Cybersecurity Conditions

Of Attero B.V. and its associated legal entities

Colofon

date	October 9th 2025
version	1.1 – October 2025
status	final

ATTERO B.V.

Oude Apeldoornseweg 41
7333 NR APELDOORN
Postbus 40047
7300 AX APELDOORN

E-mail: info@attero.nl
Internet: www.attero.nl

1 Definitions

For the purposes of this conditions annex, the following definitions of terms apply:

Tender:	see the Standard Terms and Conditions of Purchasing Products and Services of ATTERO BV and its associated legal entities (hereinafter: 'Standard Terms and Conditions of Purchase')
Request:	see Standard Terms and Conditions of Purchase
Attero:	see Standard Terms and Conditions of Purchase
Management documentation:	hard-copy and digital documents, including physical and logical network drawings, configuration documents, an inventory of all components and software (including version and serial numbers), user manuals and installation- and configuration manuals, as well as procedures for rebooting and restoring the hardware and software in question, that are used to deal with system errors.
Source Code:	the whole of software instructions in their original programming language, including the corresponding Documentation, intended to be executed by a computer, in a form that a programmer with knowledge and experience of the used programming method and technique, will be able to change the software.
Cybersecurity:	endeavors to prevent loss, disruption, and misuse of IT and OT systems and in doing so to contribute to the availability, integrity, confidentiality and verifiability of the Information Provision (IP) and Industrial Automation and Control Systems (IACS).
Service/Services:	installation and implementation services, maintenance and support, and other activities to be performed in accordance with the Agreement.
Documentation:	every description of Goods and their properties, whether or not specifically intended for their installation, implementation, use, management or maintenance.

Escrow:	to deposit a copy or the original of the software and Source Code with an independent third party, to ensure Attero can use this or instruct for it to be used under its own authority to resolve errors and to otherwise maintain and manage software and Customized Software, when one more conditions set out in the Escrow agreement are invoked.
Customised Software:	software that has been developed, designed, produced specifically for Attero under an Agreement, or that is or has been designed or produced under the leadership and supervision of Attero, or on the basis of its instructions or designs, including the corresponding Documentation.
Agreement	Every legal relation governed by these Cybersecurity Conditions by virtue of Article 2.1 as described in the Standard Terms and Conditions of Purchase.
Parties:	see Standard Terms and Conditions of Purchase
Process automation:	comprises the automated control of continuous processes and batch processes with a computer or process computer. Process automation is often part of an overarching production or operating system and a synonym of Operational Technology (OT), of which IACS form part.
Other Party:	see Standard Terms and Conditions of Purchase
Goods:	see Standard Terms and Conditions of Purchase
CISO:	Chief Information Security Officer

2 Context

Under the Dutch Cybersecurity Act (Cbw), Attero qualifies as an essential entity for its activities in the field of energy generation and as an important entity for its activities in the field of waste processing. The resulting obligations with regard to the security of network and information systems form the basis for imposing additional cybersecurity conditions on suppliers and service providers.

3 Scope

1. The Cybersecurity Conditions apply to every Request, Tender and Agreement that Attero sends to the Other Party, receives from the other Party, or concludes or implements with the Other Party, and that involves activities that take place in the domain of office automation or process automation in any way.

2. These Cybersecurity Conditions are a supplement to the Standard Terms and Conditions of Purchase and do not amend or replace any Article thereof. In case of any conflict, the provisions of the Standard Terms and Conditions of Purchase always apply.

3. It is only possible to deviate from the Cybersecurity Conditions with Attero's written permission.

4. Other Party Cybersecurity conditions or similar named conditions having the same purpose, never apply to a Request, Tender to or Agreement with Attero.

4 Legislation and regulations

1. These Cybersecurity Conditions shall be governed by Dutch law. If any provision is in breach of mandatory law, this provision is not binding. However, all other provisions remain in full force.

2. The Other Party shall cooperate fully and without delay in complying with obligations arising from applicable laws and regulations concerning the security of network and information systems, including the Wbni/Bbni and, once in force, the Cyber Security Act (Cbw).

3. The Other Party processes personal data or other data in accordance with the applicable legislation and regulations, including the General Data Protection Regulation (GDPR) and the associated General Data Protection Regulation Implementation Act (UAVG).

4. The Other Party enables Attero to comply with legal requirements, For example by fully cooperating concluding a data-processing agreement, on the basis of an Attero template, or by carrying out a Data Protection Impact Assessment (DPIA), if Attero deems this to be necessary.

5 Training, certification, and training requirements

1. The Other Party must have a valid ISO 27001 certificate or be able to demonstrate that it works in accordance with the guidelines of IEC 62443-2-1 (or another relevant part of the IEC 62443 series). At Attero's request, the Other Party must submit the relevant certificate, audit report, or statement of conformity.

   If the Other Party is not ISO 27001 certified or cannot demonstrate that it works in accordance with IEC 62443, it must, in consultation with Attero, define, implement, and maintain the relevant organizational and technical control measures as described in EN-ISO/IEC 27002:2022 and/or IEC 62443.

6 Screening

1. In case of Services delivered to Attero, if required by Attero, employees of the Other Party, shall have a Certificate of Good Conduct Natural Persons/Criminal Records Check (VOG NP). Screening shall take place on at least the following job aspects: 11, 12, 13, 36, 38, 41, 61, 62 and 71.

2. If Attero requires, employees of the Other Party show their VOG NP at Attero's first demand. If they cannot show it, they shall be denied access to Attero immediately. Notwithstanding, the Other Party shall meet obligations and agreements that result from the Agreement (for example delivery dates) immediately and without prejudice.

