ICS 35.020
CCS L80

团　　体　　标　　准

T/CHI XXX—202X

智能网联汽车数据安全要求

Requirements of data security for intelligent and connected vehicles

（征求意见稿）

提交反馈意见时，请将您知道的专利连同支持性文件一并附上。

202X-X-X 发布　　202X-X-X 实施

中国高技术产业发展促进会　发　布

目　　次

前　言

本文件按照 GB/T1.1—2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由重庆钮维思网络科技有限公司提出。

本文件由中国高技术产业发展促进会归口。

本文件主要起草单位：重庆钮维思网络科技有限公司、青岛理工大学、内蒙古工业大学、武汉船舶职业技术学院、南京理工大学、湖北文理学院。

本文件主要起草人：刘媛妮、潘福全、李雷孝、杨宜平、卢建云、陈运星、张丽霞。

本文件为首次发布。

引　言

随着智能网联汽车技术的迅速发展，汽车数据的安全性和隐私保护问题愈发突出。各级政府纷纷呼吁加强对车辆数据的监管与管理，以应对潜在的安全隐患。为了提升数据的安全性与完整性，增强数据的可追溯性，促进高效数据流通，建立信任机制，并确保遵循相关政策法规的要求，我们提出制定智能网联汽车数据安全要求标准。该标准的实施将有助于汽车行业更好地遵守政策法规，降低法律风险，提高行业信誉，为智能交通的可持续发展提供坚实的保障。

本文件主要针对智能网联汽车数据的安全管理和使用进行规范与指导，旨在提升数据管理的规范性，提高汽车数据的使用效率，确保数据安全性。遵循本标准将对保障汽车系统的安全稳定运行、提升交通决策的科学性和准确性、促进汽车数据资源的共享与利用、加强智能网联汽车行业的监管与管理，以及提高公众对智能交通系统的信任度等方面具有重要意义。

智能网联汽车数据安全要求

1 范围

本文件规定了智能网联汽车数据安全的基本原则、数据分类分级方法、全生命周期（采集、传输、存储、使用、加工、提供、公开、删除）安全要求、安全保障措施及数据安全监测与应急处置要求。

本文件适用于智能网联汽车相关企业（包括汽车制造商、零部件供应商、软件提供商、服务提供商等）开展数据安全保护工作，也可为第三方测评机构开展相关测评提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T41871—2022 信息安全技术 汽车数据处理安全要求

GB/T40429—2021 汽车驾驶自动化分级

3 术语和定义

下列术语和定义适用本文件。

3.1

智能网联汽车 intelligent and connected vehicle

搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与X（车、路、人、云等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现安全、高效、舒适、节能行驶，并最终可实现替代人来操作的新一代汽车。

[来源：GB/T40429—2021，3.1，有修改]

3.2

汽车数据 automotive data

通过智能网联汽车采集、生成、记录、传输的数据，包括车辆运行数据、位置数据、操作数据、环境数据、音视频数据以及基于上述数据加工处理形成的衍生数据。

注：不包括企业内部生产管理、客户关系管理等与车辆使用和用户无关的数据。

3.3

汽车数据处理者 automotive data processor

开展汽车数据处理活动的组织或个人，包括：

a) 汽车制造商、零部件和软件供应商；

b) 经销商、维修机构以及出行服务企业；
c) 智能网联汽车平台、内容或服务提供商等。

3.4

个人信息 personal information

以电子或者其他方式记录的与以识别或者可识别的自然人有关的各种信息。
[来源：GB/T 35273—2020，3.1，有修改]

3.5

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息。
[来源：汽车数据安全管理若干规定（试行），第三条]

3.6

重要数据 important data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、经济运行、社会稳定、公共健康和安全的数据。
注：智能网联汽车重要数据的具体范围依据国家有关法规和标准确定。
[来源：GB/T41871—2022，3.5，有修改]

3.7

车外数据 external vehicle data

通过车辆传感器等设备采集的车辆外部环境信息，如周围地形、地貌、交通状况、车辆、行人、地理位置信息等。

3.8

车身数据 vehicle body data

反映车辆本身状态、运行和操控的数据，如车辆识别代号（VIN）、车速、加速度、制动状态、轮胎压力、电机转速、能耗、故障代码等。

3.9

座舱数据 cabin data

通过车内传感器等设备采集的驾乘人员及舱内环境信息，如音视频录音录像、生物特征识别信息、面部表情、驾驶行为习惯、座椅位置、温度设置等。

3.10

运行数据 operational data

反映车辆自身行驶、操控、部件工作状态及车辆控制指令的数据。

注：运行数据是车辆控制和功能实现的核心，通常包括但不限于：车辆速度、加速度、转向角、档位、电池电量、电机转速、制动状态、加速踏板开度、自动驾驶系统发出的控制指令（如转向、加速、制动指令）以及车辆关键系统（如动力系统、制动系统）的故障代码等。

