CARIAD
A VOLKSWAGEN GROUP COMPANY

Cyber Security Basic Requirements from Feb. 17th 2022 of CARIAD SE (in the following „CSBR")

"This English Translation ("CSBR") of the Cyber Security Grundanforderungen (CSGA) is for information only. The CSBR and its terms shall be construed according to German law (German version: CSGA). If the English meaning in the courtesy translation (CSBR) differs from the German legal meaning of the German agreement (CSGA) and its terms, the German meaning shall apply."

The Project (also) include aspects related to cyber security. Due to regulatory requirements, the Client must provide comprehensive cyber security for its products ("**Product**" is to be understood as all objects that the Client places on the market and which contain project scopes. This includes in particular vehicles, charging hardware and apps) throughout the entire product life cycle. This is impossible within the project scope without the involvement of the Contractor. Therefore, the Contractor shall agree to contribute as stipulated by the provisions of this CSBR.

With this proviso, the Parties agree to the following:

1. Terms

Terms in italics in this CSBR have the meaning defined in Annex 1.

2. Systematic Testing

2.1. The Contractor must fulfill the following requirements with regard to systematic testing, which are also included in the Group Basic Requirements for Software (GBRS, version valid for the project). They must be documented for the Client in the required form ("security verification"):

a) The Contractor must make the metrics collected available to the Client upon request. The exchange format shall be determined by the Client.

b) The Contractor must provide the Client with information about all free and open-source software elements utilized in the software delivered.

c) In addition to implementing suitable coding policies or modeling guidelines, the Contractor shall also implement security coding policies.

d) State-of-the-art metric and defect analysis tools must be integrated into the software development process to fulfill the requirements of this section.

e) The known errors arising from the project scope and their effects must be documented.

f) The version used for all software elements and, if applicable, the patch level must be documented.

g) The project scope must not contain any known vulnerabilities. Any deviations must be addressed in the risk analysis and justified.

h) At the Client's request, the Contractor must grant the Client the opportunity to per-form tool-based analyses of the entire source code with the Contractor on the Con-tractor's premises.

i) The Contractor must regularly provide security verification with every software delivery, as coordinated with the Client.

2.2. The Client shall define the specific verification format along with the delivery modalities and confirm these annually, if necessary:

a) The security verification must contain a summary of the results from the security risk analyses.

b) The security verification must illustrate that the security requirements have been implemented and verified.

c) The security verification must illustrate that the security coding guidelines have been complied with.

d) The security proof must illustrate that the reaction process for handling any vulnerabilities identified and the active monitoring of the scope of delivery have been implemented.

3. Penetration Testing

3.1. The Contractor expressly permits the Client and grants the Client the corresponding rights to extensively review, modify and test the project scopes for cyber security vulnerabilities at any time, in particular before and after any products equipped with the project scopes delivered are put into circulation by the Client. Therefore, the Client may in particular utilize or permit the use of any methods and techniques (including security/penetration tests and analyses such as circumvention of protective measures, reverse engineering, fuzzing, sniffing, spoofing, eavesdropping and manipulation, code injection/execution, disassembly, decompilation) that serve to identify vulnerabilities, either

a) itself,

b) through third parties instructed to do so or in cooperation with the Client; or

c) by other third parties in the context of any competitions organized by the Client (including bug bounty programs).

3.2. During the course of the penetration tests, unintended access to systems and data belonging to the Contractor or third parties outside the actual project scope may be possible as a possible cyber security vulnerability. If such access is detected, the Contractor and the Client shall discuss the issue before continuing the tests. In the process, the Client shall strive to refrain from actually accessing the systems or data wherever possible. Taking into account the restrictions described above, the Contractor expressly permits the Client to carry out tests in this respect as well, and assures that it possesses the necessary authority to grant this permission or has obtained such from third parties (in particular from its suppliers).

3.3. In the event of a contractually permissible use of the project scopes by other VW Group companies, these companies shall also be entitled to perform the actions specified under this item 3.

3.4. The Contractor's obligations shall remain unaffected. Neither the Client's right to perform tests nor the actual performance of tests shall limit the Contractor's obligations towards the Client or third parties or justify any joint responsibility on the part of the Client.

4. Incident/Vulnerability Management

4.1. The Contractor must establish a contact for a bi-directional response process for handling *cyber security notifications* and respond to inquiries from the Client within a reasonable period of time. The Client and the Contractor shall agree on specific references that shall be drawn on when communicating individual cyber security messages. If the Contractor employs subcontractors during the project, the Contractor shall require the subcontractors to set up comparable contacts to enable them to respond with the appropriate speed and detail, depending on the level of relevance or urgency of the cyber security notification.

