1. Scope of application

1.1. These General Information Technology Conditions (hereinafter referred to as "**GITC**" apply to the information technology or communication technology (hereinafter referred to as "**IT**") services used by AUDI HUNGARIA Zrt. and/ or AUDI HUNGARIA AHEAD Kft. (hereinafter referred to also as "**Customer**") and the activities involving data controlling and data processing. The provisions of these GITC shall apply, as appropriate, also to other services and contracts if the **Partner** is given access to the Customer's IT systems in the course of performance or works with the Customer's IT systems or accesses to the Customer's information and data in any other way.

2. Performance of the Contract

2.1. The term "**Contract**" is defined in section I.7 of the Customer's General Terms and Conditions of Purchase (hereinafter referred to as "**GTCP**").

2.2. If the subject-matter of the Contract is to achieve a result, the Partner undertakes to document performance appropriately and, if needed, inform the Customer as he expects of the state of the service.

2.3. Should the Partner's staff member be provided access to the Customer's IT systems, the staff member's data shall be processed and used in an affiliated company of AUDI AG or VOLKSWAGEN AG (hereinafter referred to as "Concern Company(ies)"). The Partner shall obtain a prior written consent from his staff members concerned to the data processing mentioned above and, if so needed by the Customer, present these documents to him; the Partner shall be solely liable for non-compliance with these obligations.

2.4. Unless otherwise provided in the Contract, the Partner shall perform all necessary infrastructure services to the Customer without claim the refund of any costs. Infrastructure services shall mean all preparatory services necessary for preparation of the software and/or hardware service and/or application (for example the design, development, set-up or installation of systems, IT workplace).

2.5. If so needed by the Customer, the Partner will make an arm's length offer for support services. Support services shall mean any services accompanying all software and/or hardware services and/or applications and/or infrastructure services (e.g. training, consultancy, optimization, maintenance and preservation).

3. Licence conditions

3.1. Open Source software

3.1.1. Any software with open source code may only be used during performance of the Contract with the Customer's prior written consent.

3.1.2. Should the Partner use a software with open source code without the Customer's prior written consent, then – if so needed by the Customer – he shall replace the software with open source code by an equivalent software with closed source code.

3.1.3. The Partner shall fully release the Customer from third-party claims arising from use by the Partner of open source code software without the Customer's prior written consent and the related costs.

3.2. Click Wrap / Shrink Wrap licence

3.2.1. The Customer excludes application of Click Wrap / Shrink Wrap licence conditions.

3.3. Licence audits

3.3.1. Should the Partner inform the Customer in writing, with appropriate explanation, that, in his opinion, the Customer breaches the rules for the right of use of a software delivered by him, then the Customer will conduct a licence audit in connection with the software concerned (review of compliance with the rules for right of use) and the Customer will inform the Partner of the results of the licence audit.

4. IT Security Requirements

4.1. In the course of performance of the Contract, the Partner shall provide data and system protection requirements complying with the latest ISO 9001 standard and ISO 27000 standards, as well as the state-of-the-art science and technology, so in particular he will secure the Customer's systems according to state-of-the-art technology against unauthorized access by third parties (e.g. hacker attacks) and undesired data transfer (e.g. spams).

4.2. In the course of performance of the Contract, the Partner shall comply with the Customer's regulations relating to the data controlled and processed by him. The data concerned by the relevant Contract shall be classified by the Customer according to confidentiality, integrity and availability (hereinafter referred to as "data classification"). The detailed requirements for data classification are included in Annex No. 1 to the GIITC. In the course of determining the data classification and confidentiality obligation, „Trusted Information Security Assessment Exchange" (hereinafter referred to as TISAX) relevance is also determined. If a purchase order / contractual order requires a TISAX certification corresponding to the requested documents, the Partner undertakes to provide such certification or to obtain the TISAX certificate. The period of time during which the TISAX certificate is obtained shall not exceed 12 months after acceptance of the Contract, except if the minutes on the negotiation provide otherwise. In the case of a Contract with TISAX relevance, the Partner shall observe the AUDI concern's TISAX audit processes. The Customer shall inform the Partner in writing of the detailed steps of the TISAX certification process and the measures to be taken in writing, based on the currently effective TISAX certification process.

4.3. If so needed by the Customer, the IT

system developed or provided by the Partner shall pass the penetration test to be implemented based on the recommendations of the OWASP Application Security Verification Standard Project and OWASP Top Ten Project. The penetration test shall be carried out by the Customer and/or his external partner. If so needed by the Partner, it is possible to present the result of a penetration test ordered by him, which shall be consulted with and approved by the Customer in writing. The Penetration Test report and action plan presented by the Partner shall not be older than 1 year. The penetration test approved by the Customer in writing and presented by the Partner may replace the penetration test carried out by the Customer and/or its external Partner.

