the sensors accessible and, where necessary, moves any samples or materials present itself. XiltriX engineers are not authorised to move or remove the customer's samples and will under no circumstances do so.
- If the customer does not follow XiltriX's recommendations for calibration and validation and/or does not have calibrations performed by XiltriX or by a partner certified or approved by XiltriX, XiltriX's guarantees and agreed service levels will not apply, as these are conditional on calibrations being carried out correctly.

18. Order of precedence of documents

In the event of a conflict between documents, the following order of precedence applies, with a document listed higher taking precedence:

1. The agreement (the accepted proposal) together with the accompanying addenda. In the event of a conflict between them, the most recent addendum prevails.
2. This service level agreement.
3. The XiltriX general terms and conditions.

If a data processing agreement has been concluded between the parties, it takes precedence over the above documents with regard to the processing of personal data.