DAKTEL GROUP

DAKTEL CLOUD SERVICES

Security & Resilience Overview

How Daktel Cloud Services is built, secured and kept available – the architecture, access control, container hardening, data security, backup and recovery, and the way every device authenticates to the platform.

VERSION	DATE	CLASSIFICATION
1.2	**OCTOBER 2026**	**FOR CUSTOMERS & PARTNERS**

AT A GLANCE

Built to stay up, and to stay closed.

Daktel Cloud Services (DCS) is the platform behind the Daktel ecosystem: every home, every watch and every call flows into it, GNI reads it, and the response centers act on it. This overview sets out how the platform is run and protected. The figures are Daktel's operating standards; the sections follow the questions a security review usually asks, in the order it usually asks them.

99.999%

availability of the portal and the sensor-data systems – up to six minutes a year

4 × daily

database backups, every six hours, in several regions and with several providers

AES-256

encryption of sensitive fields, records and databases at rest; TLS 1.3 in transit

Zero trust

physical and digital MFA, segmentation, strict permissions – management from two locations only

01 **Architecture & control**

02 **Access & identity**

03 **Containers & hardening**

04 **Data security**

05 **Backup, availability & recovery**

06 **Devices & connectivity**

01

Architecture & control

One control system, no single provider.

A central control system	Daktel Cloud Services (DCS) is run by a central control and monitoring system. It monitors, processes and forecasts cases, manages versions and code distribution, issues and distributes certificates, and monitors and manages the databases.
Built in-house, hosted anywhere	The system and its components are developed and maintained internally, with the support of Cloudflare, and integrate fully with the cloud services of AWS, Google Cloud, Microsoft Azure, DigitalOcean and other DNS and CDN providers.
Portable in a crisis	In a disaster or “chaos” situation, the containers – some of them, the sub-services running with a provider that has gone down or stopped serving a region, or in exceptional cases the entire architecture – can be copied to any other provider in a limited time, depending on the affected system.
Two DNS providers	A secondary DNS provider (IBM NS1) keeps the DCS portal reachable even when the primary provider (Cloudflare) is unavailable. AXFR queries keep the DNS records synchronised between both providers at all times.

02

Access & identity

Two locations, every factor, no shortcuts.

Management access	Access to and management of the systems is possible from two locations only – London and the Czech Republic – with physical and digital multi-factor authentication, segmentation, user control and strict permissions on a zero-trust basis.
Signing in to the portal	Users sign in with an email address and password, a reCAPTCHA check and a second factor: a six-digit code sent to the mobile number registered by the system administrator.
New devices and brute force	A login from a device the system does not recognise sends the user an email with the details. A rate limit caps the number of failed attempts, so repeated or brute-force login attempts are stopped.
Databases	Connecting to a database requires multi-factor authentication – a username and password combined with x.509 certificates – plus further parameters defined by Daktel. Role-based access control (RBAC) governs access at database and record level, and IP whitelisting and virtual private networks limit where a connection can come from.

03

Containers & hardening

No command line, no open ports, no public libraries.

Everything runs in containers	All Daktel Cloud services run in containers customised for the central system: full isolation from system processes, image-based deployment, version handling and recovery, multi-container support, scalability, virtualisation and high-performance packet inspection.
Continuously watched	The containers keep a continuous connection to the central security systems, which monitor them and hold their current status. Frequent health checks from several regions verify the availability of Daktel's systems in every critical area of activity.
No attack surface to speak of	The containers have no command-line interface, so they are not directly exposed to surface attacks. Once a container is installed and its firewall and security measures are configured for its service, user permissions and processes such as SSH and FTP are stopped and removed. Access is possible only in a controlled way through the system; no unused port is open, and direct or remote access to the servers is not possible.
Trusted libraries only	Development libraries are not updated from public sources such as npm. Versions tested by Daktel are stored in an internal, trusted repository and imported from there by the containers as needed.
Secure development	Development is supervised to prevent common vulnerabilities such as injection attacks and insecure configurations. Employees are trained regularly, and Daktel stays current with vendors such as MongoDB and Redis on security features and best practice.

04

Data security

Encrypted, monitored, masked.