4.2. The Contractor must appoint *a person responsible for the security* of its project scope (*Chief Information Security Officer, Chief Product Security Officer*, or similar) and set up a functional e-mail address as the contact for messages from the Client, which is capable of encrypted communication (see also General Purchasing Conditions). The Contractor must save the information in the supplier database (accessible via the One.Group business platform) and update it as required.

4.3. If the Contractor becomes aware of cases belonging to the *Weakness* category or higher, or has reason to believe that a case belonging to the *Vulnerability* category or higher is contained within the project scopes, it shall notify the Client immediately (hereinafter "**Notification**"). Where suspicion arises in the following cases:

a) **Client's products** already ***put into circulation***

b) IT systems that serve to implement the scope of the order

c) Vehicle projects in development

d) Any other issues related to the project scope the Notification shall be sent to the Client's Incident Team at the following email address:

CARIAD contact for vulnerabilities: vuln@cariad.technology

CARIAD contact for incidents: sirt@cariad.technology

4.4. The Contractor shall provide an initial analysis for each Notification within a reasonable period of time. The specific content of the initial analysis shall include at least the categorization and description of the suspected case, a description of the path of attack, a description of the effects, an assessment of the probability of occurrence, the affected products, scopes, parts, components, systems and projects together with the

specific software version and the probable risk, as well as a proposal describing possible countermeasures including a schedule and the responsibilities. If necessary, the scope of the initial analysis can be expanded if agreed between the Contractor and the Client.

4.5. Within a reasonable period of time set by the Client, the Contractor shall then carry out a detailed technical analysis in close coordination with the Client, and develop specific countermeasures as well as an implementation plan. Depending on the urgency level of the Notification, the rectification of the causes of the problem must be carried out immediately (*Incident* category or higher) or (*Vulnerability* category and below) not carried out until after the effectiveness has been proven and the Client has issued a written instruction to do so. In the case of notifications with *Vulnerability* urgency levels and below, the type of order or processing is always clarified before the problem is rectified, i.e., whether the service is classified as warranty, support, an individual order or similar. The Contractor shall provide detailed documentation of every aspect.

4.6. If the Contractor plans on external communication that pertains to the Client, this must be coordinated with the Client's Incident Team.

4.7. At the Client's request, the Contractor must provide a reasonable number of hardware and/or software samples at its own expense to enable the Client to verify the vulnerability and the solution provided.

4.8. The Contractor must establish a process for active and continuous monitoring of the cyber security status for the project scope and demonstrate this to the Client as per the "Automotive Cybersecurity Management System Audit" VDA standard.

4.9. The suitability of a time period is determined, in particular, by the Client's ability to fulfill its legal and official (notification) obligations on time, taking into account the Client's internal processing times.

4.10. Any other information obligations on the part of the Contractor, e.g., supplier self-disclosure at procurement and quality of purchased part, shall remain unaffected.

5. Support Period

5.1. The Contractor shall guarantee and be capable of providing support and maintenance services to rectify cyber security vulnerabilities for a period of fifteen (15) years after End of Production ("EOP") (see GBRS), unless a different period is specified in the order

(e.g., in the specifications) for the specific project. This shall include the ability to customize all specifications associated with the software as well as the source code, create the corresponding binaries, and perform all levels of testing. In this context, EOP refers to the end of production of the product which the project scopes are installed in or used in.

5.2. The Client may request that the source code including the entire required development environment with SOP along with all subsequent major releases be deposited with an independent third party specified by the Client ("Depository"). After depositing the items, the Contractor shall not be entitled to recover these until the support period expires, irrespective of the legal grounds. The Depository shall become the owner of the deposited items at the moment of the deposit. The Depository shall be entitled, solely in the event of the insolvency of the Contractor or the discontinuation of business by the Contractor, to grant to the Client (i) the transferable ownership of the deposited items, to the extent that ownership thereof is transferable, in particular to the physical documentation and the deposited data carriers, and (ii) to the extent that ownership of the deposited items cannot be granted, in particular to the software stored on the deposited data carriers, the right to use, duplicate and adapt, in particular to eliminate errors, to modify, expand and create interfaces, free of charge and without any restrictions regarding content, space or time, and also to sublicense to group companies for the purpose of rectifying defects and vulnerabilities.

6. Providing hardware and software information (Asset Management)

6.1. If the project scopes become part of products, the Contractor must provide the Client with at least the following information as part of the hardware/software documentation (see also component and interdisciplinary specifications) for the project:

a) Hardware information must be provided by the TIER 1 in the HAMON system in accordance with contractual agreements (including eNA), from a cyber security perspective, in particular:

- Project data of the component (intelligent components, e.g., controllers, processors)
- Component manufacturer
- Manufacturer part numbers of the components

b) The following software information must be provided:

- Bootloader name and version
- Operating system name and version
- List of all drivers used
- Information about any software (on the control unit) (regardless of whether in-house development, free and open-source software, purchased software)
    - Software module/library manufacturer
    - Software module/library designation
    - Software module/library version number
    - Software module/library link to source
    - Software module/library hash value incl. hash algorithm

The initial software information shall be entered by the Contractor during the product development and qualification process. The complete data for the series production version must be provided in the relevant systems by the time of development release. If the scope of delivery changes during the course of the support processes, these changes shall be integrated into the documentation by the Contractor.