3.11

数据生命周期 data lifecycle

数据从产生、采集、传输、存储、使用、加工、提供、公开到销毁/删除的全过程。

3.12

数据控制器 data controller

能够决定数据处理目的、方式等的组织或个人。

注：在智能网联汽车领域，通常指汽车制造商或其指定的服务提供商。

3.13

数据处理 data processing

受数据控制器委托，代表数据控制器实施数据处理活动的组织或个人。

3.14

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.15

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

注：匿名化处理后的信息不属于个人信息。

[来源：中华人民共和国个人信息保护法，第七十三条]

3.16

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化处理后的信息仍属于个人信息。

3.17

用户主体 user entity

对自身相关汽车数据行使管理权利的个人，通常为车主、主要驾驶人或乘车人。

3.18

默认不收集 collection by default off

除非用户主动选择开启，否则智能网联汽车的各项数据采集功能应处于关闭状态。

注：涉及车辆安全驾驶的必需功能除外。

4 数据安全基本原则

4.1 合法合规原则

数据处理活动应当严格遵守国家关于网络安全、数据安全、个人信息保护、道路交通安全以及智能网联汽车管理的法律法规、部门规章和政策要求。数据处理者应建立合规管理体系，确保数据处理的目的、方式、范围等均具有合法的依据，并及时关注和适应法律法规的动态变化。

4.2 目的明确原则

任何数据处理活动都应具有明确、具体、合理的特定目的。数据处理者应在数据收集前向个人告知数据处理的目的，并在产品设计、服务协议和隐私政策中予以清晰说明。后续的数据使用、加工、共享等行为不应超出与初始目的直接相关的合理范围。如需变更目的，应重新取得个人同意或符合法律规定的其他情形。

4.3 最小必要原则

数据处理者应秉持数据最小化理念，仅处理与实现处理目的直接相关的最少类型和数量的数据。数据处理活动应以满足目的为限，数据收集范围、存储期限、访问权限等均应控制在实现处理目的所必需的最小范围内。在智能网联汽车场景下，尤其应对车内摄像头、麦克风等敏感设备的数据采集进行严格限制，实现“默认不收集”或“用时采集、过后即删”。

4.4 安全防护原则

数据处理者应根据本标准第5章确定的数据安全级别，采取与之相适应的、严格的技术措施和管理措施，确保数据在全生命周期内的安全性。

保密性：防止数据被未经授权的访问、泄露。

完整性：防止数据被未经授权的篡改、破坏。

可用性：确保授权用户或系统在需要时能够可靠地访问和使用数据。

防护措施应能有效抵御可预见的安全威胁，并将安全风险降低到可接受的水平。

4.5 权责一致原则

应明确智能网联汽车产业链中各相关方（如汽车制造商、零部件供应商、软件提供商、服务提供商、经销商等）在数据安全保护方面的责任和义务。数据控制器应对数据处理活动负总责，确保与数据处理者之间的责任边界清晰。应建立完善的数据安全责任制度和问责机制，确保责任落实到岗、到人。

4.6 生命周期管理原则

数据安全保护应覆盖数据从产生、采集、传输、存储、使用、加工、提供、公开到最终销毁或删除的全过程。数据处理者应针对生命周期的不同阶段，制定并实施相应的安全策略和控制措施，形成闭环管理。特别是在数据销毁阶段，应采用不可恢复的技术手段，确保数据被彻底删除。

4.7 主体责任原则

智能网联汽车的整车制造商作为产品的责任主体和用户关系的主要承担者，应承担起数据安全的主要责任。汽车制造商应负责建立覆盖其产品和服务的数据安全管理体系，并对供应链中的零部件供应商、服务提供商等的数据处理活动进行有效管理和约束，确保整个产品生态的数据安全。

5 智能网联汽车数据分类与分级

5.1 数据分类

5.1.1 按数据来源分类

车外环境数据：通过车载传感器（如摄像头、雷达、激光雷达）及车外通信接口（如V2X）获取的车辆外部环境信息。例如：道路基础设施信息、周边车辆/行人信息、交通标志信息、环境影像等。

车身数据：通过车辆内部网络（如CAN、LIN、以太网）及控制器（ECU）产生的反映车辆自身状态的信息。例如：车辆速度、加速度、转向角、胎压、电池状态、发动机转速、制动状态等。

