ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/TXXXXX—XXXX

交通运输 信息安全规范

Transportation - Information Security Specification

（征求意见稿）

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。

（本稿完成日期：2017-7-31）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中 国 国 家 标 准 化 管 理 委 员 会　发 布

目　　次

前　　言

GB/T XXXXX《交通运输 信息安全规范》作为交通运输信息安全方面的纲领性标准，为交通运输提供必要的信息安全标准化保障。

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由全国智能运输系统标准化技术委员会(SAC/TC268)提出并归口。

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。

本标准起草单位：交通运输部公路科学研究院、北京中交国通智能交通系统技术有限公司、360企业安全集团、恒安嘉新(北京)科技股份公司、国家互联网应急中心、北京信息科技大学、天津中兴智联科技有限公司、成都卫士通信息安全技术有限公司、北京江南天安科技有限公司、中兴通讯股份有限公司、北京天融信网络安全技术有限公司、电信科学技术研究院、北京启明星辰信息安全技术有限公司、亚信安全、北京云星宇科技服务有限公司、广州华工信息软件有限公司、上海蔚来汽车有限公司、青岛真情巴士集团有限公司、深圳市金溢科技股份有限公司、北京易华录信息技术股份有限公司、深圳成谷科技有限公司。

本标准主要起草人：王笑京、孟春雷、宋向辉、武俊峰、梅新明、周洲、王龑、郑新华、刘鸿伟、王永建、王立岩、赵童、孙婧、吴秋新、马涛、罗俊、赵云辉、徐晖、林兆骥、庄莉、姚健、王洪岩、张会增、罗海龙、段作义、张建文、刘景飞、王强。

交通运输 信息安全规范

1 范围

本标准规定了交通运输信息安全技术体系架构和信息安全总体技术要求，包括构成交通运输信息系统的用户终端、载运装备单元、基础设施单元、计算中心、网络和通信各基本组成部分的信息安全通用和专项技术要求。

本标准适用于指导交通运输信息系统运营者针对不同系统的特定信息安全需求提出具体的信息安全标准、规范、实施指南等，也可用于指导开展信息安全技术体系规划、设计、建设、运维等工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 20839-2007 智能运输系统 通用术语

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 20839-2007和GB/T 25069-2010中的某些术语和定义。

3.1

交通运输信息系统 transport information system

交通运输信息系统是指交通运输领域由计算机或者其他信息终端及相关设备和网络组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。通常由终端、载运装备单元、基础设施单元、计算中心、网络和通信等全部或部分组成。

3.2

信息安全 information security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[GB/T 25069-2010，定义2.1.52]

3.3

交通运输关键信息基础设施 transport critical information infrastructure

是指交通运输领域一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的信息系统（含网络）。

3.4

交通运输信息系统运营者 operators of transport information system

是指交通运输信息系统的所有者、管理者和服务提供者。

3.5

用户终端 user terminal

在交通运输业务中出行者、交通业务管理人员等使用的智能终端设备，包括交通运输通用用户终端和交通运输专用用户终端。

3.6

交通运输通用用户终端 general user terminal for transport

在交通运输业务中使用的通用桌面终端设备和移动智能终端设备，包括台式机、笔记本电脑、智能手机、平板电脑等。使用中会安装交通运输相关软件、应用。

3.7

交通运输专用用户终端 special user terminal for transport

在交通运输业务中使用专用终端设备，包括移动执法终端、联网收费终端、读写卡终端（机具）等。

3.8

载运装备单元 vehicle side unit

车辆、船舶、集装箱等交通运输装备与基础设施单元、终端或计算中心通信的装置、智能设备或通信模块等，包括PDU、T-box等。

3.9

基础设施单元 infrastructure side unit

为实现交通运输业务功能，部署在路侧、岸侧的设备或模块等，包括通信设备、智能设备、信息发布设备、状态监测设备、环境监测设备等。

3.10

网络和通信 network and communications

利用通信线路和通信设备将分布在不同地点的交通运输信息系统或信息节点等互相连接起来，按照共同的网络和通信协议，共享硬件、软件，最终实现资源共享和信息互联互通的系统。

