Guideline
准则
Information Security
Valid from 2023/03/01
有效期自 2023/03/01
Version 1.0
版本 1.0

Published by
发布
P/BT *IT*

Guideline manager
政策经理
P/BT *IT*
Garcia Sotelo, Jorge Carlos (CIO)
P/BT *IT*
Garcia Sotelo，Jorge Carlos (CIO)

Other contacts
其他联系人
P/BT-Z *IT Governance, IT Security, BPM*
Begolli, Genc (CISO)
P/BT-Z *IT 管理、IT 安全、BPM*
Begolli，Genc (CISO)

GUIDELINE

准则

INFORMATION SECURITY GUIDELINES FOR EXTERNAL COMPANIES

外部公司信息安全准则

PURPOSE

目的

These Information Security Guidelines comprise the information security regulations that suppliers must observe when using information and/or IT devices (e.g. personal computers, workstations and mobile devices) of the ordering party.

这些信息安全准则包括供应商在使用订购方的信息及/或 IT 设备（如个人电脑、工作站及移动设备）时必须遵守的信息安全规定。

Suppliers are defined as any third party companies that are providing services to the Volkswagen Group based on a contractual relationship. Subsidiary companies, Brands of the Volkswagen Group and companies that are majority owned by the Volkswagen Group are excluded from this definition. These guidelines are aimed at the suppliers' management, employees and relevant sub-contractors. This group is hereinafter referred to as the "contractor".

供应商是指根据合同关系向大众汽车集团提供服务的任何第三方公司。 大众汽车集团的子公司、品牌和大众汽车集团拥有多数股权的公司不在这一定义范围内。 这些准则针对供应商管理层、员工及相关分包商。 本集团以下称为“承包商”。

The Information Security Guidelines protect the confidentiality, integrity and availability of information and the rights and interests of the ordering party and all natural persons and legal entities that maintain a business relationship with the ordering party and/or perform work for it.

信息安全准则保护信息的机密性、完整性和可用性，并保护订购方和与订购方保持业务关系和/或为其工作的所有自然人和法人实体的权益。

DOCUMENT STRUCTURE AND TARGET AUDIENCE

文件结构和目标受众

The document contains three chapters. The following table lists the document structure and the target audience for each chapter.

本文件包含三章。 下表列出了文件结构和每章的目标受众。

Chapter **章节**	**Chapter** **章节**	**Chapter** **章节**
1	All Suppliers	The requirements of this chapter must be observed by all suppliers. Additional

	所有供应商	requirement are contained in chapters two and three, depending on the type of access to the Group network or systems 所有供应商都必须遵守本章的要求。 第二章和第三章载有其他要求，具体取决于对集团网络或系统的访问类型
2	Suppliers that have access to the Group network or systems 有权访问集团网络或系统的供应商	Additionally, the requirements contained in chapter 1 must be observed 此外，必须遵守第 1 章中的要求
3	Suppliers that do not have access to the Group network or systems 无权访问集团网络或系统的供应商	Additionally, the requirements contained in chapter 1 must be observed 此外，必须遵守第 1 章中的要求

1

BASIC REQUIREMENTS

基本要求

The following requirements must be observed by all suppliers within the scope of this document.

本文件范围内的所有供应商必须遵守以下要求。

Requirements for the ordering party are not within the scope of this document.

对订购方的要求不在本文件的范围内。

1.1 ORGANIZATIONAL REQUIREMENTS

1.1 组织要求

Regulations of the respective Group Company on bringing IT devices that do not belong to the ordering party on the companies' premises or secure areas must be observed.

必须遵守各集团公司关于将不属于订购方的 IT 设备带入公司场所或安全区域的规定。

Usage of software or data belonging to the ordering party on IT systems or storage devices that are not provided or approved by either the ordering party or the supplier is not permitted.

不允许在非订购方或供应商提供或批准的 IT 系统或存储设备上使用属于订购方的软件或数据。

Usage of software and data belonging to a Volkswagen Group Company on file-services or internet cloud-services that are not approved by the ordering party is not permitted.

不允许在未经订购方批准的文件服务或互联网云服务上使用属于大众汽车集团公

司的软件和数据。

The distribution of data to third parties is only permitted with written approval by the data owner of the ordering party.

只有获得订购方数据所有者的书面批准，才允许向第三方分发数据。

The regulations of the ordering party for usage, storage and any processing of personal data must be observed:

必须遵守订购方关于个人数据的使用、存储和处理的规定：

- The collection, processing or usage of personal details (e.g. name, phone number, e-mail address, date of birth) is only permissible provided that the consent of the party involved (individual) has been obtained or there is a legal basis for it.
- 收集、处理或使用个人信息（如姓名、电话号码、电子邮箱地址、出生日期）必须获得相关方（个人）的同意或有法律依据。
- The handling and usage of personal data stored at Audi FAW NEV is only allowed to act within the scope of ones duties. An transmission of these data is not allowed to unauthorized third person (e. g. customers, external employees, employees).
- 奥迪一汽新能源汽车有限公司所存储的个人数据的处理和使用仅限于职责范围内。 不允许向未经授权的第三方（如客户、外聘人员、员工）传输这些数据。
- In principle, communication devices and data media, on which personal, confidential or secret data of the ordering party are stored, may only leave the Audi FAW NEV site in an encrypted form.
- 原则上，存储订购方个人数据、机密数据或秘密数据的通信设备和数据媒体在离开奥迪一汽新能源汽车有限公司时必须进行加密。

Employees of the contractor must be obligated by their company management to non-disclosure in accordance with the non-disclosure agreement between the contractor and the ordering party. The ordering party may inspect these agreements at any time.

承包商的员工必须由其公司管理层根据承包商和订购方之间的保密协议承担保密义务。 订购方可随时查阅这些协议。

If data of the ordering party is stored on mobile systems or IT devices it must be encrypted using current state of technology hardware or software. Additional requirements for encryption and authentication can be found on the Group Suppliers Portal1.

如果订购方的数据存储在移动系统或 IT 设备上，则必须使用最新技术水平的硬件或软件对其进行加密。 有关加密和身份验证的其他要求可在集团供应商门户 1 上找到。

Before travel abroad, the country specific regulations for use of security technologies (e.g., encryption) must be observed.

出国旅行前，必须遵守特定国家/地区有关使用安全技术（例如加密）的规定。

After end of the contract, data of the ordering party must be handed over and deleted on the devices and storage media of the supplier. Legal requirements (e.g. retention periods) must be observed.

合同终止后，必须移交订购方的数据并从供应商的设备和存储媒体上删除。 必须遵守法律要求（如保留期）。

1.2 HUMAN RESOURCES SECURITY

1.2 人力资源安全

A user ID that is no longer needed or access authorization that is no longer needed for access to data of the ordering party must be reported promptly to the ordering party and responsible units (e.g. responsible user administrator of the ordering party), so that the corresponding Blocking/Deletion can occur.