座舱数据：通过驾驶舱或乘客舱内的设备采集的，反映驾乘人员状态及交互行为的信息。例如：驾驶员面部特征、疲劳状态、语音指令、车内影像、座椅位置设定等。

远程服务与管理数据：通过远程通信终端（T-Box/联网模块）与云端服务平台交互产生的数据。例如：车辆状态上报数据、远程控制指令、OTA升级包、导航路径信息、娱乐服务内容等。

5.1.2 按数据内容/属性分类

车辆控制数据：直接或间接用于控制车辆行驶行为的关键数据。例如：自动驾驶系统的决策规划指令（转向、加速、制动）、线控执行器的控制信号等。

地理位置数据：能够反映车辆或个人精确或模糊位置的信息。例如：GPS/北斗坐标、行驶轨迹、常去地点、导航数据等。

生物特征数据：基于个人生理或行为特征生成的，用于身份识别或状态判断的数据。例如：人脸图像、指纹、声纹、心率、眼动轨迹等。

操作历史数据：记录用户或系统对车辆进行操作的历史信息。例如：驾驶里程、充电记录、设置偏好、故障码历史、系统交互日志等。

应用日志数据：车辆系统及应用软件运行过程中产生的用于记录运行状态、调试和审计的数据。例如：系统事件日志、应用崩溃报告、网络访问日志等。

5.1.3 按数据关联主体分类

个人信息：能够单独或者与其他信息结合识别特定自然人的各种信息。例如：车主身份信息、行程轨迹、驾驶习惯、生物特征信息等。

重要数据：依据国家网信部门及相关主管部门的规定，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

非个人信息/一般数据：除个人信息和重要数据之外的其他车辆数据，通常为经过有效匿名化处理或本身不涉及个人和公共利益的数据。

5.2 数据分级方法

5.2.1 分级要素与影响程度定义

表1 数据安全分级要素与影响程度定义

影响对象	极高影响	高影响	中等影响	低影响
国家安全	对国家安全造成严重损害	对国家安全造成显著损害	对国家安全造成一般损害	对国家安全无损害或影响极小
公共利益	对社会公共秩序、公共健康安全造成特别严重危害	对社会公共秩序、公共健康安全造成严重危害	对社会公共秩序、公共健康安全造成一定危害	对社会公共秩序、公共健康安全影响极小
个人权益	导致个人生命健康受到严重危害，或造成特别巨大财产损失（≥人民币50万元）	导致个人隐私严重泄露，或造成重大财产损失（人民币10万至50万元）	导致个人隐私泄露，或造成较大财产损失（人民币1万至10万元）	对个人权益影响极小或可忽略
车辆行驶安全	直接导致车辆发生致命性事故，造成人员死亡或群伤	直接导致车辆发生严重事故，造成人员重伤或车辆严重损坏	影响车辆正常行驶功能，可能增加事故风险	对车辆行驶安全无影响

5.2.2 数据级别划分

根据数据安全分级要求与影响程度定义，将智能网联汽车数据划分为以下四个级别：

a） 第四级数据（Level 4，极高影响级）。

1）通常为核心数据。一旦发生安全事件，会对国家安全、公共利益、个人权益或车辆行驶安全造成极高影响（见表1“极高影响”列）。

2）涉及国家秘密的核心数据：依法确定为国家秘密的数据。

3）关键实时控制指令：自动驾驶系统在特定场景下（如高速、拥堵路段）发出的，其实时篡改（延迟/注入攻击成功）可直接导致车辆碰撞、人员死亡的指令（如紧急制动指令、紧急转向避让指令）。

4）未脱敏的、大规模（如超过10万人）高精度敏感区域地理信息：如军事基地、核设施的厘米级三维地理模型。

b） 第三级数据（Level 3，高影响级）。

1）通常为重要数据和部分高度敏感的个人信息。一旦发生安全事件，会对国家安全、公共利益、个人权益或车辆行驶安全造成高影响（见表1“高影响”列）。

2）重要数据：依据国家规定划定的智能网联汽车重要数据。

3）高精度敏感区域地理信息：未脱敏的国防科工单位、关键基础设施周边米级精度的地理坐标数据。

4）未脱敏的生物特征数据：可用于身份鉴别的驾驶人面部原始图像、声纹模板等。存储时必须采用强加密（如国密SM4/AES-256），传输通道必须为安全加密通道（TLS 1.2以上）。