6.2. Any other information obligations on the part of the Contractor, e.g., for free and open-source software included in the project scope or the obligation to enter data into HAMON, shall remain unaffected.

7. Securing the supply chain

The Contractor shall ensure that all subcontractors working on the project or whose components are used in the project shall also be required to comply with this CSBR. It shall be liable for the fault of its subcontractors as though for its own fault.

8. Others

8.1. The Parties agree that this CSBR shall also apply to those project scopes that have already been provided as part of the project prior to the signature of this CSBR.

8.2. Changes and amendments to this CSBR shall not be effective unless they are made in writing. This also applies for a change in the written form clause.

8.3. If one term of this CSBR is or becomes ineffective, the validity of the remaining terms of the CSBR shall not be affected. The Parties agree to negotiate in good faith on a provision replacing the invalid provision.

8.4. The law of the Federal Republic of Germany shall apply exclusively, unless otherwise agreed. The applicability of the United Nations Convention on Contracts for the International Sale of Goods of April 11, 1980 is excluded.

Attachment:

Annex 1: Supplementary Document regarding Terminology and Definitions

Annex 1: Supplementary document regarding terminology and definitions

When interpreting and applying the basic cyber security requirements, the following definitions apply in particular:

BTV	Component manager
Bug Bounty Program	Initiative to uncover errors and weak points with material or cash prizes for the discoverers
Chief Information Security Officer	Contact person for the security of information in his company
Chief Product Security Officer	Contact person for the safety of his delivered product
Code injection/execution	Bringing in / executing code by processing invalid input data
Coding guidelines	Rules and standards to improve software quality
Collected metrics	Predefined metrics for evaluating software quality (see GBRS)
CSBR	Cyber security basic requirements
Cyber Security messages	Differentiation of 5 levels of urgency
Cyber Security information	All information that is recorded as part of the monitoring process and whose cyber security relevance (potential weak point) has not yet been classified. Urgency level 1
Cyber Security event	Cyber security information that is classified as potential weak points (without risk assessment) for the company or its products and requires further treatment (CSI process, information assessment, etc.). Urgency level 2
Cyber Security weakness	Errors in the security concept or in the implementation (technical, organizational, procedural) of an asset. Urgency level 3
Cyber Security vulnerability	Weakness of an asset that can be exploited by one or more threats. Urgency level 4
Cyber Security incident	Individual or a series of undesired or unexpected cyber security events that prove the exploitation of a vulnerability and could have a significant influence on the

	security of a component / function (e.g. cause damage to the asset). Urgency level 5
Delivered software	Software supplied is the software supplied by the contractor (including contractor software, additional software, software from third parties).
Disassemblierung	Conversion of binary machine code into readable assembly language
Eavesdropping und Manipulation	Reading or modification of exchanged digital data
eNA	Electronic Nomination Agreement
EOP	End of Production
Free and Open Source Software	Free and Open Source Software (FOSS) is any software that is distributed under usage and license conditions, the essential obligation of which typically includes passing on or disclosing the source code of the software when it is distributed. Free and open source software is a variant of third party software.
Fuzzing	Fuzzing is a technique for testing software using invalid, unexpected, or random input data
Group Basic Requirements Software (GBRS)	Group cross-sectional specification for the regulation of software quality (Konzern Grundanforderung Software (KGAS))
HAMON	VW Group's platform for information on electrical and electronic components
Incident Team	The incident team coordinates the processing of cyber security reports

Informationen der Free and Open Source Software	For each FOSS element used, at least the following information must be included: • Surname • Unique version identification • License name with a unique license version number • Full license text • Download link for the license text and the source code including the last access date • Source code and copyright notices • Information as to whether the source code and copyright notices are to be passed on or published • Any sub-elements that are required to use the software element, including the aforementioned information on licensing
Responsible for security	Contact person for the safety of his delivered product
Sniffing	Technology for analyzing network traffic
Spoofing	Technology for disguising one's own identity in networks
System	The system is the entire scope of delivery to be provided by the contractor. The system consists of system elements.
System element	A system element is a logical component of a system. System elements are described in the system architecture specification. Typical system elements are software, hardware (e.g. sensors, actuators, circuit boards, components and connections) and mechanics (e.g. housing).