7 Policy, processes, and procedures

1. If the Other Party manages accounts related to Services, in case of an employee of the Other Party or any Other party subcontractors employees leaves service, the Other Party shall withdraw the relevant rights as soon as possible and shall inform Attero in writing. If Attero manages the account of the employee in question, the Other Party shall also inform Attero of his leaving service in writing as soon as possible, in order for Attero to withdraw the relevant account right.

2. Connecting and disconnecting all kinds of equipment by the Other Party, including portable media, to Attero’s systems or subsystems, shall only take place in consultation with and following written approval from Attero.

3. The maintenance or modification of Attero’s systems or subsystems or systems or subsystems to be supplied shall only be carried out with systems that have been updated with the latest security updates and patches by the Other Party, and that have up-to-date virus-protection equipment.

4. For a system or subsystem to be supplied or maintained, the Other Party shall prepare a patch policy that demonstrates how the system or subsystem in question must be patched, whilst keeping the impact on the live system to an absolute minimum.

5. Prior to providing Services, the Other Party aligns its design and change process and procedures with Attero's in writing. Only designs validated by Attero may be implemented in Attero’s office and/or process automation domains. Attero’s

permission is without prejudice to Attero being able to invoke services from the Other Party that do not comply with the requirements imposed on it.

6. The Other Party cooperates fully and without delay setting up a back-up process and procedure, containing all the details performing planned and/or ad hoc back-ups and restores of systems and subsystems periodically, resulting in recovery of the relevant systems and subsystems full functionality.

8 Incidents

1. In an annex to the Agreement, the parties record an incident-response process and procedure and escalation procedures.

2. The incident-response process referred to in paragraph 1 includes at least that the Other Party provides a telephone and written report to Attero's CISO (Chief Information Security Officer) within 24 hours of incidents, including malware (for example ransomware and cryptoware), a data breach, or abnormal system behavior whilst providing Services to Attero.

3. The process referred to in paragraph 1, and both procedures, are evaluated annually by the Parties, and updated if required, at least during the term of the Agreement.

4. The Other Party records internal security incidents and provides Attero with a written report each quarter. The report notes at least the number of incidents that affected the Other Party, the way in which they were resolved, and the impact they have or had on providing Services or Goods to Attero.

5. If Attero decides to carry out or to instruct an investigation due to an incident, the Other Party shall cooperate in full with that investigation.

9 Logging and monitoring

1. Attero logs actions of employees of the Other Party on its network, systems and subsystems, so that a forensic or other reconstruction can be made after incidents. If employees of the Other Party are in default, Attero is entitled to terminate the Agreement immediately without the Other Party being entitled to any form or damages.

2. In addition to paragraph 1 of this Article, Attero is entitled to claim compliance with parts or all of the Agreement, whilst it is also entitled to additional damages due to losses caused by delays and consequential damage. If the aforementioned compliance is not possible, Attero is entitled to replacement and additional damages.

10 Hardware and software deliveries

1. Goods that are supplied by the Other Party to Attero, including hardware and software, shall comply fully and demonstrably with Attero's technical Cybersecurity Conditions.

2. All source code (Software and Customized Software) is handed over to Attero during

the implementation of the completion protocol.

3. At Attero's request, the Other Party shall always deposit a copy of the software and Source Code of Customized Software specifically for Attero in Escrow with a professional source-code escrow agent approved by Attero in writing. A form of active Escrow must be arranged that reasonably guarantees that the carrier of the deposited Source Code actually contains all the Source Code that is required to obtain insight into the architecture, design choices, chosen algorithms, and other preparatory materials that led to the deposited Source Code.

4. In the event of Source-Code Escrow, the Other Party shall submit written confirmation from that escrow agent to Attero no later than on the date of delivery, which demonstrates that the Source Code Cum Annexis (C.A.) of the Customized Softwarewas deposited with that escrow agent. If the Source Code C.A. is modified at any time, the Other Party undertakes to deposit the amended version or versions with that escrow agent.

5. Attero is entitled to require issue of all the versions of the Source Code C.A. that are with the escrow agent free of charge, if and insofar as it states in writing to the escrow agent that it dissolved the Agreement due to circumstances that are in the sphere of risk of the Other Party, or that is was terminated by the Other Party or will be terminated within one month, or is not renewed. Should the situation occur, the Other Party grants Attero the right to use or to instruct the use et cetera of the Source Code C.A. as described in the Agreement. Attero may also require the escrow agent to issue a statement that the Source Code was deposit with him accurately and in full.

6. If Escrow does not form part of the Agreement, Attero is entitled to demand and commit yet at any time during the connected Agreement.

7. The Other Party shall provide Attero with all the Management Documentation that pertains to the hardware and software that are supplied.

8. If maintenance of Attero's hardware and software forms part of the Agreement, the Other Party ensures that all the corresponding Management Documentation remains accurate and up to date.

11 Audits

1. Attero is entitled to carry out or to instruct cybersecurity-related audits at all times.

2. The Other Party shall cooperate immediately and in full with the audits referred to in paragraph 1 of this Article.

3. If the Other Party is in default regarding to paragraph 2, Attero is entitled to fully terminate the Agreement following a written demand without the Other Party being entitled to any form or damages.

4. In addition to paragraph 3 of this Article, Attero is entitled to claim compliance with parts or all of the Agreement, whilst it is also entitled to additional damages due to losses caused by delays and consequential damage. If the aforementioned compliance is not possible, Attero is entitled to replacement and additional damages.