5）车辆动态控制数据：实时油门、刹车、转向控制信号，其篡改可能引发严重事故。

c） 第二级数据（Level 2，中等影响级）。

1）通常为敏感个人信息和重要的车辆运行数据。一旦发生安全事件，会对个人权益或车辆行驶安全造成中等影响（见表1“中等影响”列）。

2）行程轨迹与习惯偏好：能够推断个人身份、行为模式的连续地理位置信息、驾驶行为数据（如急加速/急刹车频率）。

3）车辆运行状态数据：车速、电机转速、剩余电量、里程等。

d） 第一级数据（Level 1，低影响级）。

1）通常为非个人信息、匿名化数据或公开数据。一旦发生安全事件，造成的影响程度为低（见表1“低影响”列）。

2）经过有效匿名化处理的数据：满足k-匿名（k≥50）、差分隐私（ε≥1）等标准，无法重新识别到特定个人或车辆的数据。

3）公开地图信息：从公开渠道获取的导航电子地图数据。
车辆基本型号信息：不关联具体车辆VIN码的车型配置信息。

4）分级流程与动态调整

数据处理者应建立数据分级目录，并定期（如每年）或在数据内容、处理目的、应用场景发生重大变化时，重新进行数据分级评估和调整。分级流程应包括数据资产梳理、影响分析、级别判定、审核确认等步骤。

6 数据全生命周期安全要求

6.1 数据采集

6.1.1 告知-同意机制

在首次使用产品或服务、首次收集新增数据类型时，应通过车载交互界面（HMI）或与之绑定的移动应用，以清晰易懂的语言和形式，向用户逐项说明数据收集的目的、类型、范围、使用方式、存储期限、是否向第三方共享等信息，并取得用户自主作出的授权同意。对于敏感个人信息（如生物特征、行踪轨迹）及座舱内摄像头、麦克风的启用，应取得用户的单独同意。

告知可读性：车载HMI的告知文本字体大小、对比度应符合车载环境下的可读性要求，避免在驾驶过程中进行复杂交互。主要告知文本字符高度不低于4mm，或在典型观看距离下达到视觉角度20分以上。

同意记录可审计性：用户的同意、拒绝或撤销同意等操作记录应被安全、准确地记录和存储。同意记录应包含时间戳、操作内容、用户标识（如匿名化ID），并确保日志的完整性和防篡改性，留存时间自操作发生之日起不少于3年。

6.1.2 最小化采集

遵循默认不收集原则。仅在实现特定的、明确的业务功能所必需时，方可收集相应的数据。数据收集的范围和频率应限制在实现处理目的的最小范围内。

可配置开关：应为用户提供明确的数据采集控制选项，特别是针对座舱数据（如车内摄像头、麦克风）和位置数据的采集功能，应提供独立的开关。相关功能开关在硬件或系统层级实现，默认状态应为“关闭”。用户关闭后，除法律法规强制要求外，相应传感器应停止数据采集或仅在车端处理不输出。

按需采集：对于非持续运行的功能（如一次性的语音助手查询），应实现“用时采集、事后即焚”。此类数据的本地缓存时间不应超过完成该次功能处理所必需的时间，原则上不超过24小时。

6.1.3 车内处理优先

对于支持在车端完成计算和处理的数据，应优先在车内进行处理，仅将处理结果或必要的非原始数据传出车外，以减少敏感数据暴露的风险。

人脸识别认证应在车内完成特征值比对，仅将“认证成功/失败”的结果上传至云端，而非原始人脸图像。语音指令应在车内完成识别，将文本指令上传，而非原始音频数据。

涉及生物特征识别的功能，其原始生物特征信息（如人脸原图、声纹原始特征）不得传输至车外，除非法律法规另有规定或为用户主动发起的特定服务（如客服录音）。

6.2 数据传输

6.2.1 通信安全

应对智能网联汽车涉及的不同通信链路采取安全防护措施。

车云通信：远程信息处理终端（T-Box）与云端服务平台之间的通信。

V2X通信：车辆与车辆、道路基础设施、行人等之间的通信。

车内网络通信：车载总线（如CAN FD、 Automotive Ethernet）上各电子控制单元（ECU）之间的通信。

加密与认证：车云通信必须使用基于证书的双向认证和强加密协议。采用TLS 1.2及以上版本，加密套件优先使用国密算法套件或国际公认的强套件（如ECDHE-RSA-AES256-GCM-SHA384）。