对于访问订购方的数据，不再需要的用户 ID 或不再需要的访问授权必须及时报告给订购方和责任单位（例如订购方的相关用户管理员），以便进行相应的封存/删除。

Identification media that is no longer needed (e.g., Smartcards, SecurID cards) must be returned immediately to the ordering party.

不再需要的身份验证媒体（如智能卡、SecurID 卡）必须立即归还给订购方。

Allocated devices (e.g. laptops), data and storage media must be returned to the ordering party when they are no longer needed or at the end of the assignment.

分配的设备（如笔记本电脑）、数据和存储媒体在不再需要或任务结束时必须归还给订购方。

The loss of IT devices or media for authentication must be immediately reported to the responsible unit of the ordering party: Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn***

如果丢失了用于身份验证的 IT 设备或媒体，必须立即报告给订购方的责任单位：奥迪一汽新能源汽车有限公司 IT 用户服务部 ***it.uhd@audi-faw-nev.com.cn***

1.3 PHYSICAL AND ENVIRONMENTAL SECURITY

1.3 物理和环境安全

IT devices that store or process data of the ordering party must be used in a way that prevents unauthorized persons to view or access this data. Special care must be taken when using mobile devices.

存储或处理订购方数据的 IT 设备的使用方式必须防止未经授权的人员查看或访问这些数据。 使用移动设备时必须特别小心。

Confidential and secret documents must not be left unattended to prevent unauthorized viewing.

机密和秘密文件不得无人看管，以防止未经授权的人员查看。

1.4 ASSET MANAGEMENT

1.4 资产管理

1.4.1 Classification guidelines

1.4.1 分类准则

Classification includes the three security objectives confidentiality, integrity and availability and must be carried out for all information and IT Systems processing information.

分类有机密性、完整性和可用性三个安全目标，必须对所有信息和处理信息的 IT 系统进行分类。

The supplier must request the confidentiality, integrity and availability classification from the ordering party (for the scope of the services or work provided).

供应商必须要求订购方提供机密性、完整性和可用性分类（针对所提供服务或工作的范围）。

Information (security objective confidentiality) must be protected from unauthorized access throughout its entire life cycle in accordance with measures required by its confidentiality classification. Confidentiality classification may include an expiration date.

信息（机密性安全目标）的机密性分类措施必须能够在其整个生命周期内防止未经授权的访问。 机密性分类可以包括到期日期。

For processing data the classification for integrity and availability must be examined and determined by the respective process owner, if necessary. This classification must be evaluated regularly and adapted if necessary.

关于处理数据，必要时必须由相应的流程所有者检查和确定完整性和可用性的分类。 必须定期评估此分类并在必要时进行调整。

Correctness of the classification must be confirmed by the Information Owner.

分类的正确性必须由信息所有者确认。

1.4.1.1 Confidentiality

1.4.1.1 保密性

Information that is not intended for general publication must be made accessible only to those who are authorized to access it (Need to Know Principle).

非一般性信息必须仅供获得授权的人员访问（按需知密原则）。

Requirements for information creators and information owners:

信息创建者和信息所有者的要求：

- Newly created information and data must be labeled by the creator. The information creator is the person or group of people creating an information or document. The creator must classify/label the document or information in accordance to the classification level determined by the information owner.
- 新创建的信息和数据必须由创建者标记。 信息创建者是创建信息或文件的个人或群体。 创建者必须根据信息所有者确定的分类级别对文件或信息进行分类/标记。
- The information owner is responsible for the classification. The information owner is the person or group of people who have been identified by management as having responsibility for the maintenance of the confidentiality of that information. The information owner may change during

the lifecycle of the information.

» 信息所有者负责分类。 信息所有者是被管理层确定为有责任维护该信息机密性的个人或群体。 在信息的生命周期中，信息所有者可能会发生变化。

» The creator must request the correct classification from the information owner.

» 信息创建者必须要求信息所有者进行正确的分类。

» Confidentiality classification must be defined for all IT systems.

» 必须将所有 IT 系统定义为机密性分类。

» If the classification is currently unclear, for example, because the document / IT system was just newly created, the classification “Confidential” must be used.

» 如果当前分类不明确，例如，在文件/IT 系统刚刚新建时，则必须使用“机密性”分类。

» The Information owner must check the confidentiality classification for internal / confidential / secret information (at the latest during next revision or update) if the classification is still correct and label the information accordingly.

» 分类正确时，信息所有者必须检查内部/机密/秘密信息的机密性分类（最迟在下一次修订或更新时），并相应地标记信息。

Requirements for the recipient:

信息接收者的要求：

» Unlabeled information and data is defined as internal.

» 必须将未标记的信息和数据定义为内部信息。

» The information owner must be contacted if there are any doubts about the correctness of the classification.

» 如果对分类的正确性有任何疑问，必须联系信息所有者。

The following classification levels for information with regard to requirements for confidentiality are defined:

信息的机密性级别分类要求如下所述：

Classification **分类**	**Definition** **定义**
Public **公开**	Information that is not subject to any restrictions and, e.g., can be published by the company in newspapers or in the internet. 不受任何限制的信息，例如公司可以在报纸或互联网上发布的信息。 The public use of company information requires the approval of the responsible unit: Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn.*** 公开使用公司信息须经责任单位批准： 奥迪一汽新能源汽车有限公司IT用户服务部***it.uhd@audi-faw-nev.com.cn。***

	Examples: press releases, product catalog for customers 例如，新闻稿、客户产品目录
Internal **内部**	Unauthorized knowledge, sharing or usage of this Information only has minor influence on reaching product or project targets. Therefore, this information can be made accessible to an eligible group of persons. 未经授权知悉、共享或使用这些信息对达到产品或项目目标的影响很小。 因此，这些信息可以提供给符合条件的人群。 Loss of confidentialitymay have consequences, albeit of a minor nature; for example: 失去机密性可能会产生轻微后果；例如： » claims for damages by individual persons or organizations are unlikely » 个人或组织可能不会提出损害索赔 Examples: business communication data (e.g. phone number, mail-address), occupational safety specifications, work regulations 例如，业务通信数据（如电话号码、电子邮箱地址）、职业安全规范、工作规定
Confidential **机密**	Information whose knowledge or disclosure to unauthorized persons could jeopardize the achieving of product and project objectives and must therefore only be made accessible to a limited group of authorized persons. 让未经授权的人员获知信息或向其披露信息可能会危及产品和项目目标的实现，因此只能向有限的获授权群体提供信息。 Consequences in the event of loss of confidentiality are probable and measurable, e.g.: 失去机密性可能会造成可衡量的后果，例如： » loss of customers » 客户流失 » downturn in sales figures/turnover » 销售数据/营业额下滑 » claims for damages by individual persons or organizations » 个人或组织提出损害索赔 Examples: personal data, that are above business communication data (e.g. salary) budget plans, revision reports 例如，超出业务通信数据范围的个人数据（例如薪资）、预算计划、修订报告
Secret **秘密**	Information whose knowledge or disclosure to unauthorized persons could seriously jeopardize the achieving of company objectives and must therefore be subject to a highly restrictive distribution list and strict controls. 让未经授权的人员获知信息或向其披露信息可能会严重危及公司目标的实现，因此必须遵守严格限制的收件人列表和严格控制措施。 Violation of confidentiality has considerable effects on the image/the

	appearance of the company and/or economic consequences, e.g.: 违反机密性规定会对公司的形象和/或经济造成相当大的影响，例如： » considerable loss of customers » 大量客户流失 » sharp declines in sales figures/turnover » 销售数据/营业额急剧下降 » claims for damages by numerous persons or organizations » 许多个人或组织提出损害索赔 » exclusion from certain markets » 一些市场排斥 » negative effects on public standing » 负面公众形象 Examples: special types of personal data (e.g. health information), cycle plans, plans about the company's strategy, design picture of prototypes 例如，特殊的个人数据（例如健康信息）、周期计划、公司战略计划、原型设计图片