The Partner shall remedy the IT security weak points and deficiencies revealed by the penetration test at the latest until transfer for operation and provide for approval of such remedy by the Customer.

4.4. In the course of performance of the services, the Partner shall comply with the Customer's information security requirements, which are available in the main text of these GITC and its annexes, as well as in the special documents relating to the relevant Contract.

4.5. The Partner shall inform the contributors involved in performance (including, in particular, but not limited to: employees, subcontractors, agents, other third parties) of the contents thereof, prior to their access to the Customer's systems, in full compliance with the IT security requirements. Customer shall provide security and awareness training opportunities to the persons involved by the Partner in performance and working with information and such persons must attend such training. In the case of services whereby also information of Customer is processed, the Partner shall designate, in a documented form, a contact person in charge of information security issues (dedicated or non-dedicated depending on the volume of the service). The suppliers shall designate, document and send to Customer in a documented form the names and particulars of the persons participating in the relevant service and having access to information of Customer (taking also the relevant data protection rules into consideration), who may get in contact with such data either periodically or continuously.

4.6. The Partner shall regularly (at least once in a year) inspect whether the Partner's user rights are adequate for his tasks. If necessary, the rights need to be amended as appropriate. The Partner shall inform the Customer of the result of the revision of rights in writing.

4.7. The Customer shall manage the security requirements for the temporary (e.g. transition) period of the services separately from the continuous service period; in such periods the Partner shall apply different security measures and audit methods.

4.8. For the purposes of fast, efficient and uniform management of information security incidents, the Customer's procedures for management of information security incidents must be observed by the Partner from starting of the relevant service. The Partner shall in each case send a written notice to the Customer immediately of any information security incident affecting the services provided to the Customer or the Customer's data (CERT-AudiHungaria@audi.hu). The Customer shall inform the Partner in writing of his procedure for management of information security incidents and the actions to be taken, taking the respective information security incident into consideration.

4.9. The Partner shall document and immediately inform the Customer in writing of any changes that might affect the service provided to the Customer, so in particular, including but not limited to:

- any change in the Partner's contributors;
- use of a new technology, product or version;
- any change in the place where the service is provided, other changes in the physical environment;
- any services provided to a third party that might affect the service provided to the Customer.

4.10. If so needed by the Customer, the Partner shall submit written reports on the information security audits conducted for him and associated with the security aspects of the services provided to the Customer.

4.11. Each Partner shall comply with the provisions of Annex No. 1 to these GITC („Information Security Procedural Directives for External Staff Members and Partner Companies").

5. Revision Clause

5.1. The Partner shall grant a right to the Customer and/or his external partners and/or to VOLKSWAGEN AG's concern, that may be exercised at any time, under which, after prior notification, they may inspect and review:

- **all data relating to the business events between the Partner and the Customer;**
- **the Partner's and/or his contributors' IT security documents (regulations, work instructions, etc.) and processes, compliance with the Customer's IT security requirements;**

in the premises of the Partner and/or his contributors.

6. Others

6.1. Should any provision of these GITC conflict with the provisions of the GTTP, the provisions of these GITC shall have precedence.

6.2. Effective date: 01.07.2023 as of which date the General Information Technology Conditions issued on 29.07.2021 become null and void.

AUDI HUNGARIA Zrt.
Registered seat: 9027 Győr, Audi Hungária út 1.
Court of Registry of the Tribunal of Győr
Company Reg. No.: Cg. 08-10-001840

VAT numbers:
Hungarian VAT No.: 23391475-2-08
Hungarian EU VAT No.: HU23391475

AUDI HUNGARIA AHEAD Kft.
Registered seat: 9027 Győr, Audi Hungária út 1.
Court of Registry of the Tribunal of Győr
Company Reg. No.: Cg. 08-09-035615

VAT numbers:
Hungarian VAT No.: 32230866-2-08
Hungarian EU VAT No: HU32230866

Annex No. 1 to the General Information Technology Conditions - Information Security Procedural Directives for External Staff Members and Partner Companies

Version: 1.0 (30.05.2023)
Issued by: Legal Department
Corporate Directive owner: IT Security/Governance
Regulation No.: Information Security Corporate Directive U_2.024 Annex No. 4

Scope

The procedural directives shall apply to the partners (hereinafter referred to as “Service Provider”) who provide services to AUDI HUNGARIA Zrt. and/ or AUDI HUNGARIA AHEAD Kft. (hereinafter referred to as „Customer”) and his fulfilment partners (hereinafter referred to as “contributors”).