V2X安全：应遵循国家V2X通信安全标准，使用公钥基础设施（PKI）对消息进行签名和验证，确保消息的真实性和完整性。

车内网络安全：对高安全级别的控制指令和状态数据（如Level 3及以上），应在数据链路层或应用层实施安全机制。使用如AUTOSAR SecOC（Secure Onboard Communication）等机制，为关键数据提供新鲜度保护和消息认证码（MAC），MAC长度不低于64位。

6.2.2 通道安全

建立端到端的安全传输通道，防止数据在传输过程中被窃听、篡改、重放或中间人攻击。

证书管理：用于车云通信的服务器证书和车辆端证书应由可信的证书颁发机构（CA）签发，并建立严格的证书生命周期管理流程。证书有效期不超过1年，并具备吊销检查机制。

6.3 数据存储

6.3.1 存储位置

在境内运营中收集和产生的重要数据和个人信息，应当在境内存储。因业务需要，确需向境外提供的，应按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

数据处理者应能通过技术手段（如系统配置、日志审计）证明其存储系统的主副本位于中国境内。

6.3.2 加密存储

存储静态数据时，应对个人信息和重要数据进行加密保护。

车端存储：存储在车载存储设备（如eMMC, SSD）中的敏感数据（如日志、缓存的身份信息）应进行加密。使用硬件安全模块或可信执行环境支持的加密引擎，采用AES-128或国密SM4及以上强度的加密算法。

云端存储：存储在云数据库或对象存储中的敏感数据必须加密。采用服务端加密（使用云服务商管理的密钥或客户自持密钥）或客户端加密，算法强度不低于AES-256。

6.3.3 访问控制

实施基于角色的访问控制，遵循最小权限原则，严格限制对数据的访问权限。

访问敏感数据的权限审批流程必须有记录。

对数据仓库、数据库的批量查询和导出操作需经过额外审批和监控。

6.3.4 存储时限

根据法律法规规定和业务处理目的，为不同类型的数据设定合理的存储期限。期限届满后，应主动删除或进行匿名化处理。

建立明确的数据留存策略文档，明确规定各类数据的存储期限。例如，车辆故障数据可能留存至车辆报废，而用户行程轨迹数据留存不超过6个月。

系统应具备自动删除过期数据的功能，并有日志记录删除操作。自动化删除任务的执行成功率应不低于99.9%。

6.4 数据使用与加工

6.4.1 访问控制与审计

对所有数据访问、查询、分析、加工操作实施严格的权限控制和日志记录，并定期进行审计。

日志留存：所有数据访问日志应被完整记录，包括访问时间、访问者身份、访问的数据范围、操作类型（读、写、删）等。安全日志的留存时间自产生之日起不少于6个月，用于审计的日志应防篡改。

定期审计：至少每半年进行一次数据访问行为的合规性审计。

6.4.2 匿名化与去标识化

将数据用于模型训练、数据分析等内部研发目的时，原则上应使用经过匿名化或去标识化处理的数据。

技术有效性：采用的匿名化技术应能有效降低重标识风险。采用k-匿名技术时，k值应不小于50；采用差分隐私技术时，隐私预算 ε 应根据场景设定，一般不大于1.0。应定期对匿名化数据集进行重标识攻击测试，确保风险可控。