3.11

计算中心 computing center

由实现交通运输信息系统核心计算功能的软硬件设备及其所在物理环境构成的计算和运行环境，包括机房设施、主机设备、基础软件、应用软件和数据存储等。

3.12

安全单元 security element（SE）

含有中央处理单元（CPU）的集成电路模块，负责载运工具（OBU）和基础设施（RSU）的访问许可、信息鉴别和加密保护等。

3.13

应用优先级 application priority

载运装备单元中的应用根据功能和操作需求，关联到一个应用优先级，应用优先级别可分为生命安全应用、行驶辅助应用和增值服务应用三个层次。

3.14

生命安全应用 safety related application

包括紧急碰撞与伤害减弱，潜在碰撞与伤害减弱和防止，紧急事件通知（如前车急刹）等；紧急情况通知（如事故，急救车辆，突发性环境恶化通知）等应用。

3.15

行驶辅助应用 driving aid application

包括基础设施侧单元向载运装备通知的高优先级的公共安全信息相关通知;安全相关道路状况紧急通知如红绿灯周期、急转弯等；行车辅助消息如自动驾驶、路侧周期广播、定位差分信号等。交通信息播报等应用。

3.16

增值服务应用 value-added service application

包括非优先类业务如在线支付充值、个性化导航服务、行车路线建议、电子商务等应用。

3.17

保密性 confidentiality

使数据不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069-2010，定义2.1.34]

3.18

完整性 integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

[GB/T 25069-2010，定义2.1.34]

3.19

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069-2010，定义2.1.34]

3.20

数据新鲜性 data freshness

数据新鲜性是防止已成功接受的历史数据再次被接收处理，或超出数据接收时间的数据被接收，或超出数据合法性范围的数据被接收。

3.21

合作式智能交通系统 cooperative ITS

合作式智能运输系统是由载运装备单元、基础设施单元、数据传输网络、网络管理控制平台、业务管理平台、网关设备等部分共同组成的信息管理、控制、分发的系统，可以向交通运输管理者、业务提供者和使用者提供服务和应用的综合性信息系统。

3.22

辅助驾驶 driving assistance

利用传感探测、自动控制、通信等技术，通过载运装备单元和基础设施单元的智能探测、载运装备-载运装备和载运装备-基础设施通信等方法，为驾驶员提供信息服务与支持、紧急情况下的预警和控制干预支持等功能，提高驾驶员出行安全和效率。

[GB/T 20839-2007，定义7.2]

4 交通运输信息系统安全技术体系架构

交通运输信息安全技术体系架构由用户终端安全、载运装备单元安全、基础设施单元安全、计算中心安全、网络和通信安全、通用安全技术六部分构成，通用安全技术是对其余五个体系组成部分共性要求的汇总，见图1。