1 Purpose

These information security procedural directives determine the rules for information security the service providers have to observe in the course of management of information and operation of IT devices (e.g. computers, workstations, laptops, smart phones or tablets).

Service provider shall mean any third party who provides services to Customer under contractual relationships. These action directives have been drawn up for the service providers' managers, staff members and fulfilment partners (e.g. subcontractors) (hereinafter referred to as "contributors").

The purpose of these information security procedural directives is to provide for the confidentiality, integrity and availability of information, as well as to protect the rights and interests of the Customer and all natural persons and legal entities who maintain business relationships with and/or pursue activities for the Customer.

1.1 Abbreviations and definitions

Abbreviation/term	Explanation
Information originator	A person or group of persons who/which generates certain information or a document. The originator shall classify/mark a document/information according to the classification level defined by the information owner.
Information owner	A person or group of persons who/which is appointed by the management to protect certain confidential information. The information owner may change during the lifetime of the information.

2 Document Structure and Target Group

This document consists of three chapters. The following table shows the structure of the document and the target groups by chapters.

Chapter	Target group	Notes
3	All service providers	Each service provider shall comply with the requirements set out in this chapter. Chapters 4 and 5 include additional requirements to be complied with depending on the options of access to the concern's network and systems.
4	Service providers who have access to the concern's network and systems	The requirements defined in chapter 3 must also be complied with.
5	Service providers who do not have access to the concern's network and systems	The requirements defined in chapter 3 must also be complied with.

3 General Requirements

Each service provider shall comply with the following requirements according to the definitions set out herein.

The requirements relevant to the Customer shall not be included in this document.

3.1 Organizational requirements

The IT devices other than those made available by the Customer may be brought in the company's area or the Customer's security areas subject to the regulations of Customer.

The data and software owned by the Customer shall not be used in IT systems or storage devices that are made available or approved by a party other than the Customer or the service provider.

The data and software owned by Customer shall not be used for a file provider or internet cloud provider not approved by the Customer.

The data can be forwarded to third parties only based on the written approval issued by the Customer's data owner.

The Customer's regulations for collection, processing and use of personal data shall be observed (see Appendix 7.2.1).

The service provider's management shall require its staff members to keep secret according to the confidentiality agreement between the Customer and the service provider. The Customer shall always be entitled to inspect these agreements.

The Customer's data stored on mobile systems or IT devices shall be encrypted by state-of-the-art hardware and software. The additional requirements for encryption and authentication are available at the concern's supplier portal (see Appendix 7.2.2).

Prior to travelling abroad the requirements for use of the security technologies (e.g. encryption) applied in the country concerned shall always be taken into consideration.

When the contract expires, the Customer's data shall be delivered to the Customer and erased from the service provider's devices and storage media. The statutory requirements (e.g. retention periods) shall also be observed.

3.2 Personal security

The user concerned shall immediately notify the ordering body (e.g. the Customer's competent user administrator) of the user identifiers or the accesses to the Customer's data that are no longer needed to enable the appropriate locking/erasure.

Any identification media no longer required (e.g. Smartcards, SecurID cards) shall be immediately returned to the ordering body.

The devices (e.g. laptops) and storage media delivered for use and the data storage devices shall be returned to the Customer when the contract expires or when they are no longer needed.

The user shall immediately report loss of the IT devices delivered to user or the media used for authentication to the Customer's competent body (see Appendix 7.2.3).

3.3 Physical and environmental security

The IT devices storing or managing the Customer's data shall be used so as to avoid that any unauthorized person can inspect or have access to the data. Special caution needs to be exercised during use of mobile systems.

In order to avoid unauthorized inspection, confidential or secret data must not be left without supervision in any time.

3.4 Management of organizational values

3.4.1. Regulations for classification

Classification shall be carried out based on the three purposes of protection – confidentiality, integrity and availability – in respect of all information and data processing IT systems.

The service provider shall obtain from the Customer the classification according to confidentiality, integrity and availability (in respect of the scope of the relevant services).

The information (purpose of protection: confidentiality) shall be protected by the measures corresponding to their confidentiality classification against unauthorized access during their whole life. The expiry date of confidentiality classification may be set.

If necessary, the relevant process owner shall check and define classification according to integrity and availability in the course of data processing. The current classification shall be regularly evaluated and changed, as necessary, with participation of the information owner.

The information owner shall confirm correct classification.

3.4.1.1. Confidentiality

Information not addressed to all staff members may be made freely accessible only by authorized persons (based on the "need-to-know" principle).