6.4.3 开发测试数据管理

严禁在开发、测试、演示环境中使用真实的个人信息和重要数据。

测试数据应通过合成数据生成或脱敏技术获得。脱敏必须是不可逆的，例如，对VIN码、身份证号等标识符进行泛化或假名化处理。

建立测试数据管理流程，确保测试环境与生产环境有效隔离。

6.5 数据提供与公开

6.5.1 共享审批

向第三方提供数据前，必须进行数据安全影响评估，评估共享目的、数据范围、接收方安全保障能力等风险。共享个人信息时，应再次获得用户的明确授权。

数据共享审批记录、安全评估报告及用户授权凭证应存档备查，保存期限不少于3年。

6.5.2 安全协议

应与数据接收方签订具有法律效力的数据保护协议，明确双方的安全责任、数据处理目的、保护措施、安全事件通知和处置义务。

协议应明确要求接收方不得将数据用于约定目的之外的范围，并应具备对接收方履约情况进行审计的权利。

6.5.3 公开要求

公开数据前，必须经过严格的脱敏和保密审查，确保公开的数据不包含任何个人信息、重要数据或未公开的商业秘密。

公开数据的脱敏效果需经过独立复核，确保无法还原出原始敏感信息。

6.6 数据删除

6.6.1 响应权

应建立便捷的渠道，响应用户提出的数据删除请求（如账户注销、撤回同意）。当处理目的已实现、无法实现或者为实现处理目的不再必要时，数据处理者应主动删除数据。

在收到用户符合条件的删除请求后，应在15个自然日内完成删除操作并给予用户反馈。

6.6.2 彻底删除

数据删除应确保数据内容不可恢复，包括从所有存储位置（生产系统、备份系统、缓存等）中删除。

车端删除：对于存储在车辆本地且用户要求删除的数据，应执行安全擦除指令。对于车载固态存储，应使用物理块覆写技术进行删除。

云端删除：应建立备份数据清理流程。删除操作应有验证机制，例如，定期由内部审计或第三方进行抽样验证，确认数据已从所有相关系统中被彻底清除。验证报告应留存。

7　安全保障措施要求

7.1　组织管理要求

7.1.1　数据安全管理机构与职责

组织应建立跨部门的数据安全管理委员会或指定高级管理人员（如首席数据安全官）作为数据安全负责人，负责制定数据安全战略、审批重大数据处理活动、协调资源并监督数据安全工作的落实。智能网联汽车整车制造商应承担数据安全主体责任。

明确责任部门：应设立专门的数据安全或网络安全部门，职责清晰界定，并具备足够的独立性。应发布正式的组织架构和岗位职责说明书。

汇报机制：数据安全负责人应能直接向最高管理层（如CEO或董事会）汇报数据安全风险和状况。每季度至少汇报一次。

7.1.2　制度与流程建设

应制定覆盖数据全生命周期的管理制度和操作规程，如数据分类分级管理办法、数据安全应急预案、数据访问权限审批流程等。

形成受控的文件体系，并确保相关员工可以便捷获取和查阅。每年至少对制度进行一次评审和更新。

7.1.3　人员培训与意识教育

应定期对全体员工（特别是研发、测试、运维、数据分析等岗位）进行数据安全法律法规、标准规范、技术技能和案例的培训，提升全员数据安全意识。

岗位针对性培训：对智能网联汽车研发人员，应重点培训车内数据安全处理、隐私设计等知识。

培训效果评估：全体员工年度的数据安全培训覆盖率应达到100%，且通过率不低于90%。关键岗位人员应通过专项考核。

7.2　技术保障要求

7.2.1　车辆网络安全

车辆的网络安全管理体系应符合国际国内相关法规和标准要求（如UNECE R155 CSMS、ISO/SAE 21434），确保车辆具备持续的网络安全防护能力。

入侵检测/防御系统：车辆应具备检测潜在网络攻击（如异常CAN总线消息、恶意网络扫描）的能力。车载IDS应能对已知攻击模式的检测率不低于95%，误报率低于5%。检测到高风险事件时，应能在本地记录并具备安全上报云端的能力。

安全升级：应建立安全的空中下载技术（OTA）升级机制，确保升级包的完整性、机密性和真实性。OTA升级包必须100%经过数字签名验证，升级过程需支持断点续传和回滚机制。从云端服务器到车端升级过程的端到端加密率应为100%。