1.4.1.1 Integrity

1.4.1.1 完整性

Error-free information processing and protection against unauthorized changes must be ensured.

必须确保信息处理无错误并防止未经授权的更改。

The following classification levels for information with regard to requirements for integrity are defined:

信息的完整性级别分类要求如下所述：

Classification **分类**	**Definition** **定义**
Low **低**	A violation of integrity has no foreseeable effects on the business activity or on the image/appearance of the company. 失去完整性不会对业务活动或公司形象产生可预见的影响
Medium **中**	A violation of integrity has only a minor impact on business activity and/or the image/appearance of the company. 失去完整性会对业务活动和/或公司形象产生轻微影响。 Consequences are possible, but minor in nature; for example: 可能会造成轻微后果；例如： » Minor delays in work processes » 工作流程中的轻微延误 » Errors/faults do not affect work results (no production

	downtimes) » 不影响工作结果的错误/故障（无生产停机时间） » Decisions are not negatively affected » 决策不会受到负面影响 » Claims for damages by individual persons or organizations are unlikely » 个人或组织可能不会提出损害索赔 Examples: location plans, organization charts, and individual internal phone numbers 例如，位置图、组织结构图和个人内部电话号码
High **高**	A violation of integrity has perceivable effects on the business activity and/or on the image/appearance of the company. 失去完整性会对业务活动和/或公司形象产生明显影响。 Consequences are probable and measurable, e.g.: 可能会造成可衡量的后果，例如： » loss of customers probable » 可能的客户流失 » downturn in sales figures/turnover probable » 可能的销售数据/营业额下滑 » definite delay in work sequences » 工作流程中的明显延迟 » faults/malfunctions have a perceptible effects on work results (high production downtimes) and/or a few service processes fail » 对工作结果有明显影响的错误/故障（生产停机时间长）和/或一些服务流程错误 » decisions are negatively affected/incorrect decisions are probable » 决策受到负面影响/可能做出不正确的决策 » claims for damages by individual persons or organizations are probable » 个人或组织可能提出损害索赔 Examples: JIT orders, press releases, contents of the Internet presence, data for production control 例如： JIT订单、新闻稿、网站内容、生产控制数据
Very high **极高**	A violation of integrity has considerable effects on the business activity and/or on the image/appearance of the company with corresponding consequences, e.g., 失去完整性会对业务活动和/或公司的形象产生相当大的影响，并造成相应的后果，例如： » considerable loss of customers » 大量客户流失

	» claims for damages by numerous individual persons or organizations » 许多个人或组织提出损害索赔 » sharp declines in sales figures/turnover » 销售数据/营业额急剧下降 » exclusion from certain markets » 一些市场排斥 » considerable delays in work sequences » 工作流程中的严重延迟 » faults/malfunctions have severe effects on work results and/or several service processes fail (very high production downtimes) » 对工作结果有严重影响的错误/故障和/或数个服务流程错误（生产停机时间非常长） » decisions are seriously negatively affected/incorrect decisions » 决策受到严重的负面影响/不正确的决策 Examples: financial reporting (e.g., annual financial statement), patents, cryptographic keys, payroll 例如，财务报告（如年度财务报表）、专利、密钥、工资表

1.1.1.1 Availability

1.1.1.1 可用性

Information must be made available within an agreed time frame.

必须在约定的时间范围内提供信息。

The following classification levels for information with regard to requirements for availability are defined:

信息的可用性级别分类要求如下所述：

Classification **分类**	**Definition** **定义**
Low **低**	The availability of the IT system can be less than 95 percent regarding failure or unacceptable response time without resulting in significant damage (financial or to the image of the company). 对于错误或不可接受的响应时间，IT系统的可用性可以低于95%，但不会造成重大损害（财务或公司形象）。 Example: Intranet application containing general information for employees 例如： 包含员工一般信息的内联网应用程序
Medium **中**	The availability of the IT system must be at least 95 percent regarding failure or unacceptable response time. Lower availability will lead to significant damage (financial or to the image of the company).

	对于错误或不可接受的响应时间，IT系统的可用性必须至少为95%。较低的可用性会导致重大损害（财务或公司形象）。 Example: Applicant portal 例如： 申请门户
High 高	The availability of the IT system must be at least 98 percent regarding failure or unacceptable response time. Lower availability will lead to significant damage (financial or to the image of the company). 对于错误或不可接受的响应时间，IT系统的可用性必须至少为98%。较低的可用性会导致重大损害（财务或公司形象）。 Examples: Payroll, bookkeeping 例如： 工资表、簿记
Very high 极高	The availability of the IT system must be at least 98 percent regarding failure or unacceptable response time. Lower availability will lead to significant damage (financial or to the image of the company). 对于错误或不可接受的响应时间，IT系统的可用性必须至少为98%。较低的可用性会导致重大损害（财务或公司形象）。 Example: IT system, whose failure will result in an immediate production halt. 例如： IT系统，其故障将导致立即停产。 Significant damage is, for example: 重大损害例如： » Loss of customers 客户流失 » Claims for damages by numerous individual persons or organizations or associations 许多个人、组织或协会提出损害索赔 » Sharp declines in sales figures/turnover 销售数据/营业额急剧下降 » Exclusion from certain markets 一些市场排斥 » Faults/malfunctions have severe effects on work results and/or several service processes fail (very high production downtimes) 对工作结果有严重影响的错误/故障和/或数个服务流程错误（生产停机时间非常长）

1.1.2 Information labeling and handling

1.1.2 信息标记与处理

Information must only be made accessible to the authorized group of persons. This is only permissible in the scope of the tasks agreed on and with compliance to existing regulations. The "Need to know" principle must be

applied.