Requirements relating to originators and owners of information:

- The originator (see 1.1 – Information originator) shall mark newly generated information and data.
- The owner of the information (see 1.1 – Information owner) shall be responsible for classification.
- The originator shall ask the information owner to submit the correct classification.
- Confidentiality classification shall be performed for each IT system.
- If classification is not yet clear, e.g. in the case of newly generated documents/IT systems, classification shall be marked as „confidential".
- In the case of internal, confidential and secret information, the information owner shall (at the latest upon the next revision and update) verify whether the existing confidentiality classification is correct and shall also mark it as appropriate.

Requirements relating to recipients:

- Information and data not marked shall be processed as "internal".
- If any doubt arises in connection with classification, the information owner shall be contacted.

As regards the confidential nature of information, the following specific classification levels exist:

Classification	Definition
Public	Information free of any restriction, e.g. that publishable in the press or the internet. Public use of corporate information is subject to the competent body's consent (see Appendix 7.2.4). Examples: press communications, product catalogues intended for customers
Internal	Information the knowledge or abusive forwarding or use of which by unauthorized persons affects achieving of the product and project goals only to a slight extent, so it may be made accessible by the authorized persons. Infringement of confidentiality may involve adverse consequences, even if they are insignificant. Example:

	• It is not probable that certain persons or organizations raise claims for damages Examples: business communication data (telephone number or e-mail address), industrial OHS requirements, schedule of work
Confidential	Information the disclosure or publication of which to unauthorized persons might jeopardize achieving of the product and project goals so it may be made accessible only to a closed group of authorized persons. Infringement of confidentiality will presumably result in measurable adverse consequences, e.g.: • loss of customers • fall in sales figures/turnover • claims for damages of certain persons or organizations Examples: in addition to business communication data, personal data (e.g. payment), budget planning, revision reports
Secret	Information the disclosure or publication of which to unauthorized persons might grossly jeopardize achieving of corporate goals so it may be made accessible only to a limited number of persons under strict control. Infringement of confidentiality has a considerable adverse effect on the image and corporate design of the company and involves economic consequences, e.g.: • considerable loss of clients • considerable fall in sales figures/turnover • claims for damages of various persons or organizations • exclusion from certain market areas • adverse effects in public assessment Examples: special types of personal data (e.g. health data), cycle plans, strategic corporate plans, prototype drawings

3.4.1.2. Integrity

Accurate information management and protection against unauthorized changes must be ensured.

In respect of the integrity of information, the following specific classification levels exist:

Classification	Definition
Low	Infringement of integrity has no foreseeable effect on business activities or the image or corporate design of the company.
Medium	Infringement of integrity has a slight effect on business activities or the image or corporate design of the company. It may involve adverse consequences, even if they are insignificant. Examples: • slight delay in work processes • defects that have no effect on work results (no loss in production) • no adverse effect on decisions • it is not probable that certain persons or organizations raise claims for damages Examples: site plans, organizational charts, certain internal telephone numbers
High	Infringement of integrity has a manifest effect on business activities or the image or corporate design of the company.

	It will presumably result in measurable adverse consequences, e.g.: • probable loss of clients • probable fall in sales figures/turnover • considerable delay in work processes • defect/deficient operation that has a manifest effect on work results (serious loss in production) and/or loss of certain service processes • adverse effect on decisions/probability of erroneous decisions • it is probable that certain persons or organizations raise claims for damages Examples: JIT orders, press communications, content of internet presence, production management data
Very high	Infringement of integrity has a considerable effect on business activities and/or the image or corporate design of the company and it involves corresponding consequences, e.g.: • considerable loss of clients • claims for damages of various persons or organizations • strong fall in sales figures/turnover • exclusion from certain market areas • considerable delay in work processes • defect/deficient operation that has a serious effect on work results and/or loss of several service processes (very serious loss in production) • considerably adverse effect on decisions/erroneous decisions Examples: preparation of the balance-sheet (e.g. annual financial statements), patents, cryptographic keys, payroll accounting

3.4.1.3. Availability

The information shall be available in the specified duration.

In respect of the availability of information, the following specific classification levels exist:

Classification	Definition
Low	Availability of the IT system shall not be less than 95% in respect of failures or unacceptable response times without causing a considerable disadvantage (material disadvantage or that affecting the corporate image). Example: Intranet application with general information for staff members
Medium	Availability of the IT system shall be minimum 95% in respect of failures or unacceptable response times. Lower availability gives rise to a considerable disadvantage (material disadvantage or that affecting the corporate image). Example: tenderer's portal
High	Availability of the IT system shall be minimum 98% in respect of failures or unacceptable response times. Lower availability gives rise to a considerable disadvantage (material disadvantage or that affecting the corporate image). Examples: payroll accounting, bookkeeping
Very high	Az IT-rendszer rendelkezésre állása kiesés vagy nem elfogadható válaszidők vonatkozásában legalább 99% kell legyen. Az alacsonyabb rendelkezésre állás jelentős (anyagi vagy a vállalatról kialakított képet érintő) hátrányhoz vezet. Example: IT system, the failure of which gives rise to direct stoppage of production.

