



## GENERAL TERMS & CONDITIONS OF PURCHASE – ANNEX 1:

### IT / IT-SECURITY

1. The Contractor will comply with the IT-Security requirements of the Customer when providing the contractual services. The Contractor also ensures this for any subcontractors.

The Contractor ensures that all persons employed by him in the provision of the service (including third parties / subcontractors) know and adhere to the relevant IT-Security requirements of the Customer.

The specifications are available [www.vwgroupsupply.com](http://www.vwgroupsupply.com) under the heading:

„Information“ → „Divisions“ → „Procurement“ → „Terms and Conditions of Purchasing“ → „AUDI AG“ → „Further Audi Locations“ → „AUDI BRUSSELS S.A./N.V.“ → „Information-Security-Framework“

At the request of the Contractor, the specifications can also be provided by email.

The IT-Security requirements can be specified / supplemented / further specified by means of special documents as part of the tender (e.g. specifications, information security concept).

2. When providing the contractual services, the Contractor will comply with the current state of the art in terms of data and system security in accordance with the quality level of the ISO 9001 family and the ISO 27000 family and in particular the Customer's systems according to the current state of technology against unauthorized access by third parties (e.g. hacker attacks) as well as against unwanted data transmission (e.g. spam).

The Contractor also ensures this for any subcontractors.

3. The Contractor will check the software and data carriers provided to us with an up-to-date virus scan program and ensure that the software and data carriers do not contain any so-called malware (software with harmful functions), computer viruses or worms, Trojan horses or the like.

4. The Contractor will provide and deploy carefully selected and trained specialist personnel in good time and ensure that the contractual services are provided in good time. Upon request, the Contractor will provide the Customer with appropriate evidence of the relevant qualifications of the personnel deployed.

The Contractor also ensures this for any subcontractors.

A contact person / project manager of the Contractor named by the Contractor plans, coordinates and ultimately supervises the provision of the contractual services and our provision / cooperation services.

5. If the subject of the contractual services is the creation of a result, the Contractor's main obligation is to technically document the contractual services in a comprehensible manner and to inform us with sufficient accuracy on request about the status of the contractual services.

6. Software must always be delivered to us with user documentation and - unless it is standard software - including source code and programming documentation.

7. The Contractor's access to our systems by means of remote data transmission is only permitted with our express written consent. The Contractor is obliged to inform himself about the applicable security guidelines and concepts, which we will make available to the Contractor on request. He will comply with these and instruct the employees and third parties / subcontractors that are permitted under these conditions in writing about their content before accessing our systems.

8. IT-Resources that are provided by us may only be used by the Contractor and his employees and / or subcontractors to fulfill the contractual services. Passwords or passwords may not be saved or passed on; these must be changed after 365 days at the latest.

The Contractor may use the IT-Resources provided and is not allowed

- to make any changes to the hardware
- to deactivate and / or change any safety settings or programs
- to install any software

In the case of provided, mobile IT resources (e.g. laptop), the Contractor takes suitable measures to ensure that they are protected against loss and theft.

The Contractor ensures that this is observed by all persons employed by him (including third parties / subcontractors).

9. We reserve all rights, in particular property rights and copyrights, to the technical requirement profiles, illustrations, drawings, calculations, samples and other documents made available to the Contractor; they may not be made accessible to third parties without our express written consent. Such documents and information are to be used exclusively for the provision of the contractual services and are to be returned to us without being asked after the contractual services have been concluded.

10. Unless otherwise stipulated in the order, the Contractor will provide all necessary infrastructure services for us at no additional cost. Infrastructure services are all preparatory services required in connection with the software and / or hardware services and / or applications (such as planning, construction, construction or installation of systems or IT-Workstations).

11. At our request, the Contractor will offer us support services at customary market conditions. Support services are all accompanying services required in connection with the software and / or hardware services and / or applications and / or infrastructure services, such as training, advice, optimization, maintenance / care.

12. If the Contractor provides us with standard software (also by way of a download), we acquire simple, sub-licensable, temporally, spatially and content-unrestricted rights for our own use.

13. For all other results that are the subject of the contractual services (individual software, software created in the context of customizing, documentation, concepts, etc.), we acquire exclusive, transferable, sub-licensable, temporally, spatially and content-unrestricted usage rights

14. Use of open source software in the context of contractual services is only permitted with our prior written consent.

15. If the Contractor uses open source software without our prior written consent, the Contractor must, at our request, do everything reasonable to replace the open source software with proprietary software of equal value. This is done cost-neutral for the Customer.

16. The Contractor shall indemnify us indefinitely from all third-party claims and associated costs due to the use of open source software by the Contractor without our prior consent, unless the Contractor is not responsible for the use.

17. "Click Wrap- / Shrink Wrap" license terms are not effective against us under any circumstances.

18. In order to handle security incidents, the Contractor must adhere to the Customer's incident management procedure from the beginning of the respective service.

The Contractor must inform the Customer immediately in writing of IT-Security incidents by email to [ciso.audibx@audi.de](mailto:ciso.audibx@audi.de) as soon as the Customer's data / information / systems are or could be directly or indirectly affected.

This also applies to IT-Security incidents in which the Customer's data / information is processed and / or stored on the Contractor's infrastructure / systems and any subcontractors.

19. The Contractor shall designate a contact person for IT-Security issues for the Customer in writing if the Customer's information / data is processed and / or stored on the Contractor's systems / infrastructure. To this end, the Contractor sends an email to [it-sec-external.audibx@audi.de](mailto:it-sec-external.audibx@audi.de) with the data of the contact person (name, email address, telephone number) and company data (name, address).

20. If required by the Customer, the Contractor must submit written reports on IT-Security reviews carried out at his or her subcontractor, which are related to security aspects of the services provided for the Customer.

21. The Contractor instructs the persons employed by him (including third parties / subcontractors) about their content before accessing the Customer's systems.

The Contractor carries out suitable awareness measures to raise awareness of the topic of IT-Security for the persons employed by him (including third parties / subcontractors) if these persons have access to the Customer's data.

If necessary, the Customer can offer additional IT-Security training, which is binding for the performance of special activities.

22. The Contractor grants the Customer and / or a third party commissioned by the Customer and / or the corporate auditing of VOLKSWAGEN AG / AUDI AG the right to be exercised at any time, after prior notification:

- all data on business transactions between the Contractor and the Customer;
- the IT-Security documents (regulations, work instructions, etc.) and processes of the Contractor and any sub-companies with regard to compliance with the Customer's IT-Security specifications

to inspect and check at the Contractor and any subcontractors.

23. The Contractor grants the Customer, after prior registration, the right to carry out an IT-Security audit at the Contractor and any subcontractors if one or more of the following points apply:

- the Contractor processes and / or saves Customer data classified as "confidential" or "secret" on their own systems / infrastructure
- Use of data transmission (remote data transmission) between the Contractor's systems / infrastructure and the Customer's systems / network
- The Contractor provides services in the field of "prototypes" (vehicles, parts, components and assemblies)
- The Contractor provides services in the field of "immobilizer-relevant" components

The Customer can also commission third parties to carry out the IT-Security audit.