必须仅由获授权群体访问信息。 只有在商定的任务范围内并遵守现有规定的情况下才允许这样做。 必须采用“按需知密”原则。

Information must be protected against access by unauthorized persons according to its current confidentiality classification during the entire life cycle. The following regulations apply:

必须根据当前的机密性分类保护信息，在其整个生命周期内防止未经授权的访问。 以下规定适用：

Classification **分类**	**Definition** **定义**
Public **公开**	» Labeling: none / optional (e.g. in imprint) 标记：无/可选（例如在印刷时） » The corporate design guidelines regarding the position of the classification label must be observed 必须遵守关于分类标签位置的公司设计准则 » Duplication and distribution: no restrictions 复制和分发：无限制 » Storage: no restrictions 存储：无限制 » Deletion: no restrictions 删除：无限制 » Disposal: no restrictions 处置：无限制
Internal **内部**	» Labeling: Confidentiality level in national language/none or Internal on the first page of the document. » 标记： 在文件的第一页上用本国语言标注机密性级别/无或“内部” » The corporate design guidelines regarding the position of the label must be observed » 必须遵守关于标签位置的公司设计准则 » Duplication and distribution: only to authorized group employees and authorized third parties within the task or application area » 复制和分发：仅在任务或应用领域的范围内获授权的集团员工和获授权的第三方 » Storage: protection against unauthorized access » 存储：防止未经授权的访问 » Deletion: data that are no longer needed must be deleted. » 删除：不再需要的数据必须删除。 » Disposal: proper disposal: Personal related, confidential and secret paper documents must be disposed of in secure way (e. g. document containers). Data carriers that are no longer needed

	must be deleted reliably by overwriting or be physically destroyed. » 处置：妥善处置： 与个人相关的、机密的和秘密的纸质文件必须以安全的方式处置（例如文件容器）。 不再需要的数据载体必须以可靠的方式通过覆写或物理销毁来删除。
Confidential **机密**	» Labeling: Confidentiality level in national language/confidential" indicated on each page of the document in electronic and printed form » 标记： 在电子文件和印刷文件的每一页上用本国语言标注机密性级别/“机密” » The corporate design guidelines regarding the position of the label must be observed. 必须遵守关于标签位置的公司设计准则。 » Duplication and distribution: Only to a limited range of authorized group employees and authorized third parties within the task and application area. The person distributing the information is responsible for using suitable distribution routes, in order to protect the information and data from unauthorized access and/or unauthorized overhearing (e.g., encryption). » 复制和分发： 仅在任务或应用领域的范围内有限的获授权的集团员工和获授权的第三方 信息分发人员有责任使用合适的分发途径，以保护信息和数据免遭未经授权的访问和/或未经授权的窃取（例如采用加密）。 » Storage: only accessible to a limited range of authorized group employees and authorized third parties within the task and application area (e.g., by closed user groups). Suitable storage locations and/or storage media must be used. » 存储：仅在任务或应用领域的范围内有限的获授权的集团员工和获授权的第三方（例如闭合用户群）。 必须使用合适的存储位置和/或存储媒体。 » Confidential documents must be stored in locked steel furniture or in rooms that are locked when they are not in use and which can only be opened by a restricted group of people. » 机密文件必须存放在上锁的钢制家具中，或者存放在不使用时上锁的房间中，只能由有限的群体打开。 » Deletion: data that are no longer needed must be deleted. » 删除：不再需要的数据必须删除。 » Disposal: proper disposal: Personal related, confidential and secret paper documents must be disposed of in secure way (e. g. document containers). Data carriers that are no longer needed must be deleted reliably by overwriting or be physically destroyed. » 处置：妥善处置： 与个人相关的、机密的和秘密的纸质文件必须以安全的方式处置（例如文件容器）。 不再需要的数据载体必须以可靠的方式通过覆写或物理销毁来删除。 » Authentication: Strong Authentication For internal, confidential or secret data of the ordering party the following authentication methods are permitted: » 身份验证： 强身份验证

对于订购方的内部、机密或秘密数据，允许使用以下身份验证方法：

Authentication class **身份验证等级**	**Authentication class** **身份验证等级**	**Authentication class** **身份验证等级**
Strong authentication 强身份验证	Secret or Confidential 秘密或机密	2 of 3 (knowledge, possession, quality criteria), e. g.: 三选二（知悉、拥有、质量标准），例如： Authentication via VOLKSWAGEN PKI Card with PIN without a time component or biometric component 通过大众汽车PKI卡进行身份验证，有PIN码，无时间组件或生物识别组件 One-Time-Password Token (e.g. SecurID card) with PIN-Pad 一次性动态密码（如SecurID卡），有密码键盘 One-Time-Password Token (e.g. SecurID card) without PIN-Pad with PIN-request 一次性动态密码（如SecurID卡），无密码键盘，要求输入PIN码
Weak authentication 弱身份验证	Internal 内部	1 of 3 (knowledge, possession, quality criteria), e. g.: 三选一（知悉、拥有、质量标准），例如： One-Time-Password Token (e.g. SecurID card) without PIN-Pad without PIN-request 一次性动态密码（如SecurID卡），无密码键盘，不要求输入PIN码 Software certificate with/without passphrase 带/不带密码的软件证书 central defined User-ID with password 带有密码的中央定义用户ID

	» Transportation: Confidential documents and storage media must be sent in sealed neutral envelopes; if appropriate “personal” may be added, meaning that the documents can only be handed to the named recipient. » 运输： 机密文件和存储媒体必须用密封的中式信封发送；在适当的情况下，可以标注“个人”，这意味着文件仅能交给指定的收件人。
Secret **秘密**	» Labeling: Confidentiality level in national language/Secret" indicated on each page of the document. » 标记： 在文件的每一页上用本国语言标注机密性级别/“秘密” » The corporate design guidelines regarding the position of the label must be observed. » 必须遵守关于标签位置的公司设计准则。 » Also, each page must indicate page x of y. » 此外，必须在每一页上标注“第 x 页，共 y 页”。 » Duplication and distribution: Only to an extremely limited range (e.g., list of names) of authorized group employees and authorized third parties within the task or application area after prior approval by the information owner. If technically possible data has to be encrypted according to the current state of technology. Comparable security solutions have to be used if this is not possible. Additional case-related technical or organizational protective measures must be implemented (e.g., denying forwarding or printing, watermarks). Suitable communication media must be used in order to prevent listening in (e.g., encrypted video conference). » 复制和分发： 在信息所有者事先批准后，仅在任务或应用领域的范围内十分有限的获授权的集团员工和获授权的第三方（例如使用名单）。 如果技术上可行，必须使用最新技术对数据进行加密。 如果不可行，必须使用类似的安全解决方案。 必须实施其他与案例相关的技术或组织保护措施（例如，拒绝转发或打印、水印）。 必须使用合适的通信媒体以防止偷听（例如加密视频会议）。 » Storage: only accessible to an extremely limited range (e.g., list of names) of authorized group employees and authorized third parties within the task or application area (e.g., by closed user groups). If technically possible data must be encrypted according to the current state of technology. Comparable security solutions have to be used if this is not possible. » 存储：仅在任务或应用领域的范围内十分有限的获授权的集团员工和获授权的第三方（例如闭合用户群）（例如使用名单）。 如果技术上可行，必须使用最新技术对数据进行加密。 如果不可行，必须使用类似的安全解决方案。 » Secret documents must be stored in locked steel furniture locked with different locks to the standard locks. Mobile Storage devices with secret information must be stored in appropriate data safes. » 秘密文件必须存放在用非标准锁上锁的钢制家具中。 包含秘密信息的移动存储设备必须存放在适当的数据保险箱中。 » Deletion: data that is no longer needed must be deleted » 删除：不再需要的数据必须删除 » Disposal: proper disposal (see ap