	A considerable disadvantage might be, e.g.: • loss of customers • claims for damages of various persons, organizations, or associations • strong fall in sales figures/turnover • exclusion from certain market areas • defect/deficient operation that has a serious effect on work results and/or a loss of several service processes (very serious loss in production)

3.4.2. Marking and management of information

The information may be made accessible only to certain authorized persons for the purposes of the activities agreed upon, while the relevant regulations are simultaneously observed. At the same time the „need-to-know" principle shall be observed.

The information shall be protected against unauthorized access according to their current confidentiality classification during its entire lifetime. The following regulations are in force:

Classification	Regulations
Public	• Marking: none/optional (e.g. marking in the imprint) • The corporate requirements for placing of the marking of classification must be observed. • Reproduction and distribution: no restrictions • Storage: no restrictions • Erasure: no restrictions • Destruction: no restrictions
Internal	• Marking: The confidentiality level is given in the language of the country concerned/no or "internal" marking on the first page of the document • The corporate requirements for placing the marking of classification must be observed. • Reproduction and distribution: permitted only to the concern's authorized staff members and authorized third parties in the course of and/or within the scope of their activity • Storage: protection against unauthorized access • Erasure: the data that are no longer needed must be erased. • Destruction: regular destruction (see Appendix 7.2.5)
Confidential	• Marking: The level of confidentiality is given in the language of the country concerned/marking as "confidential" on each page of the document in an electronic or printed form • The corporate requirements for placing the marking of classification must be observed. • Reproduction and distribution: permitted only to the concern's authorized staff members and authorized third parties in the course of and/or within the scope of their activity. The person distributing the documents shall be responsible for the protection of the appropriate distribution channels against unauthorized access to the information and data and/or unauthorized interception (e.g. by encryption). • Storage: permitted only to the concern's authorized staff members and authorized third parties in the course of and/or within the scope of their activity (e.g. in a closed user group). Appropriate storage facilities and/or data storage devices must be used. • Confidential documents, if they are not needed, must be stored in a locked safety box or in a locked room that may be opened only by a specified group of authorized persons.

	• Erasure: the data that are no longer needed must be erased. • Destruction: regular destruction (see Appendix 7.2.5) • Authentication: Strong authentication (see Appendix 7.2.6) • Transport: Confidential information and data storage devices shall be dispatched in closed, neutral envelopes; if necessary, marked as "personal" which means that the envelope may be handed over directly to the specified recipient only.
Secret	• Marking: The level of confidentiality is given in the language of the country concerned/marking as "secret" on each page of the document • The corporate requirements for placing the marking of classification must be observed. • Besides, each page shall be marked as "page x/y". • Reproduction and distribution: a narrow group of the concern's authorized staff members (e.g. list of names) and authorized third parties in the course of and/or within the scope of their activity based on the information owner's prior consent. If it can be solved in technical terms, all data shall be encrypted according to the state-of-the-art technology. If it is not possible, a similarly strong security solution must be applied. Depending on application, additional technical and organizational measures shall be taken (e.g. prohibition of forwarding and printing, watermark). Appropriate channels suitable for communication and preventing interception (e.g. encrypted video conference) shall be used. • Storage: a narrow group of the concern's authorized staff members (e.g. list of names) and authorized third parties in the course of and/or within the scope of their activity (e.g. in a closed group of users). If it can be solved in technical terms, all data shall be encrypted according to the state-of-the-art technology. If it is not possible, a similarly strong security solution must be applied. • The encrypted documents shall be stored in a locked safety box to be equipped with separate locks. The mobile storage media containing secret information shall be stored in appropriate data guards. • Erasure: the data that are no longer needed must be erased. • Destruction: regular destruction (see Appendix 7.2.5) • Authentication: Strong authentication (see Appendix 7.2.6) • Transport: secret documents and data storage devices shall be dispatched in neutral, closed external envelopes (without marking as "personal", "secret" etc.) that shall contain another envelope marked as „secret", which is to contain the secret documents.

The requirements for management of information (marking, reproduction, distribution, storage, erasure and destruction) shall apply also to the IT systems (e.g. databases and security media) as appropriate.

3.4.3. Management of storage devices and storage media

Storage media (e.g. CDs, DVDs, USB storage devices and hard disks) shall be protected against loss, destruction and exchange, as well as unauthorized access.