In transit	All services use HTTPS. TLS 1.3 is the standard protocol, with TLS 1.2 as the fallback when a client does not support it; a small number of point services that require it are limited to TLS 1.0.
At rest	Fields, records or entire databases classified as sensitive – by the systems or by the end user – are encrypted in the database with AES-256.
Kept current	The databases are updated regularly to the latest version, so security patches apply at both database and operating-system level.
Monitored	Daktel monitors database activity for compliance and security, and runs Database Activity Monitoring (DAM) to analyse that activity for threats.
Outside production	Development and testing that involve sensitive information are done on masked and anonymised data, so nothing is disclosed outside the production environment.
Retention	Sensor data is not deleted from the systems. Subscriber data can be deleted by the users of the portal.

05

Backup, availability & recovery

Six minutes a year.

Backups	Every Daktel Cloud database is backed up every six hours – four times a day – in several regions and with several providers at the same time. Storage servers are backed up hourly or every twelve hours, depending on the data. Source code, software, components and configurations are backed up online and offline and synchronised frequently. All backups are stored globally, so the loss of a single location loses no data.
Availability	The portal, its interfaces and the sensor-data collection systems are classified as critical and run at 99.999% availability – up to six minutes of downtime a year. Other core components are classified internally: 99.999% for critical services, about 99.98% (up to one hour a year) for regular services, and 99.97% (up to two and a half hours a year) for supporting services.
When a database is unavailable	Processed alerts from the sensors are written locally by a high-performance, mmap-based service. If the responsible database is unavailable, the service checks its availability and writes everything it holds as soon as the database is back. If that service is itself unavailable, the main service allocates memory, uses an equivalent engine of its own and writes the alerts to a local file, to be saved in processing order once saving is possible.
Before an error happens	If a database becomes unavailable for any reason, the systems that monitor it notify Daktel's response system immediately – before any read or write is attempted – so an automatic routine or a person can act before data is at risk. If the local saving processes fail despite the database being available, an alert in the control systems calls for human intervention and a review of the processed data.

06

Devices & connectivity

Cellular, certificated, verified on every connection.

Cellular for data, Wi-Fi for position	The devices are SIM-based and communicate over cellular networks (3G/4G/5G by device version), so they stay available in a power outage, when the home network is down. Data never travels over the subscriber's Wi-Fi. Wi-Fi is used for positioning only: indoors, the X10 reads nearby access points – the home's included – and needs at least three for a reliable position inside a building; outdoors it uses the global satellite networks.
Verified on every connection	Before every connection – a new registration, or a device switched off and on – the device passes a series of checks against its authentication services.
X10 Smart Care Watch	The X10 series uses a TLS socket. Keys and certificates are issued to the device during registration by an internal protocol and renewed on a schedule set per device by a certificate-management system – a new device leaving the factory carries no built-in keys or certificates that would give it access to the systems.
Safe Home hubs	The PM hub series uses a TCP/IP socket; its security and authentication process is blockchain-based, with further parameters defined by Daktel to ensure a trusted connection.
Fallback channels	Every device version has backup protocols – HTTPS and SMS – for downtime and for situations where reception is not enough for a stable connection or for data transfer.
Two-factor registration	Registering any device that connects to the systems or their applications requires two-factor authentication by the end user.
From the device to the center	The services a device connects to verify the communication and the authenticity of its data against defined protocols – to manage resources and to spot abnormal connections or faulty devices. From there the data goes over TLS, Pub/Sub and WSS to the distribution and notification systems, where it is processed, stored and passed to the response centers.

CONTACT

Questions about this document?

For security questionnaires, tender documentation or a technical review with Daktel's engineering team, write to **support@daktelgroup.com**.

INTELLECTUAL PROPERTY

All intellectual property rights in and to DAKTEL CLOUD SERVICES, including all content, software, designs, documentation and related materials, are and shall remain the exclusive property of DAKTEL CLOUD SERVICES and platform.

© 2026 Daktel Group. This document describes Daktel Cloud Services as operated at the date above and is provided for information to customers and partners. Operating standards are reviewed and may change; the current version is available from Daktel on request.