7.2.2 数据安全技术

应在IT系统、云平台和车端部署必要的数据安全技术工具。

数据加密与脱敏：敏感数据存储加密覆盖率应达到100%；测试环境使用生产数据脱敏的比例应达到100%。

访问控制与审计：对核心数据资产的访问日志记录率应达到100%。

数据泄漏防护：应在网络边界和终端部署DLP系统，监控和阻止敏感数据违规外泄。DLP策略对预设的敏感数据模型（如VIN码批量导出）的检测率应不低于90%。

7.2.3 安全监测与响应

应建立统一的安全运营中心或类似机制，对车辆、车联网平台的数据安全状态进行7x24小时监控，并建立安全事件应急响应流程。

安全监控平台发出高级别警报（如Level 3及以上数据疑似泄露）后，运营人员应在≤5分钟内确认警报。

确认发生数据安全事件后，应按照预案启动响应机制，初步遏制措施（如隔离受影响系统、暂停数据接口服务）应在≤1小时内完成。

7.3 供应链数据安全管理

7.3.1 供应商准入与合同约束

智能网联汽车制造商（作为数据控制器）必须将数据安全要求延伸至整个供应链。应在采购合同或技术协议中明确对零部件供应商、软件供应商、服务提供商等的数据安全要求。

合同条款：合同应明确供应商的数据安全责任、义务、遵守的标准（如本标准）、安全事件通知时限、审计配合义务以及违约处罚条款。

新签或续签的与数据处理相关的供应商合同，100%包含数据安全条款。

7.3.2 供应商风险评估与审计

应定期对关键供应商（如T-Box、智能座舱、自动驾驶系统供应商）的数据安全能力进行评估或审计。

评估覆盖率：对提供涉及处理Level 3及以上数据的零部件或服务的供应商，应每年进行一次数据安全风险评估。此类供应商的年度评估覆盖率应达到100%。

审计：对于评估中发现高风险或发生安全事件的供应商，应启动现场数据安全审计。

7.3.3 软件物料清单

应建立和维护软件物料清单，清晰掌握车辆中所用软件组件（特别是开源软件）及其版本信息，以便快速定位和修复漏洞。

针对新车型项目，应生成完整的SBOM，并建立流程确保在获得新的漏洞信息后，能在预设时限（如14个自然日）内完成影响性分析。

8 数据安全监测与应急处置

8.1 数据安全监测

数据处理者应建立覆盖车辆、车联网服务平台以及供应链环节的立体化数据安全监测预警机制，能够实时或准实时地监测数据处理活动的异常行为和安全状态的变化。

8.1.1 车端监测

应通过在车辆关键电子控制单元或车载网络中部署轻量级代理，监测与数据相关的异常活动。监测内容应包括但不限于：

对敏感数据（如生物特征数据、控制指令）的异常访问模式。

车内网络（如CAN总线）上出现异常的数据包（如不符合预设周期、格式或数值范围）。

未经授权的数据导出尝试（如通过OBD接口或外部设备）。

车端监测代理应能检测到已知的恶意数据访问模式，检测率不低于90%。检测到高风险事件应能在本地生成日志，并具备按策略向云端安全运营平台上报的能力。

8.1.2 平台端监测

应利用安全信息和事件管理系统，对车联网服务平台的数据访问、使用、流转行为进行集中监控和分析。监测内容应包括但不限于：

大规模、高频次的数据查询和导出操作。

非业务高峰时段的异常数据访问。

用户数据的大量跨地域访问。

平台端应对所有数据访问操作进行100%日志记录。应建立基于机器学习的用户行为分析模型，对偏离基线的异常行为生成警报，误报率应优化至可接受水平（如低于10%）。

8.1.3 预警机制

应根据数据安全级别和威胁情报，设定不同等级（如蓝、黄、橙、红）的预警阈值。一旦监测数据超过阈值，系统应自动触发预警，并通知相关责任人。

高级别（橙、红）预警信息应通过多种途径（如短信、应用内通知）确保在5分钟内送达至少两名指定安全负责人。

8.2 应急处置

数据处理者应制定针对不同场景和数据安全级别的数据安全事件应急预案，并定期演练。发生数据安全事件时，应立即启动预案，采取与事件危害程度相适应的处置措施，并按规定及时上报。

8.2.1 应急预案

预案应充分考虑智能网联汽车的特点，包含但不限于以下场景：

车辆级事件：如大规模车辆数据被远程恶意爬取、单个车辆座舱数据泄露。

平台级事件：如车联网平台遭入侵导致用户个人信息泄露、OTA升级服务器被篡改。

供应链事件：如关键供应商数据泄露波及整车企业。

预案应明确指挥架构、处置流程、沟通策略、恢复步骤和法律责任。

8.2.2 处置措施

处置应遵循“抑制-消除-恢复-总结”的流程。针对智能网联汽车的特殊性，处置措施必须优先考虑车辆行驶安全和人身安全。

抑制：立即采取措施控制事态影响范围。例如，切断恶意IP对平台的访问、通过OTA对受影响车辆下发安全策略（如暂停有风险的数据上传功能）、在确保安全的前提下对车辆进行远程隔离。