The media storage devices used no longer shall be destructed in a secure way (see Appendix 7.2.5).

3.4.3.1. Exchange of information

In the course of all conversations affecting or containing confidential or secret information (including telephone, video and web conference conversations) it shall be ensured that no unauthorized persons can intercept such conversations.

In order to avoid that data are forwarded to any wrong place, fax numbers and e-mail addresses shall be obtained from the current lists or from the recipient.

When IT devices and storage media are transported outside the Customer's plant, the regulations of Customer shall be observed (see Appendix 7.2.7).

The responsibilty for the content and distribution of e-mail messages shall be borne by the sender and that for their further processing and distribution shall be borne by the recipient.

It is prohibited to generate and send chain e-mails.

3.5 Management of information security incidents

Any information security incident affecting the Customer's data or systems (e.g. errors occurring or infringement of the information security regulations) shall be immediately reported to the competent body (see Appendix 7.2.8).

The points supposed to be vulnerable, and the security gaps of the IT system shall be immediately reported to the competent body (see Appendix 7.2.9). Inspection of the vulnerable points and security gaps (e.g. intrusion detection) may only be carried out by the competent body (see Appendix 7.2.10).

The supposed loss of confidential or secret information shall be immediately reported to the competent body (see Appendix 7.2.11).

3.6 Compliance and adherence to statutory requirements

The service provider shall set up compliance management being in conformity with the legal and corporate requirements (including management of resources, an internal audit system, IT service continuity management and protection of information) to include the Customer's all information, hardware and software.

Compliance management shall consist of the following items.

3.6.1. Early risk recognition

Such a process shall be developed that allows early recognition of the risks and potential threats affecting the IT systems and data.

For the purposes of management of the recognized risks, preventive actions and measures shall be determined.

3.6.2. Intellectual property/licence management

All rights connected with intellectual property rights (e.g. copyrights for software, documents and graphics, design marks, trademarks, patents and source code licences) shall be respected and simultaneously observed.

Use of unlicensed software (pirate software) is prohibited.

The licensed software shall be subject to the statutory requirements for copyright (e.g. copying will be deemed as violation of copyright, except if it is made for security and archiving purposes).

Infringement of these provisions may involve criminal consequences and may result in a temporary measure or a claim for damages.

Licensed software may be used for the purpose agreed upon, in conformity with the effective regulations and the licence agreement concluded with the manufacturer.

3.6.3. Data protection

The effective data protection rules and regulations shall be observed (see Appendix 7.2.12).

The service provider's management shall require to oblige contributors to observe the statutory data protection regulations (see Appendix 7.2.12).

3.6.4. Compliance with the provisions of the contract

The service provider's IT organization shall observe the Customer's contractual requirements. In order to enforce the contractual requirements, measures allowing supervision and updating from time to time of the service provider's own organizational regulations should be taken.

3.6.5. Internal regulations

For the purposes of compliance with the requirements and appropriate management of the Customer's information, hardware and software, the service providers shall prescribe regulations and principles of conduct for their staff members.

3.7 Breach of and compliance with the rules

Any breach of the information security action directives shall be investigated in each case according to the corporate, contractual and statutory regulations and agreements and will result in the appropriate legal consequences.

4 Additional requirements for service providers having direct access to the concern's internal network

4.1 Definition

The service providers belonging to one of the following categories shall observe the following regulations:

- service providers whose clients (user devices) has been made available by a subsidiary of the Volkswagen concern
- service providers who have remote access (e.g. TravelX, Safe, Secure i.Do-Client) or direct access by another VPN solution to the Volkswagen Corporate Backbone (CBB)
- service providers who are directly connected to CBB
- service providers who are connected to CBB via PFN (Central supplier network (CSN))

The service providers may operate in the area of their own company and also in the area of a concern company.

4.2 Regulations

4.2.1. Internal organization

The service providers may implement or initiate provison or installation of hardware and software only in their competent special field (the Customer's special field).

Use of the hardware and software provided is subject to the regulations of Customer (see Appendix 7.2.13).

Opening of IT devices or changes in the hardware (e.g. removal/installation of hard disks, memory modules) and manual modifications of security settings (e.g. in the web browser) are permitted only to the competent bodies (see Appendix 7.2.14).

Use or subsequent modification of the client's programs is possible only if the competent body (see Appendix 7.2.14) has permitted it.

The IT devices provided must not be used for the processing of the data of customers who do not belong to the concern.

Use of the Customer's IT devices or data by the service provider's staff members shall be subject to the Customer's express consent. The client shall be entitled to ban access or use (e.g. in the case of an abuse).