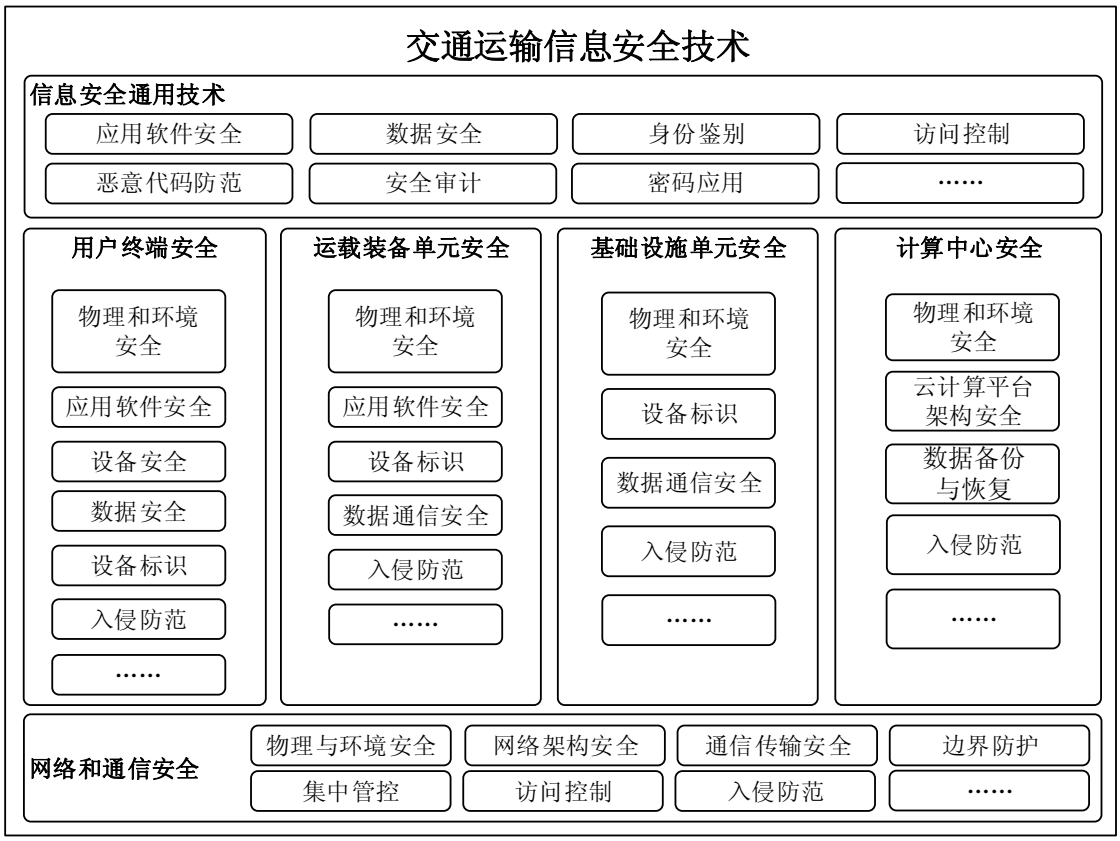

图1 交通运输信息安全体系架构图

5 交通运输信息系统通用安全技术要求

5.1 应用软件安全

应用软件安全技术要求包括：

a) 交通运输信息系统相关软件上线前，均应通过软件安全性测试；

b) 交通运输信息系统中应用软件应及时升级到最新版本，在软件升级前应进行必要的验证；如需远程升级，需在具有系统安全保障的条件下进行，并记录升级过程的相关信息；

c) 交通运输信息系统中的重要应用软件应具备相应的抗应用层攻击和渗透入侵能力；

d) 交通运输信息系统中的各软件应能监测、记录网络运行状态和各类网络安全事件，留存相关的网络日志不少于六个月；

e) 交通运输信息系统中的重要应用软件在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复；

f) 交通运输信息系统中的重要应用软件在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施。

5.2 数据安全

数据安全技术要求包括：

a) 应采用校验码技术或密码技术保证交通运输重要数据在传输过程和存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要个人信息等；
b) 应采用密码技术保证交通运输重要数据在传输过程和存储过程中的保密性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要个人信息等；
c) 交通运输信息系统运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内安全存储；
d) 应提供交通运输重要数据的本地数据备份与恢复功能，定期备份重要数据；
e) 交通运输关键信息基础设施等应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
f) 交通运输信息系统应仅采集和保存业务必需的用户个人信息（姓名、交通工具编号等），并对其用户信息严格保密，建立健全用户信息保护制度；
g) 应禁止未经授权访问和非法使用用户个人信息；
h) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
i) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

5.3 身份鉴别

身份鉴别技术要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b) 应强制用户首次登录时修改系统设置的初始口令；
c) 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术应使用密码技术来实现。
d) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
e) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关必要的保护措施；
f) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；
g) 应强制用户首次登录时修改初始口令；
h) 按照“后台实名、前台自愿”的原则，要求用户在各类交通运输应用中进行实名身份（基于姓名、身份证号、VIN 号、移动电话号码等）注册，系统应对实名情况进行校验。

5.4 访问控制

访问控制技术要求包括：

a) 应提供访问控制功能，对登录的用户分配账号和权限；
b) 应重命名或删除默认账号，修改默认账号的默认口令；
c) 应及时删除或停用多余的、过期的账号，避免共享账号的存在；
d) 应授予不同账号为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