消除：根除事件原因。例如，修复系统漏洞、查杀恶意软件、吊销泄露的证书。

恢复：恢复正常的业务和数据服务。例如，验证OTA通道安全后恢复功能、从备份中恢复被篡改的数据。

从确认事件发生到完成初步抑制措施的时间（遏制时间）应不超过1小时。对于涉及车辆控制安全的事件，响应时间应在分钟级。

a） 上报与沟通

1）应严格按照国家网络安全、数据安全和个人信息保护相关法律法规的要求，向行业主管部门和监管机构报告。

2）在发现可能危害国家安全、公共利益或个人权益的重大数据安全事件后，应在72小时内完成初步情况上报。

b） 演练

1）应至少每年组织一次跨部门的综合性数据安全应急演练，演练应模拟真实事件，检验预案的有效性和人员的响应能力。

2）演练后应形成演练评估报告，对发现的问题进行整改，预案更新率应达到100%。

8.3 审计与改进

8.3.1 数据安全审计

8.3.1.1 审计应覆盖数据全生命周期各阶段的安全控制措施落实情况，并延伸至关键供应商。

8.3.1.2 审计方式应包括内部审计和第三方审计。

8.3.1.3 每年至少进行一次全面的内部数据安全审计。每两年或发生重大变更后，建议由独立第三方进行审计。

8.3.2 风险评估

8.3.2.1 应建立常态化的数据安全风险评估机制，特别是在推出新车型、新服务、新技术应用或数据处理场景发生重大变化时，必须进行风险评估。

8.3.2.2 风险评估应基于本标准的分类分级要求，识别资产、威胁、脆弱性，并评估风险等级。

8.3.2.3 全面风险评估应至少每年进行一次。专项风险评估应在相关项目启动后3个月内完成。

8.3.3 持续改进

8.3.3.1 应建立基于审计结果、风险评估结论、安全事件教训、监管要求变化和新技术发展的持续改进机制。

8.3.3.2 所有发现的问题都应纳入整改跟踪流程，直至闭环。

8.3.3.3 审计和风险评估中发现的高风险项，整改完成率应达到100%，中风险项整改完成率不低于90%。

8.4 数据风险评估

8.4.1 数据泄露风险：评估数据泄露的可能性，识别潜在的安全威胁和漏洞，制定有效的应对措施。
8.4.2 合规风险：审查数据处理流程是否符合监管要求，防止因不合规而带来的法律风险。
8.4.3 运营风险：检查数据的使用是否会对汽车运营和维护产生负面影响，确保数据不会导致车辆功能失常或其他安全问题。

8.5 数据处理与使用评估

8.5.1 数据共享与流通：审核数据共享的流程，确保数据共享时符合规定，并确保数据不会被滥用。
8.5.2 数据去标识化：对于涉及个人隐私的数据，评估去标识化措施是否有效，确保用户隐私得到保护。
8.5.3 数据处理目的：确保数据的收集和处理目的明确，并且数据处理活动始终符合最初设定的目的。

8.6 审计与报告

8.6.1 定期审计：进行定期的内部审计，评估数据管理的各项措施是否符合预定的安全、质量和合规标准。
8.6.2 审计日志：保持详尽的审计日志，记录数据访问、修改和处理的详细信息，确保能够追溯数据处理的全过程。
8.6.3 评估报告：定期发布评估报告，向管理层和监管机构汇报数据安全、质量和合规性状况。

8.7 应急响应评估

8.7.1 应急预案：评估现有的数据安全事件应急预案，确保在发生数据泄露或其他安全事件时能够迅速采取有效措施。
8.7.2 响应能力：检查数据安全事件响应能力，确保相关人员在事件发生时能够迅速定位问题并采取措施。

附录 A
（资料性附录）
智能网联汽车数据分类分级清单示例

注：本附录提供了常见数据类型的分类分级示例，旨在帮助理解和使用本标准。实际数据级别需由数据处理者根据具体业务场景和安全影响分析最终确定。

表A.1 智能网联汽车数据分类分级表

数据类别	数据示例	建议级别	分级理由说明
车辆控制数据	自动驾驶系统实时决策的控制指令（转向、制动、油门）	Level 4	直接关系到车辆行驶安全，篡改可导致致命事故。
	远程泊车指令	Level 3	在低速场景下，误操作可能导致车辆碰撞或财产损失。
地理位置数据	高精度（厘米级）军事管理区地理信息	Level 4	涉及国家安全。
	车辆实时GPS轨迹（关联VIN）	Level 3/2	如为车队数据（重要数据）则为Level 3；如为单车个人行程轨迹则为Level 2。
	匿名化处理后的区域车流量统计信息	Level 1	不关联个人和车辆，影响范围小。
生物特征数据	驾驶员状态监测（DMS）采集的原始面部图像	Level 3	高度敏感的个人信息，泄露对个人隐私造成严重侵害。
	经过车内处理仅输出“疲劳状态”标识（如：正常/疲劳）	Level 2	仍可推断个人状态，但敏感性降低。
运行数据	电池包实时电压、温度等关键安全参数	Level 3	篡改可能掩盖安全隐患，引发热失控等严重安全事故。
	车速、里程、平均电耗	Level 2	可推断驾驶习惯，属于个人敏感信息。
车外数据	V2X接收到的前方车辆紧急制动预警消息	Level 3	消息篡改或伪造可能干扰驾驶员判断，引发事故。
座舱数据	车内录音、录像	Level 3	高度敏感的隐私数据。
	语音助手交互指令（经处理，不存储原始音频）	Level 2	仍可能包含个人信息。