Contents

1 Scope

This security policy is mandatory for all supplier and service providers and their employees (hereinafter referred to as "supplier") who access the IT and OT systems and infrastructure, or process Information of Auria Solutions UK I LTD or its subsidiaries and affiliates, (hereinafter referred to as “AURIA” or the “Company”) personally, or remotely or who enter the company premises. These specifications are to be understood as minimum requirements for the provision of services within Auria.

If these minimum requirements cannot be met by the supplier, Auria will initiate appropriate measures together with supplier to achieve the common goal.

Auria reserves the right to update and version this policy.

2 Policy

To reduce Information Security risks for Auria, the supplier agrees to implement suitable security standards. These standards should guarantee:

- protection of confidential information/data from both employees and business partners of Auria and, associated with this, the confidential treatment of data
- availability of data, applications and the technical IT infrastructure
- compliance with the integrity of data and IT and OT systems
- backup and restoration of data/IT infrastructure in the event of a failure or disaster
- the minimization of downtimes of IT and OT systems
- the company's good reputation in the public eye
- the avoidance of massive financial and intangible consequences for the company and for employees due to violations of contractual agreements or laws.

3 Measures

3.1 Access

3.1.1 Physical Access

Suppliers must register and identify themselves at the reception of Auria before physically gaining access to other rooms or zones. After successful authentication, the supplier will be given a visitor's pass, which must be worn permanently and clearly visible while on the Auria’s’ premises and which must be returned when leaving the premises.

For necessary physical access within the scope of service provision, Auria's security zone concept must be observed. The supplier's access is restricted to the areas necessary within the scope of their service provision and requires approval from Auria in the event of a change.

Access by suppliers to electronically secured zones is logged.

3.1.2 Access to systems

To access the IT or OT systems within Auria, personal access data is required for each employee of the supplier who is authorized to access them. The access data must be kept safe and protected against unauthorized access. Passing on this access data to other employees or storing the access data in an unsafe manner is prohibited. Access that is no longer required must be reported immediately to the Auria contracting body so that this access can be revoked. The use of IT and OT systems by unauthorized persons must be prevented. The access regulations and access controls must be observed.

3.1.3 Remote access

External access to Auria's networks may only be made via a VPN tunnel. The necessary software and access is provided by Auria and only this may be used. Suppliers must ensure that their own network does not allow uncontrolled third-party access to Auria's network. If requested, suppliers must be able to provide evidence of the purpose for which certain access was made. Suppliers may only use the access to copy or extract data from Auria's IT systems for which they have been authorized. No unauthorized software may be installed and/or information may be extracted or withdrawn from the IT systems.

3.2 Information Handling

Confidentiality, commitment, and non-disclosure agreements are part of the service contract. Employees of the supplier must be bound to these agreements.

3.2.1 Confidentiality

"Information" within the meaning of this obligation means all data, documents and other information that Auria makes available to the supplier in any form (e.g. verbally or in writing or by inspection) in direct or indirect connection with the project/order or that the supplier and service provider receives or creates - including copies and summaries created.

The supplier will always keep all information made available to them by Auria in

this context strictly confidential and protect it from access by third parties. This also applies to analyses and results that are created based on the information made available. To ensure confidentiality, the supplier undertakes to take appropriate technical and organizational measures to protect the information.

Excluded from this confidentiality obligation are only information that is generally accessible, was legally known to the supplier prior to receipt without an obligation of confidentiality, was approved for publication in writing by Auria or must be disclosed due to binding official or judicial orders or mandatory legal provisions.

In the event of a disagreement between the parties as to whether the information provided should not or should no longer be treated as confidential due to the exceptions mentioned above, Auria has a binding right of determination vis-à-vis the supplier. The obligation of confidentiality applies beyond the duration of the service.

3.2.2 Use of information

The supplier undertakes to use the information in accordance with the contract exclusively in connection with the tasks assigned to him. The information may not be used for other purposes, in particular not for competitive purposes, or made available to third parties, including non-affiliated companies, employees, subcontractors or consultants.

3.2.3 Handling and transfer of information

The supplier takes all precautions to avoid passing on of information. The information may only be passed on to the supplier's own employees and only if and to the extent that this is absolutely necessary for the performance of the task. The principle of data economy is observed.

The supplier also undertakes to instruct its employees who work for Auria within the scope of the contract in accordance with this agreement and to oblige them to comply with the resulting conduct.

3.2.4 Data protection and telecommunications secrecy

The supplier undertakes to comply with all applicable legal regulations for the protection of data and information. In particular, the supplier undertakes to ensure that data and telecommunications secrecy is maintained in accordance with the Telecommunications Act (TKG) and the General Data Protection Regulation (GDPR).

The supplier is aware that, in accordance with the General Data Protection Regulation (GDPR) and the data protection regulations of the federal and state governments, persons employed by the supplier are prohibited from collecting, processing or otherwise using personal data from Auria without authorization (data secrecy). The supplier undertakes to oblige the employees employed by him to comply with these requirements and to document this in writing.