4.2.2. Physical and environmental security

The devices provided shall be used properly for their intended purpose and shall be protected against loss or unauthorized modification.

The manufacturer's instructions intended to protect the devices shall be observed.

The devices provided by the Customer (e.g. laptops, cell phones) may be removed from the Customer's plant area only in possession of the relevant permit.

4.2.3. Protection against malicious software and mobile program codes

If any suspision of infection by a malware arises, the IT devices and storage media concerned must not be used further. The competent bodies shall be immediately informed (see Appendix 7.2.9).

4.2.4. Backup

Data shall not be stored on local drives only on the specified network drives as central and automatic backup copies can only be generated in the network.

The user shall be responsible for making backup copies of the data that are not available on central network drives (e.g. local hard disk, mobile storage media) or on systems of a similar function (e.g. eRoom, SharePoint).

Backup copies and media shall be managed just like original data.

4.2.5. Access control

4.2.5.1. Business requirements for access control

Each user shall observe the following requirements:

General requirements

- Use of another person's user ID or account is prohibited.
- Transmission of identification devices (e.g. SmartCards or SecurID cards) is prohibited.
- The passwords or PIN codes assigned to a user ID intended for personal use ("personal user IDs") must be kept in secret and must not be forwarded.
- Storage or writing of passwords (e.g. recording them on paper, in a mobile phone or in a file) is prohibited if it has not be defined as a secure method (see Appendix 7.2.15).

- If it is presumable that the security of a password or PIN code has been breached or somebody has had access to the password or PIN code, the data concerned must be changed immediately.
- Temporary passwords (e.g. for a new account) must be changed upon first login.
- Each password or PIN code must be changed after the first use and at the latest after lapse of one year (the latter requirement applies only to passwords).
- Spying of passwords is prohibited.
- Passwords must be classified at least as confidential.
- If the passwords should be stored in a written form, the staff members shall store them in an appropriate place protected against unauthorized use (e.g. in a safety box), in a closed envelope. The password so protected should be updated after each change. The staff member concerned has to sign the closed envelope. As in exceptional cases (e.g. sickness) a password may need to be used, the persons authorized to open the envelope should be indicated by name, whereby the "two-person" rule must be observed. Each opening shall be documented with simultaneous notification of the staff member. The staff member shall change and secure the password immediately after each opening. IT systems (e.g. electronic password storage) having similar functions may also be used as an alternative solution.
- If work before screen is interrupted (e.g. for a break or consultation), the system shall be locked (e.g. by a password-protected screen-saver).
- Users who use a multifunction certificate for logging in the IT systems must remove their certificate from the reader when they leave the system.

4.2.5.2. Generation of passwords

In the course of generating passwords the following requirements must be complied with:

- Upon access to the Customer's systems, the staff members (of the service provider) may not use the same password for work and private purposes.
- The staff members (of the service provider) may not use the same password for the systems provided by the Volkswagen concern and for systems provided by third parties (e.g. applications, internet registrations).
- The minimum length of passwords required by the systems should be observed. These requirements are in line with the provisions of the relevant regulations (see Appendix 7.1.2).
- Trivial passwords (e.g.: „Test123456") or passwords of personal relevance (e.g. names, date of birth) must not be used.
- Should the system or application require a complex password change (see Appendix 7.1.2), the instructions should be followed. Note: you may use key words or abbreviations or distortions for secure password selection (such as: „Each morning I go to the bathroom and have a thorough wash", the password is: „Emgb&htw"). In addition, the combination of four words (e.g. „DayTreeTeaButter") may also be a secure and easily memorized password. The examples mentioned here must not be used as a real password.

4.2.5.3. PIN codes for locking smartphones and tablets

4.2.5.4. PIN codes for authentication SmartCards

The instructions described in chapter 4.2.5.2 shall be observed.

4.2.5.5. Group IDs

Use of certain group IDs by several persons for several times (e.g. training department, trainees, higher education students) is permitted subject to compliance with the following conditions:

- The user ID is issued by a competent person who draws up a written protocol on who and at which time uses what user ID and archives the relevant protocol.
- The user concerned shall confirm receipt of the user ID. Such confirmation is kept by the person responsible for the user ID.
- After receipt of the user ID, the user concerned shall replace it by a password that is known only to him or her.
- After return of the user ID, the competent person shall replace it by a password that is known only to him or her.
- Archiving of protocols shall be subject to the archiving time-limits defined for the company.

Use of user IDs that can be used by several persons at the same time (so-called “group IDs”) is permitted only if they allow that only such only applications can be run that have own user management, including personal authentication, and provide access only for reading.