» 处置：妥善处置：（见 ap

» Authentication: Strong Authentication

For internal, confidential or secret data of the ordering party the following authentication methods are permitted:

» 身份验证： 强身份验证

对于订购方的内部、机密或秘密数据，允许使用以下身份验证方法：

Authentication class **身份验证等级**	**Authentication class** **身份验证等级**	**Authentication class** **身份验证等级**
Strong authentication 强身份验证	Secret or Confidential 秘密或机密	2 of 3 (knowledge, possession, quality criteria), e. g.: 三选二（知悉、拥有、质量标准），例如： Authentication via VOLKSWAGEN PKI Card with PIN without a time component or biometric component 通过大众汽车PKI卡进行身份验证，有PIN码，无时间组件或生物识别组件 One-Time-Password Token (e.g. SecurID card) with PIN-Pad 一次性动态密码（如SecurID卡），有密码键盘 One-Time-Password Token (e.g. SecurID card) without PIN-Pad with PIN-request 一次性动态密码（如SecurID卡），无密码键盘，要求输入PIN码
Weak authentication 弱身份验证	Internal 内部	1 of 3 (knowledge, possession, quality criteria), e. g.: 三选一（知悉、拥有、质量标准），例如： One-Time-Password Token (e.g. SecurID card) without PIN-Pad without PIN-request 一次性动态密码（如SecurID卡），无密码键盘，不要求输入PIN码 Software certificate

				with/without passphrase 带/不带密码的软件证书 central defined User-ID with password 带有密码的中央定义用户ID

» Transportation: Secret documents and storage media must be placed in a closed neutral outer envelope (no additions such as “personal”, “secret”, or similar) with another inner envelope labelled “secret” inside. In the inner envelope must be the secret content.

» 运输： 机密文件和存储媒体必须使用一个密封的中式外信封（不得标注“个人”、“秘密”或类似内容）和一个标注“秘密”的内信封。 内信封里必须是秘密内容。

The regulations for handling information (labeling, duplication, distribution, storage, deletion and disposal) also apply to IT systems (e.g., for databases, backup media).

信息处理（标记、复制、分发、存储、删除和处置）的规定也适用于 IT 系统（例如数据库、备份媒体）。

1.1.3 Media handling

1.1.3 媒体处理

Data media (e.g., CDs, DVD, USB sticks, hard drives) must be secured against loss, destruction, and mix-ups, as well as against access by unauthorized parties.

数据媒体（例如 CD、DVD、U 盘和硬盘）必须防止丢失、毁坏和混淆，以及防止未经授权访问。

Data media that are no longer needed must be sent to secure disposal: Personal related, confidential and secret paper documents must be disposed of in secure way (e. g. document containers). Data carriers that are no longer needed must be deleted reliably by overwriting or be physically destroyed.

不再需要的数据媒体必须以安全的方式处置： 与个人相关的、机密的和秘密的纸质文件必须以安全的方式处置（例如文件容器）。 不再需要的数据载体必须以可靠的方式通过覆写或物理销毁来删除。

1.1.3.1 Exchange of information

1.1.3.1 信息交流

During all discussions of confidential or secret information, including telephone calls and web- or video conferences, it must be ensured that these cannot be overheard without authorization.

在讨论机密或秘密信息时，包括电话和网络或视频会议，必须确保这些信息不会在未经授权的情况下被偷听。

Fax numbers and e-mail addresses must be taken from current communication directories or requested from the recipient to prevent data from being transferred incorrectly.

传真号码和电子邮箱地址必须取自当前通信目录或向收件人索取，以防止数据传输出错。

For transport of IT devices and data media beyond the plant boundaries of the ordering party, the regulations and operating agreements of the respective group company must be observed. In principle, communication devices and data media, on which personal, confidential or secret data of the Audi FAW NEV are stored, may only leave the Audi FAW NEV site in an encrypted form.

如将 IT 设备和数据媒体运输到订购方工厂边界之外，必须遵守相应集团公司的规定和运营协议。 原则上，存储奥迪一汽新能源汽车有限公司个人数据、机密数据或秘密数据的通信设备和数据媒体在离开奥迪一汽新能源汽车有限公司时必须进行加密。

As the originator of an e-mail, the author is responsible for the content and distribution; the receiver for further processing and further distribution of an e-mail.

作为电子邮件的发起人，作者对电子邮件的内容和分发负责；接收者负责进一步处理和分发电子邮件。

The creation and sending of chain letters is not permissible.

不允许创建和发送连锁信。

1.2 INFORMATION SECURITY INCIDENT MANAGEMENT

1.2 信息安全事件管理

Information security events (e.g., vulnerabilities, violations of the Information security regulation) concerning data or systems of the ordering party must be reported immediately to the responsible unit Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn.***

有关订购方数据或系统的信息安全事件（如漏洞、违反信息安全规定）必须立即报告给责任单位奥迪一汽新能源汽车有限公司 IT 用户服务部 ***it.uhd@audi-faw-nev.com.cn。***

Suspected vulnerabilities and weak points concerning IT systems of the ordering party must be reported to the responsible unit Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn***. Testing of vulnerabilities and weak points (e.g. penetration testing) must only be performed by the responsible unit Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn***.

有关订购方 IT 系统的可疑漏洞和弱点必须报告给责任单位奥迪一汽新能源汽车有限公司 IT 用户服务部 ***it.uhd@audi-faw-nev.com.cn***。 漏洞和弱点测试（如渗透测试）只能由责任单位奥迪一汽新能源汽车有限公司 IT 用户服务部 ***it.uhd@audi-faw-nev.com.cn*** 执行。

Any suspected loss of confidential or secret information must be reported to the responsible unit Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn***. immediately.

任何疑似丢失机密或秘密信息的情况必须立即报告给责任单位奥迪一汽新能源汽车有限公司 IT 用户服务部 ***it.uhd@audi-faw-nev.com.cn***。

1.3 COMPLIANCE

1.3 合规

Compliance Management observing legal and organizational requirements (including resource management, internal control system, IT continuity management and protection of information) must be implemented by the supplier covering all information, hard- and software of the ordering party.

供应商必须实施遵守法律和组织要求的合规管理（包括资源管理、内部控制系统、IT 连续性管理和信息保护），涵盖订购方的所有信息、硬件和软件。

The compliance management must include the following aspects.

合规管理必须包括以下几个方面。

1.3.1 Early detection of risks

1.3.1 及早发现风险

A process for early detection of risks and potential threats to IT systems and data must be in place.