5.5 恶意代码防范

系统应具备恶意代码(包括病毒、蠕虫、木马等)进行检测和清除的能力，并维护恶意代码防护机制的升级和更新。

5.6 安全审计

安全审计技术要求包括：

a) 应对交通运输信息系统中的关键节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
d) 应确保审计记录的留存时间符合法律法规要求；
e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；
f) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；
g) 应对审计进程进行保护，防止未经授权的中断。

5.7 密码应用

密码应用技术要求包括：

a) 交通运输重要信息系统应采用交通运输行业统一的密钥和数字证书；
b) 交通运输重要信息系统采用密码技术保证应用系统实现身份鉴别、访问控制等安全功能，确保审计记录、数据存储和通信安全。
c) 使用的密码技术应确保自主可控；
d) 同时运行在公网和专网的信息系统，须使用密码技术保证网络系统实现安全访问路径、访问控制、身份鉴别功能；
e) 应采用密码技术保证主机设备、网络设备实现身份鉴别、访问控制、审计记录、数据传输安全、数据存储安全和程序安全；
f) 应采用密码技术实现专用终端、运载工具侧设备和基础设施侧设备的接入认证。

6 用户终端安全技术要求

6.1 物理和环境安全

物理和环境安全技术要求包括：

a) 专用用户终端应具备与工作环境相适应的物理防护措施，具备必要的防挤压、防水等能力；
b) 专用用户终端的身份标识装置应具备防物理拆卸、逻辑破坏和伪造等功能，发现标识异常时，应停止服务并发出和上传警示信息。

6.2 应用软件安全

应用软件安全技术要求包括：

a) 应用软件应经过信息系统运营者自身授权和安全评估，能够支持实现运载工具侧设备和移动应用软件安全防护需求（如密钥管理、身份认证管理、远程升级管理、安全监控、数据安全、恶

