

SecureSIGHT Platform Terms of Use

Version 1.1 - August 2026

1 Scope

These Platform Terms of Use ("**Terms**") govern access to and use of Secutec's platforms, including but not limited to SecureSIGHT, the MySecutec web application and the MySecutec mobile application, and any related interfaces (the "**Platform**").

These Terms apply to all access to and use of the Platform by the Customer and its authorised users.

These Terms complement the agreement between Secutec and the Customer, including the applicable End User License Agreement ("**EULA**"), Service Level Agreement ("**SLA**") and Data Processing Agreement ("**DPA**"). In case of conflict, the EULA, SLA and DPA shall prevail in their respective scope.

Use of the mobile application may also be subject to the terms and conditions of the applicable app store provider.

2 Access and Users

Access to the Platform is granted to the Customer and to natural persons authorised by the Customer ("**Authorised Users**").

The Platform is intended exclusively for professional (B2B) use by Customers and authorised partners.

The Customer is responsible for:

- designating and managing Authorised Users;
- ensuring that access rights are appropriately assigned and maintained;
- ensuring that all Authorised Users comply with these Terms.

The Customer remains fully liable for all acts and omissions of its Authorised Users.

Each Authorised User must:

- keep login credentials confidential;
- not share access with third parties;
- use multi-factor authentication (MFA) where required.

The Customer shall promptly revoke access rights when no longer required.

Access may also be granted on a limited basis to prospective customers or partners for evaluation or demonstration purposes, subject to these Terms.

3 Permitted Use

The Platform may be used solely for the Customer's internal business purposes and not for the benefit of third parties, unless expressly agreed otherwise in writing.

Subject to the Agreement, the Customer may:

- access and use Platform functionalities;

- view, export and use outputs generated by the Platform for internal purposes.

Certain functionalities (such as API access or partner impersonation features) may be subject to additional conditions or permissions. Where impersonation or delegated access features are made available, such use is strictly limited to authorised users and must comply with the applicable permissions and scope defined by Secutec.

The Customer shall:

- not disclose, distribute, resell, sublicense or otherwise make available any data or outputs derived from the Platform to third parties, unless expressly authorised by Secutec in writing;
- comply with all applicable laws and regulations in connection with its use of the Platform.

4 Acceptable Use

The Customer and its Authorised Users shall not:

- use the Platform in any unlawful, fraudulent or harmful manner;
- access data or systems without proper authorisation;
- share credentials or bypass authentication mechanisms;
- misuse impersonation or delegated access rights;
- attempt to gain unauthorised access to the Platform or related systems;
- interfere with or disrupt the integrity, performance or availability of the Platform;
- introduce malicious code, including viruses or harmful software;
- circumvent or breach any security or access control mechanisms;
- reverse engineer, decompile or otherwise attempt to derive source code, except where permitted by mandatory law;
- use the Platform to develop or support competing services or products;
- perform excessive automated queries, scraping, or other activities that may impact system performance;
- use data obtained through the Platform to attempt unauthorised access to systems, accounts or networks;
- use, reproduce or distribute Platform outputs in violation of third-party provider restrictions;

Secutec reserves the right to suspend or restrict access in case of violation of these Terms, in accordance with the Agreement.

Use of the mobile application may also be subject to the terms and conditions of the applicable app store provider.

5 Third-Party Services and Data

The Platform may incorporate or rely on services, data, content and functionalities provided by third-party providers ("**Third-Party Services**").

The Customer acknowledges that:

- such Third-Party Services are subject to specific limitations, restrictions and conditions imposed by the relevant providers;
- Secutec may not grant broader rights than those granted to it by such third-party providers;

- certain functionalities, data sets or outputs may be restricted, modified or withdrawn as a result of third-party requirements;
- data obtained from Third-Party Services may not be available in real time and may be subject to delays in ingestion, processing, synchronisation or display within the Platform.

The Customer shall comply with the restrictions applicable to Third-Party Services and shall not use the Platform or any data obtained through it in a manner that would place Secutec in breach of its obligations towards third-party providers.

Secutec shall not be liable for any limitation, modification, delay, inaccuracy or unavailability of Third-Party Services.

The Customer acknowledges that certain Third-Party Services may be subject to additional terms and conditions imposed by the relevant providers, which shall be deemed incorporated by reference to the extent necessary to protect Secutec's contractual position.

6 Threat Intelligence and Credential Data

Certain Platform functionalities may provide access to cyber threat intelligence data, including information relating to leaked, compromised or exposed credentials, breach sources, domains, usernames, e-mail addresses, technical indicators, risk scores and related contextual information ("**Credential Intelligence Data**").

Credential Intelligence Data may originate from Secutec, third-party intelligence providers and/or publicly available or otherwise lawfully obtained sources. The Customer acknowledges that such data may include confidential, sensitive and/or personal data and shall treat all Credential Intelligence Data as strictly confidential.

The Customer and its Authorised Users may access and use Credential Intelligence Data solely for the Customer's internal cybersecurity, fraud prevention, incident response, risk mitigation and remediation purposes.

The Customer shall not, and shall ensure that its Authorised Users do not:

- disclose, distribute, sell, resell, sublicense, publish, transfer or otherwise make available Credential Intelligence Data to any third party;
- use Credential Intelligence Data for any unlawful, harmful, offensive, investigative or surveillance purpose outside the Customer's legitimate cybersecurity interests;
- use Credential Intelligence Data to attempt unauthorised access to any account, system, network or service;
- use Credential Intelligence Data to reconstruct, validate, test or exploit passwords or other authentication credentials;
- export or transfer Credential Intelligence Data outside the Customer's organisation except where expressly authorised by Secutec in writing and subject to appropriate safeguards;
- attempt to identify, verify or confirm valid credentials based on Credential Intelligence Data;
- use Credential Intelligence Data to derive or infer authentication credentials.