必须建立早期检测 IT 系统和数据风险和潜在威胁的流程。

Preventive action and measures must be taken to mitigate detected risks.

必须采取预防行动和措施来缓解检测到的风险。

1.3.2 Intellectual property rights / License Management

1.3.2 知识产权／许可证管理

Intellectual property rights (e.g., copyrights for software, documents, and other image material, rights to drafts, trademarks, patents, and source code licenses) must be observed.

必须遵守知识产权（例如，软件、文件和其他图片资料的版权，草稿、商标、专利和源代码许可的权利）法规。

Usage of unlicensed software (pirate copies) is not permitted.

不允许使用未经许可的软件（盗版）。

License software is subject to legal provisions for copyright protection (e.g., the reproduction of software, except for backup and archiving purposes, represents an infringement of copyright). Infringements of these provisions may lead to penal measures as well as injunctive relief and damage claims.

正版软件受版权保护法规的保护（例如，除了备份和存档外，复制软件均侵犯版权）。 违反这些规定可能导致刑事诉讼以及禁令救济和损害索赔。

Company specific regulations must be observed, Copyright of the of the People's Republic of China (only binding on companies in China):

必须遵守公司的具体规定和中华人民共和国有关版权的法律法规（仅对中国公司具有约束力）：

Who violates the copyright or another after this law protected law illegally, can be taken up by the violated on removal of the impairment, with repetition danger on omission and if to the violator´s intention or negligence is a burden also on damages. At place of the damages the violated can require the delivery of the profit which the violator has achieved by the violation of the law and bill lapping about this profit.

任何人侵犯版权或受本法保护的任何其他权利时，受侵害人可以诉请消除侵权行

为，或者，如果存在再次侵权的风险，受侵害人可以诉请下达停止并终止的禁令；如果侵权系由于故意或过失，则还可以诉请获得损害赔偿。 作为损害赔偿，受侵害人可以诉请侵权人提供从侵权行为中获得的利润以及反映此类利润的详细账目。

Who reproduces a work or a treatment or transformation of a work in others than the legally admitted cases without consent of the legitimate, spreads or returns publicly, it is punished with term imprisonment up to three years or with fine. The attempt is liable to penalty.

在非法律批准的情况下，未经他人授权而复制、传播或在公开场所展示作品或修改后的作品的，将面临三年以下有期徒刑的惩罚，或是处以罚金。 此类犯罪企图均应予以惩罚。

License software must only be used for the agreed purpose and exclusively in compliance with existing provisions and the license agreements entered into with the manufacturer.

正版软件只能用于约定的目的，并且完全符合现有条款和与制造商签订的许可证协议。

1.3.3 Data protection

1.3.3 数据保护

The respective national laws and regulations for data protection must be complied with.

必须遵守相应国家的数据保护法律法规。

Contractors must be obligated by the management of the supplier company to comply with the legal requirements concerning data protection.

供应商公司的管理层必须要求承包商遵守有关数据保护的法律要求。

1.3.4 Contractual compliance

1.3.4 遵守合同

The Supplier‘s IT organization must be in compliance to the contractual requirements of the ordering party. Measures must be implemented to ensure that the suppliers own organizational regulations are reviewed and updated according to the current contractual requirements.

供应商的 IT 组织必须遵守订购方的合同要求。 必须采取措施，确保根据目前的合同要求审查和更新供应商自己的组织条例。

1.3.5 Policies and Regulations

1.3.5 政策和法规

The supplier must provide policies and regulations to its employees to ensure compliance with the requirements and adequate handling of information, hard- and software of the ordering party.

供应商必须向其员工宣讲政策和法规，以确保符合要求并妥善处理订购方的信息、硬件和软件。

1.4 VIOLATIONS AND ENFORCEMENT

1.4 违规和执法

Violations of the information security guidelines must be followed up individually as per applicable operational, contractual and legal regulations or agreements and sanctioned appropriately.

违反信息安全准则的行为必须根据适用的经营、合同和法律规定或协议单独跟进，并受到适当的制裁。

2

ADDITIONAL REQUIREMENTS FOR SUPPLIERS WITH ACCESS TO THE INTERNAL GROUP NETWORK

对有权访问集团内部网络的供应商的附加要求

2.1 DEFINITION

2.1 定义

The following requirements must be observed by all suppliers belonging to one of the following categories:

属于下列类别之一的所有供应商必须遵守下列要求：

- Are provided with clients owned by a VW Group Company
- 向其提供大众汽车集团公司拥有的客户端
- Are connected via Remote Access (e.g. TravelX, Safe, Secure i.Do-Client) or other VPN-Solutions with access to the NEV Network or any Volkswagen Group Company Network
- 通过远程访问（如 TravelX、Safe、Secure i.Do-Client）或其他 VPN 解决方案连接到奥迪一汽新能源汽车有限公司网络或任何大众汽车集团公司网络
- Are connected directly to the NEV Network or any Volkswagen Group Company Network
- 直接连接到奥迪一汽新能源汽车有限公司网络或任何大众汽车集团公司网络
- Are connected to the NEV Network or any Volkswagen Group Company via PartnerFirmenNetwork/PFN (CSN)
- 通过 PartnerFirmenNetwork/PFN (CSN)连接到奥迪一汽新能源汽车有限公司网络或任何大众汽车集团公司网络

These suppliers may be located on the premises of the Group Company or on their own companies' premises.

这些供应商可能位于集团公司的场所，也可能位于其自己公司的场所。

2.2 REQUIREMENTS

2.2 要求

2.2.1 Internal organization

2.2.1 内部组织

Suppliers must only request or initiate procurement and installation of hardware and software via the organizational unit (business department of the ordering party) that is responsible for them.

供应商只能通过对接他们的组织单位（订购方的业务部门）请求或启动硬件和软

件的采购和安装。

The use of the provided hardware and software is subject to the regulations of the respective group company. Every contractor is responsible that information, programs and communication devices are only used in a correct manner and in accordance to assigned tasks and in the company's interests. The use of private software and data on company provided communication devices is not permitted.

所提供的硬件和软件的使用受相应集团公司的规定约束。 每个承包商都有责任确保信息、程序和通信设备仅以正确的方式在分配的任务范围内使用，并符合公司的利益。 不允许在公司提供的通信设备上使用私人软件和数据。

Only the responsible units are permitted to open the IT device, make changes to the hardware (e.g., installation/removal of hard drives and memory modules), and make manual changes to security settings (e.g., browser settings).

只允许责任单位打开 IT 设备，更改硬件（例如，安装/拆卸硬盘驱动器和内存模块），以及手动更改安全设置（例如，浏览器设置）。

The use or subsequent modification of programs is only permissible with the authorization of the responsible units.

只有在责任单位授权的情况下，才允许使用或随后修改程序。

Data of any other customer that does not belong to the Volkswagen Group must not be processed on the provided IT devices.