4.2.6. Control of access to the networks

4.2.6.1. Regulations for use of network providers

The IT devices provided by the Customer may be connected with external networks (e.g. hotspot, private WIFI, except mobile networks) only if and and to the extent as is required for creating the connection to the concern’s network (by remote access/via VPN). Direct “surfing” etc. is not permitted (except by smartphones and tablets connected to mobile networks).

Connections that are no longer required must be interrupted.

4.2.6.2. Device identification within the network

Unlimited connection between communication devices and the internal network (intranet) (e.g. without a firewall) is permitted only if they are provided by the concern or a company in which the concern or one of its companies has a majority interest.

5 Additional requirements for service providers not having direct access to the concern’s internal network

5.1 Definition

The service providers belonging to one of the following categories shall comply with the requirements defined in chapter 5:

- service providers who have no direct access to the network of a concern company
- service providers to whom no user devices owned by the Volkswagen concern are provided and who use only user devices owned by the service provider’s company
- service providers with whom no connection exists via Secure Partner, remote access or other VPN solution
- The virtual desktop solutions allowing forwarding of only screen contents and the related control data shall be subject to the requirements set out in this chapter.
- These service providers exchange data with Customer.

These service providers operate in the site of their own company and shall observe their own company’s regulations.

5.2 Regulations

5.2.1. Internal organization

The data of the concern companies shall be separated from third-party data, in particular from the data of other customers of the service providers (e.g. by management of rights). The data shall not be accessible by a third party (e.g. they need to be protected by encryption).

In order to implement all necessary security measures, classification of Customer shall be applied also in the service provider's classification scheme.

The service providers shall have appropriate security measures in place within their companies for the performance of their tasks in compliance with the information security requirements set out in the regulations delivered to them.

The service providers' staff members may have access to the Customer's data only based on the „need-to-know" principle.

6 Responsibilities

These regulations shall be observed by all service providers defined as such herein.
Any deviation from these action directives that causes a decrease in the security level is permitted only periodically and as agreed upon with the competent bodies (see Appendix 7.2.16) and with the Customer.

7 Appendix

7.1 Collectively valid documents

7.1.1. Corporate Directive U_2.024: Annex No. 6 – Information Security Action Directive for System Operators and Administrators

7.1.2. Regulation Nr. 03.01.05 – Identity and Access management

7.2 Company-specific definitions

7.2.1. Personal data (e.g. name, phone number, e-mail address, date of birth) may be collected, processed or used only in accordance with the statutory and corporate regulations relating to the protection of personal data.

The personal data stored by Customer may only be used for work, if the personal data serve achieving of professional goals. Transfer of personal data to unauthorized third parties (e.g. customers, partner companies' staff members, colleagues) is prohibited.

The information available for classification of personal data is accessible in Audi Mynet at: Companies / Audi Hungaria / Organization / Central functions / IT security / IT security processes / Business criticality classification (BKE) / Documents / Data Classification Template

The IT devices and storage media on which personal, confidential or secret data are stored, may leave the area of Customer only in an encrypted form.

7.2.2. http://www.vwgroupsupply.com

7.2.3. AUDI HUNGARIA ServiceDesk, Tel. 1400.

7.2.4. Responsibility: AUDI HUNGARIA External communication/PR (G/GP-1) organizational unit

7.2.5. Personal, confidential and secret paper-based documents must be removed in a secure way (e.g. in data protection containers). Storage media used no longer must be erased in a reliable way, by overwriting or must be physically destructed.

7.2.6. In respect of all data of the Customer subject to confidentiality, the authentication procedures available in section 8.1 of „Corporate Directive U_2.024 – Annex No. 6 – Information Security Action Directive for System Operators and Administrators" are permitted depending on their classification.

7.2.7. The IT devices and storage media on which the personal, confidential or secret data of Customer are stored may leave the plant area of Customer, as a rule, only in an encrypted form.

7.2.8. AUDI HUNGARIA ServiceDesk, Tel. 1400.

7.2.9. IT-Security
7.2.10. IT-Security
7.2.11. IT-Security, Know-how Protection, Audi Hungaria's data protection officer.

7.2.12. REGULATION (EU) 2016/2016 of the EUROPEAN PARLIAMENT and of the COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – "GDPR"), as well as Act CXII of 2011 on Informational Self-Determination and Freedom of Information and other relevant legislation.

7.2.13. Each service provider shall be responsible for the regular use and application of the information, programs and IT devices only for corporate purposes and within the scope of the order for the relevant task.

7.2.14. Responsibility: Solution Center Infrastructure/End User Computing

7.2.15. Use of password safety boxes, e.g. KeePass is recommended.
7.2.16. It-Sicherheit@audi.hu