

Disclaimer

Legal disclaimer

This guide and its contents (the "Guide") are provided by NXGEN. All rights to the Guide and to the intellectual property embodied in it — including, without limitation, trademarks, trade names, logos and similar marks appearing in or on it — are protected by law. All right, title and interest in the Guide and in any related intellectual property rights belong to and remain with NXGEN and its licensors.

The Guide is provided free of charge, "as is" and for informational purposes only, without warranty of any kind. It is neither intended nor suitable to establish any legal relationship between the reader and NXGEN or its affiliates, including, without limitation, any obligation of NXGEN or its affiliates toward the reader.

The obligations of NXGEN and its affiliates in respect of NXGEN products or services purchased by a customer are governed exclusively by the terms of the agreement under which those products or services were purchased.

For clarification

The reader bears the entire risk as to the use, results and performance of the Guide. To the fullest extent permitted by applicable law, NXGEN disclaims and excludes all warranties, whether statutory, express or implied — including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third-party rights — as well as any liability or warranty arising from suggestions, specifications or samples related to the Guide.

Security and Data Retention Policy

Updated 23 September 2026

Summary

This page summarizes the security controls and data-retention behavior that customers most often ask about during onboarding, legal review, and operational governance. Covers: Security controls, Data retention.

Security controls

- **Encrypted transport** — all platform traffic is encrypted in transit using TLS 1.2 or higher.
- **Encryption at rest** — credentials and sensitive data are stored encrypted at rest (AES-256).
- **Role-based access control** — access is controlled at the application layer based on each user's assigned role.
- **Authenticated agents** — field and edge components authenticate to the platform using signed tokens before they can send data.
- **Tenant isolation** — each customer's users, sites, and camera data are isolated from every other tenant.

Data retention

GC Surge retains data for the following default periods:

DATA TYPE	DEFAULT RETENTION
Alarm data	Minimum 12 months
Audit logs	Minimum 12 months (write-once — not editable or deletable)
Billing records	Minimum 7 years
Video snapshots	90 days (configurable)

GC Surge does not provide long-term video storage. Only the snapshots attached to alarms are retained, for 90 days; full video retrieval requires your own NVR/VMS. Where a retention period in your service agreement differs from these defaults, your agreement takes precedence.