不得在提供的 IT 设备上处理不属于大众汽车集团的任何其他客户的数据。

The use of IT devices and data of the ordering party by employees of the supplier requires the express consent of the ordering party. The ordering party is entitled to prohibit access/use at any time (e.g., in cases of misuse).

供应商员工使用订购方的 IT 设备和数据需要订购方的明确同意。 订购方有权随时禁止访问/使用（例如，在滥用的情况下）。

2.2.2 Physical and environmental security

2.2.2 物理和环境安全

The provided devices must be handled correctly and protected from loss or unauthorized modification.

必须正确处理所提供的设备，防止丢失或未经授权的修改。

The manufacturer's regulations on the protection of devices must be complied with.

必须遵守制造商关于设备保护的规定。

Devices provided by the ordering party (e.g., laptops, cellular phones) may only be taken outside of the plant of the ordering party after approval.

订购方提供的设备（如笔记本电脑、手机）只有在获得批准后才能带出订购方的工厂。

2.2.3 Protection against malicious and mobile code

2.2.3 恶意和移动代码防护

IT devices and data storage devices that are suspected of being infected with

malware must not be used any further. Audi FAW NEV, IT User Helpdesk, ***it.uhd@audi-faw-nev.com.cn*** must be informed immediately.

怀疑感染了恶意软件的 IT 设备和数据存储设备不得再使用。 必须立即通知奥迪一汽新能源汽车有限公司 IT 服务部 ***it.uhd@audi-faw-nev.com.cn***。

2.2.4 Backup

2.2.4 备份

Data should be stored on the assigned storage systems and not on the local hard drive, since a central and automatic data backup is only ensured this way.

数据应存储在指定的存储系统上，而不是本地硬盘上，因为只有这样才能确保中央自动数据备份。

The user himself/herself is responsible for backing up data that is not stored on a central network storage (e.g. local hard disks, mobile data storage devices) or systems with similar functions (e.g. eroom, sharepoint, …).

由用户负责备份未存储在中央网络存储设备（例如本地硬盘、移动数据存储设备）或具有类似功能的系统（如 eroom、sharepoint 等）上的数据。

Backup media and data must be handled the same way as the original data.

备份媒体和数据的处理方式必须与原始数据相同。

2.2.5 Access control

2.2.5 门禁

2.2.5.1 User responsibilities

2.2.5.1 用户责任

The following requirements must be observed by all users:

所有用户必须遵守以下要求：

General Requirements

一般要求

- Usage of another person's user ID or account is not permitted.
- 不允许使用他人的用户 ID 或帐户。
- Passing identification media (e.g., Smartcards, SecurID cards) to somebody else is not permissible.
- 不允许将身份验证媒体（如智能卡、SecurID 卡）传递给他人。
- Passwords or PINs of a user ID assigned for personal use (defined as "person-related user ID") must not be shared or disclosed.
- 不得共享或披露分配给个人使用的用户 ID（定义为“与个人相关的用户 ID”）的密码或 PIN 码。
- Keeping a record (e.g. on paper, in mobile devices or in files) must be avoided unless these are considered as a secure method. Recommended is the usage of password vaults like KeePass.

- 必须避免保存记录（如在纸上、移动设备中或文件中），除非这些被认为是安全的方法。 推荐使用像 KeePass 这样的密码库。
- Passwords or PINs must be changed immediately whenever there is any indication that those are compromised or became known.
- 只要有任何迹象表明密码或 PIN 码被泄露或为人所知，就必须立即更改。
- Temporary passwords (e.g. for new accounts) must be changed at the first log-on
- 临时密码（如新帐户）必须在首次登录时更改
- Password or PINs must be changed at first use and then at least every year. The change interval does not apply to PINs.
- 密码或 PIN 码必须在首次使用时更改，然后至少每年更改一次。 不应按照定期间隔时间更改 PIN 码。
- Spying out passwords is not permissible.
- 不允许窥探密码。
- Passwords must at least be classified as confidential.
- 密码必须至少归类为机密。
- If passwords have to be stored in written form, they must be stored by the employee in a sealed envelope at a suitable location that is protected against unauthorized access (e.g., safe) and be updated each time the password is changed. The sealed envelope must be signed by the respective employee. The persons authorized to open the envelope must be listed on it by name. In exceptional cases (e.g., in case of illness) it may be necessary to use the stored password. This must be done according to the "two-man rule". Each opening must be documented and reported to the employee. After each opening, the employee must change the password promptly and deposit it again. IT systems offering a functionality that matches these requirements are also permissible (e.g., electronic password safe).
- 如果密码必须以书面形式存储，则必须由员工将其存储在密封的信封中并放在适当的位置（例如保险箱），以防止未经授权的访问，并在每次更改密码时进行更新。 密封的信封必须由相应的员工签名。 信封上必须列有被授权打开信封的人的名字。 在特殊情况下（例如生病时）可能需要使用这种存储的密码。 这种情况必须按照“两人规则”。 每次打开都必须记录在案并报告给相应的员工。 每次打开后，员工必须及时修改密码并重新存入。 允许使用具有这些要求功能的 IT 系统（例如电子密码保险箱）。
- When leaving the system during ongoing operation (e.g., break, meeting), the user must activate a system lock (e.g., password-protected screen saver).
- 当有正在进行的操作（例如，休息、会议）时，如离开系统，用户必须激活系统锁（例如，有密码保护的屏幕保护程序）。
- Employees who use their multifunction badge to log on to IT systems must remove the badge from the reader when leaving the system.
- 使用多功能胸卡登录 IT 系统的员工在离开系统时必须从阅读器上取下胸卡。

2.2.5.2 Password Generation

2.2.5.2 生成密码

During password generation, the following minimum requirements must be observed:

生成密码时必须遵守以下最低要求：

- Employees must not generate identical passwords for business and non-business purposes
- 员工不得为商业目的和非商业目的生成相同的密码
- Employees must not generate identical passwords for VW group provided systems and systems, provided by 3rd parties, e. g in the Internet (applications, registration services, …)
- 员工不得在互联网上（应用程序、注册服务等）为大众汽车集团提供的系统和第三方提供的系统生成相同的密码。
- Users must observe the minimum password length enforced by the system. These are defined in the password policy4.
- 用户必须遵守系统强制执行的最小密码长度。 这些在密码策略 4 中定义。
- Simple passwords (e.g. “Test123456”, “123456abcde”) or context-specific words (e.g. personal related topics like name, date of birth) must not be used.
- 不得使用简单的密码（如“Test123456”、“123456abcde”）或特定于上下文的词语（如姓名、出生日期等个人相关主题）。
- If higher password complexity is demanded by specific systems or applications (as defined in the password policy4) the enforced complexity must be used.
- 如果特定系统或应用程序（如密码策略 4 中所定义）要求更高的密码复杂度，则必须采用强制要求的复杂度。

Hint: Use mnemonic verses or abbreviations and falsifications of mnemonic verses (e.g. mnemonic verse: “In the morning I get up early and brush my teeth” results in a password of: “Itm1guE&bmT”). The examples listed here must not be used as passwords.