The Customer is responsible for ensuring that it has the necessary authority to submit and receive Credential Intelligence Data relating to its own organisation and users. Each Party shall comply with its respective obligations under applicable data protection laws.

The Customer shall implement appropriate technical and organisational measures to protect Credential Intelligence Data against unauthorised access, disclosure, loss, misuse or alteration. Access to Credential Intelligence Data shall be limited to Authorised Users with a strict need to know.

For the avoidance of doubt, Secutec does not provide, disclose or make available clear-text passwords or full authentication secrets as part of the standard Platform functionalities. Any exceptional disclosure of clear-text or partially masked passwords, if permitted by Secutec at its sole discretion, shall require Secutec's prior written approval and may be subject to additional contractual terms, security procedures, verification requirements and restrictions.

Credential Intelligence Data is provided for informational and risk mitigation purposes only. Secutec does not warrant that such data is complete, accurate, current or sufficient to detect, prevent or remediate all security risks. The Customer remains solely responsible for interpreting the data and taking appropriate security measures.

The Customer shall indemnify and hold harmless Secutec against any claims, damages, losses, fines, costs or expenses arising out of or relating to the Customer's or its Authorised Users' misuse, unauthorised disclosure, unlawful processing or breach of this article in relation to Credential Intelligence Data.

7 Attack Surface Management

Certain functionalities of the Platform may include scanning, monitoring or analysis of systems, networks, domains or other digital assets.

The Customer acknowledges that such activities may be subject to legal restrictions in certain jurisdictions and remains solely responsible for ensuring compliance with applicable laws.

The Customer represents and warrants that it has all necessary rights, authorisations and permissions to perform such activities.

The Customer shall:

- limit such activities to assets owned or controlled by the Customer, or for which it has obtained explicit prior authorisation;
- ensure that such activities do not result in unauthorised access, disruption or interference with third-party systems;
- promptly notify Secutec of any incorrect, unexpected or unauthorised assets identified through the Platform, as well as any issues, disruptions or adverse effects observed in connection with such activities;
- comply with all applicable laws and regulations.

The Customer acknowledges that such activities may involve interaction with third-party systems and that Secutec shall not be liable for any resulting claims, damages or disruptions, performance issues or temporary unavailability of systems or services.

The Customer shall indemnify and hold harmless Secutec against any claims arising from unauthorised or unlawful use of such functionalities.

8 Customer Responsibilities

The Customer is responsible for:

- ensuring that it has all necessary rights, authorisations and legal grounds to use the Platform, including with respect to any systems, assets or data analysed;
- ensuring that its systems, devices and environment are secure and compatible with the Platform;
- maintaining appropriate access control within its organisation;
- the accuracy, quality and legality of the data provided to the Platform;
- complying with any restrictions applicable to third-party services integrated in the Platform;
- promptly notifying Secutec of any suspected security incident, unauthorised access or misuse.

The Customer acknowledges that:

- the Platform processes data provided by the Customer and third-party sources;
- outputs may depend on the quality, completeness and timeliness of such data.

Where the Platform is accessed via mobile devices, the Customer shall ensure that such devices are adequately secured, including the use of up-to-date operating systems and the absence of unauthorised modifications (e.g. jailbreaking or rooting).

9 Platform Characteristics

The Platform provides visibility, insights and support functionalities in relation to cybersecurity.

Depending on the interface used (web portal or mobile application), certain functionalities may be limited (e.g. read-only access).

The Customer acknowledges that:

- cybersecurity risks cannot be fully eliminated;
- the Platform does not guarantee the detection or prevention of all threats or incidents;
- outputs, alerts and assessments require interpretation and appropriate action by the Customer.

The Platform is provided on a best-efforts basis, in accordance with Good Industry Practice and subject to the applicable SLA.

Certain interfaces (such as mobile applications) may provide limited or read-only access to data and may not reflect real-time information.

10 Availability and Changes

The Platform may be subject to:

- maintenance;
- updates and upgrades;
- temporary interruptions or reduced performance.

Secutec may:

- modify or improve functionalities;
- add or discontinue features;
- require installation of updates (for mobile or other interfaces).

Such changes are part of the normal operation of the Platform and do not give rise to compensation unless otherwise agreed in the applicable Agreement.

11 Integration with Other Terms

Use of the Platform is subject to:

- the End User License Agreement (**EULA**) for licensing, liability and intellectual property;
- the Service Level Agreement (**SLA**) for service performance;
- the Data Processing Agreement (**DPA**) for personal data processing;
- applicable privacy notices.

These documents are available on Secutec's [Legal Page](#) and form an integral part of the contractual framework.

12 Updates

Secutec may update these Terms from time to time to reflect changes in the Platform, security requirements or operational practices.

Updated versions shall apply upon publication on Secutec's [Legal Page](#).

13 Acceptance

By accessing or using the Platform, the Customer and its Authorised Users acknowledge and agree to these Terms.

14 Trial and Evaluation Use

Secutec may grant access to the Platform on a temporary basis for evaluation, demonstration or trial purposes ("**Trial Use**").

During such Trial Use:

- access is granted on a limited, non-exclusive and revocable basis;
- the Platform is provided strictly "as is" and without any service commitments;
- use is limited to internal evaluation purposes only;
- no guarantees are given regarding availability, performance or functionality;
- Secutec may suspend or terminate access at any time without notice.

Unless otherwise agreed in writing:

- Trial Use is free of charge;
- no data retention or continuity is guaranteed;
- any data provided during Trial Use may be deleted upon termination.

The Customer or prospect remains responsible for ensuring that no sensitive or production-critical data is uploaded during Trial Use.