Auria is and remains the sole owner of all data and is entitled to demand the release of individual or all data at any time. Upon termination of the contract, any use of the data by the supplier is prohibited and he/she is obliged to release all data to Auria in an appropriate form or, at Auria's request, to delete or destroy this data professionally and irretrievably.

The commissioning of subcontractors, the passing on of customer data to or for third parties and any transfer of data abroad is only permitted with the prior written consent of Auria. Auria is entitled to check compliance with the above agreements at any time.

3.3 Use of Work Equipment

3.3.1 Authentication

If suppliers are given access to IT or OT systems, the initial password must be changed after the first login. Auria's password policy must be taken into account here, including password complexity to be selected. As a general rule, a separate password must be used for each access to an IT or OT system. Passwords that the supplier already uses in a private environment must not be used.

All other means of authentication issued by Auria must be treated with the utmost care and protected from unauthorized access by third parties.

3.3.2 Use of hardware

Any use of the supplier or its employees' own hardware must be reported to Auria in advance. This hardware can only be used after inspection and written approval by Auria's IT department. This hardware must meet Auria's current security requirements. This includes, for example, installing an anti-virus program that must be installed on all IT systems of the supplier and service provider and the service company to protect against malware. All protection programs are configured and administered in such a way that they provide effective protection and prevent manipulation.

With regard to the operating systems and application software of the suppliers, they must ensure that the IT systems they provide and use are equipped with an operating system and application software that are supported.

3.3.3 Use of removable storage devices

The use of removable storage devices is prohibited. Removable storage devices within the meaning of this guideline includes USB sticks, external hard drives, and smartphones from outside the company. If removable storage devices are used for operational reasons, they must be checked beforehand by Auria's IT department.

3.3.4 Return

The supplier must, at any time upon request by Auria, hand over all information made available to him as well as evaluations, summaries, analyses, concepts, etc. prepared for him. The obligation to hand over also includes all copies, transcripts and reproductions. If handing over is not technically possible, the supplier undertakes to destroy or delete the information to be kept secret and to provide evidence of this in an appropriate form if necessary. In addition to the information to be handed over, all physical assets made available must also be returned to Auria (hardware, authentication means, etc.).

If necessary, the supplier is obliged to provide a statutory declaration with regards to the obligations mentioned here upon request. In this declaration he must assure, to the best of his knowledge and belief, that he has made every possible effort to fulfil the obligations mentioned.

The return or deletion of information from Auria does not release the supplier from the obligation to maintain confidentiality. The supplier is only released from the obligation to delete or destroy information to the extent that it is subject to statutory retention periods for the specific information.

3.4 Authority and Responsibilities

Suppliers are required to report possible improvements or weaknesses to Auria.

3.4.1 Behavior in the event of information security incidents

If the supplier becomes aware of a breach of information protection, he/she will inform Auria immediately. The same applies if the supplier or persons employed by him/her violate regulations on the protection of information / personal data or this declaration of commitment.

The supplier shall take the necessary measures to secure the information and to mitigate possible adverse consequences for Auria or data subjects and shall immediately coordinate this with Auria.

Behavior in the event of information security incidents at the supplier

The supplier is obliged to report security incidents in its organization that could potentially have a negative effect on the material and immaterial services provided or the information security level of Auria immediately and without delay. The supplier must respond immediately with initial status information to all requests or inquiries from Auria that are related to confirmed or suspected security incidents and generally to all questions about the security of external connections and the security of the IT facilities or resources used by the supplier or its subcontractors to provide the services. The initial report of a potential or already occurred security incident is made immediately by email to: infosec@auriasolutions.com

3.4.2 The supplier takes the following points into account when reporting:

- Who is reporting
- Which IT or OT system is affected
- How did you work with the IT or OT system or what did you observe
- When did the event occur
- Where are the affected IT systems located
- Document observations

3.5 License Management

Only licensed software may be used on all IT and OT systems. The owner of this license is responsible for its validity and up-to-dateness. The suppliers responsible for the various IT and OT systems must ensure that only licensed software is used as part of their service provision. If possible and economically viable, unlimited licenses should be preferred. This can prevent a functional restriction due to the expiration of the license.

The following principles apply:

- Only licensed software may be used; possible test periods provided by the manufacturer must be observed.
- Only software and hardware that is currently being maintained may be used.
- If suppliers are manufacturers of this software and/or hardware, they are responsible for appropriate maintenance and must be able to guarantee this.
- Use of company-owned software on non-company computers only with a valid license.
- No use of private software or private use of IT systems
- The supplier must regularly check the installed versions and track the available licenses and compare them with the number of products installed.

4 Document History

Revision Date	Description of Revision	Prepared By	NA Approved By	EU Approved By
Oct 2, 2024	Initial release	Albrecht, Thorsten	Gauthier, John	
Apr 4, 2026	Scope extended to all Suppliers	Albrecht, Thorsten	Ines Garcia	Gabriele Petrat