提示： 使用助记词或助记词的缩写和变型（例如助记词 “早上我早起刷牙”生成密码为： “Itm1guE&bmT”）。 此处示例不得用作密码。

Alternatively, a combination of four randomly selected words (e.g. “Sun2Wood!Tea4Time”) results in a very strong password and is easy to remember. The examples provided here must not be used as passwords.

或者，使用四个随机选择的单词（例如“Sun2Wood!Tea4Time”）组合生成一个容易记住的强密码。 此处示例不得用作密码。

2.2.5.3 PINs for unlocking Smartphones and Tablets

2.2.5.3 用于解锁智能手机和平板电脑的 PIN 码

The same requirements as defined in chapter 2.2.5.2 must be observed.

必须遵守第 2.2.5.2 节中定义的要求。

2.2.5.4 PINs for Smartcards for Authentication

2.2.5.4 用于身份验证的智能卡的 PIN 码

The same requirements as defined in chapter 2.2.5.2 must be observed.

必须遵守第 2.2.5.2 节中定义的要求。

2.2.5.5 Collective User IDs

2.2.5.5 集体用户 ID

Reuse of specific collective user IDs by various persons (e.g., training participants, interns, graduating students) is permissible if the following requirements are observed.

如果遵守以下要求，则允许不同人员（例如，培训参与者、实习生、应届毕业生）重复使用特定的集体用户 ID。

» The assignment of the user IDs must be managed by a responsible person. This person must provide written verification of who used which user ID, and when. This person must archive this verification.

» 必须由负责人管理用户 ID 的分配。 此人必须提供谁在何时使用了哪个用户 ID 的书面验证。 此人必须将此验证存档。

» Receipt of the user ID must be confirmed in writing by the respective user. The confirmation is retained by the person responsible for the user ID.

» 收到用户 ID 的相应用户必须进行书面确认。 由用户 ID 的负责人保留此确认。

» During receipt of the user ID the password must be changed by the respective user into a password only known to him/her.

» 在接收用户 ID 期间，相应用户必须将密码更改为只有他/她知道的密码。

» During return of the respective user ID, the password must be changed by the responsible person to a password only known to him/her.

» 在归还相应用户 ID 期间，负责人必须将密码更改为只有他/她知道的密码。

» The company specific archiving periods must be complied with for archiving the verifications.

» 必须遵守公司特定的存档期限来将验证存档。

User IDs that can be used simultaneously by several persons (so-called "group IDs") are not permissible unless exclusively applications can be started up with this user ID that have a separate user management including a personal authentication or only allow read access.

可由多人同时使用的用户 ID（所谓的“组 ID”）是不被允许的，除非可以用该用户 ID 专门启动具有单独用户管理（包括个人身份验证）或仅允许读取访问的应用程序。

2.2.6 Network and access control

2.2.6 网络和访问控制

2.2.6.1 Policy on use of network services

2.2.6.1 网络服务使用政策

An IT device provided by the ordering party must only be connected to networks (exempt mobile communications network) outside the company (e.g., hot spot, private WLAN) in order to set up a connection with the Group network. Direct surfing etc. is not permitted (exempt with mobile communications networks connected smartphones and tablets).

订购方提供的 IT 设备只能连接到公司外部的网络（移动通信网络除外）（例如热点、专用 WLAN），以便与集团网络建立连接。 不允许直接上网等（连接移动通信网络的智能手机和平板电脑除外）。

If no longer required, the connection must be disconnected.

如果不再需要，必须断开连接。

2.2.6.2 Equipment identification in networks

2.2.6.2 网络中的设备识别

The unrestricted connection of communication devices (e.g. without firewalls) to the internal network (Intranet) is only permitted if these are made available by the Group or by companies in which the Group or one of its companies is a majority shareholder.

只有当通信设备由集团或集团或其子公司之一是大股东的公司提供时，才允许不受限制地将通信设备（如无防火墙）连接到内部网络（内联网）。

3

ADDITIONAL REQUIREMENTS FOR SUPPLIERS WITHOUT DIRECT ACCESS TO THE INTERNAL GROUP NETWORK

对无法直接访问集团内部网络的供应商的附加要求

3.1 DEFINITION

3.1 定义

The requirements contained in chapter 3 must be observed by all suppliers that fall in one of the following categories:

属于下列类别之一的所有供应商必须遵守第 3 章中的要求：

- The supplier does not have direct access to the network of a Group Company
- 供应商不能直接访问集团公司的网络
- The supplier is not provided with clients owned by a VW Group Company and only uses clients owned by its own company.
- 不向供应商提供大众汽车集团公司拥有的客户端，供应商只使用自己公司拥有的客户端。
- Is not connected via Secure Partner, remote access or any VPN solution. Virtual Desktop solutions only permitting transfer of display and control data are excluded from this definition and may be used. For those the

requirements defined in this chapter apply.

» 未通过安全合作伙伴、远程访问或任何 VPN 解决方案连接。 仅允许传输显示和控制数据的虚拟桌面解决方案不在此定义范围内，可以使用。 对于这些，本章定义的要求适用。

» The supplier is interchanging data with Audi or Audi FAW NEV.

» 供应商正在与奥迪或奥迪一汽新能源汽车有限公司交换数据。

These suppliers are located on the premises of their own companies and obliged to follow the regulations of their own company.

这些供应商位于自己公司的场所，必须遵守自己公司的规定。

3.2 REQUIREMENTS

3.2 要求

3.2.1 Internal organization

3.2.1 内部组织

Group company data must be separated from the data of third parties (e.g via rights management) and especially from data of other customers of the supplier. It must not be accessible (e.g. implementable via encryption) by other 3rd parties.

集团公司的数据必须与第三方的数据（例如通过权限管理）分开，尤其是要与供应商的其他客户的数据分开。 这些不得被其他第三方访问（例如，可通过加密实现）。

The NEV classification must be mapped to classification schemes of the supplier to ensure that all required security measures are fulfilled.

新能源汽车分类必须反映到供应商的分类方案中，以确保满足所有必需的安全措施。

The supplier must map the information security requirements of the regulations received within the scope of his tasks to appropriate security measures in the suppliers own company.

供应商必须将其任务范围内收到的法规的信息安全要求反映到供应商自己公司的适当安全措施中。

Only employees with a need to know must be able to access data belonging to the ordering party.

只有需要知道的员工才能访问属于订购方的数据。

II. RESPONSIBILITIES

II. 责任

This regulation must be observed by all suppliers as defined in the scope of this document.

本文件范围内定义的所有供应商都必须遵守本规定。

Deviations from this guideline, that reduce the security level, are only allowed temporarily and after consultation with the CISO from Audi FAW NEV (P/BT-Z) and must be informed immediately at the ordering party.

偏离该准则会降低安全级别，仅在与奥迪一汽新能源汽车有限公司的 CISO（P/BT-Z）协商后暂时允许，并且必须立即通知订购方。