意代码防护等），形成运载工具侧、移动应用软件和服务平台的一体化防御体系；

b） 移动应用软件应对运行环境进行安全检测，如限制在 ROOT 或越狱等环境下使用；

c） 移动应用软件应具有版本检测机制，提供版本更新功能；

d） 移动应用软件应具有通信数字证书安全性校验功能；

e） 应支持移动业务应用软件仅运行在安全环境内，防止被恶意代码攻击；

f） 移动应用软件在上线前，应经过安全检测；

g） 专业移动终端上的应用软件应经过单位自身授权和安全评估。

6.3 设备安全

设备安全技术要求包括：

a） 应对专用用户终端的启用、维护、弃置等进行全生命周期管理；

b） 专用用户终端在启动前应进行安全检测；

c） 专用用户终端应拆除或封闭不必要的数据传输物理接口；

d） 对于能够接入外部设备的专用用户终端，应具有防恶意软件和入侵防护能力，对临时接入设备采取病毒查杀等安全预防措施。

6.4 数据安全

数据安全技术要求包括：

a） 专用移动终端、卡证读写设备等应采用安全模块或者达到同样安全等级的芯片存储密钥和敏感信息；

b） 定期备份关键业务数据；

c） 对用户信息（包括运载工具所有者与使用者、运载工具基础信息等）的采集、存储、传输和使用，须经过用户的明确授权。

6.5 设备标识

专用移动终端、卡证读写设备等应具有可寻址的唯一性标识，发起信息传输时应进行自身身份标识。

6.6 入侵防范

入侵防范技术要求包括：

a） 用户终端应关闭不需要的系统服务、默认共享和高危端口；

b） 专用用户终端应遵循最小安装的原则，仅安装需要的组件和应用程序。

7 载运装备单元安全技术要求

7.1 物理和环境安全

物理和环境安全技术要求包括：

a） 载运装备运行状态控制或辅助驾驶等载运装备单元应具备监测并拒绝非法物理接入的能力；

b） 为生命安全级、行驶辅助级应用提供逻辑计算基础数据的载运装备单元，应具备抗通信干扰和物理破坏等能力，并具备异常状态监测和报警的能力。

7.2 应用软件安全

应用软件安全技术要求包括：

a) 载运装备单元应用应采用经过相关的授权和安全评估，并选择具有相应安全措施（如安全启动、安全升级、安全通信、安全存储、安全监控、恶意代码防护等）的安全软件。

b) 载运装备单元应用软件应根据功能和操作需求，关联到一个应用优先级，包括生命安全级、行驶辅助级和增值服务级。

c) 生命安全级、行驶辅助级的应用软件，应进行安全性的专项测试，增值服务级应用软件按需进行安全性专项测试；

d) 生命安全级、行驶辅助级和增值服务级的资源占用优先级应逐级降低。

7.3 设备标识

设备标识技术要求包括：

a) 载运装备单元应具有可寻址的唯一性标识，发起信息传输时应进行自身身份标识；

b) 载运装备单元的身份标识装置应具备防逻辑破坏和伪造等功能，发现标识异常时，应停止服务并发出和上传警示信息。

c) 载运装备单元与中心系统、基础设施单元、专用用户终端、卡证读写设备、卡证之间应实现安全注册和基于密钥或证书的身份认证等功能。

7.4 数据通信安全

数据通信安全技术要求包括：

a) 载运装备单元与中心系统、基础设施单元、专用用户终端、卡证读写设备、卡证之间的网络传输和通信应确保数据的保密性、完整性和隐私性；

b) 载运装备单元与中心系统、基础设施单元、专用用户终端、卡证读写设备之间的网络传输和通信应能辨识数据的有效性和新鲜性等，并具有数据过滤功能；

c) 对用户信息（包括车主、车辆使用者、车辆基础信息、车辆运行数据等）的采集、存储、传输和使用，必须经过用户的明确授权。

7.5 入侵防范

入侵防范技术要求包括：

a) 载运装备单元操作系统应遵循最小安装原则，并具备相应的恶意代码防范能力；

b) 应对载运装备实现远程访问的端口进行严格控制，关闭不必要的端口；

c) 应对载运装备的全部访问点（如蓝牙、USB、CD、诊断接口、调试接口、定位系统、TPMS 射频通信、车钥匙射频通信、RFID 等）进行配置、访问控制（如白名单、数据流向、数据内容等）；

d) 载运装备关键网络边界设备（如 T-BOX、网关等）需提供边界安全防护功能；

e) 载运装备单元与外部通信采用安全接入方式，并根据应用优先级，通过不同的安全通信子系统接入网络。

f) 应采用物理隔离、强逻辑隔离或其他技术措施，实现生命安全级、行驶辅助级、增值服务级应

用的边界防护；

g) 承载生命安全级、行驶辅助级应用的载运装备单元应具备入侵防护功能和相应的报警能力，遵循故障安全原则。

8 基础设施单元安全技术要求

8.1 物理和环境安全

物理和环境安全技术要求包括：

a) 基础设施单元应具备防盗、防雷、防火、防水等物理安全防护能力和报警功能；

b) 基础设施侧设备应能保证持续的电力供应；

c) 基础设施单元在位置选择时应避免强光、电磁等辐射源的干扰；

d) 基础设施单元应具备抵御电磁、通信等干扰的能力；

e) 合作式智能交通系统等重要的基础设施单元应通过冗余或其它措施确保设备的可用性，应能够监测设备状态并提供设备不可用报警。

8.2 设备标识

设备标识技术要求包括：

a) 基础设施单元应具有可寻址的唯一性标识，发起信息传输时应进行自身身份标识；

b) 基础设施单元的身份标识装置应具备防物理拆卸、逻辑破坏和伪造等功能，发现标识异常时，应停止服务并发出和上传警示信息。

c) 基础设施单元与中心系统、载运装备单元或专用用户终端、卡证读写设备、卡证之间应实现安全注册和基于密钥或证书的身份认证等功能。

8.3 数据通信安全

数据通信安全技术要求包括：

a) 基础设施单元一般不应存储关键业务数据，确需存储的应存储于安全模块或者达到同样安全等级的芯片中；

b) 基础设施单元与中心系统、载运装备侧或专用用户终端、卡证读写设备、卡证之间的网络传输和通信应确保数据的保密性、完整性和隐私性；

c) 基础设施单元与中心系统、载运装备侧或专用用户终端、卡证读写设备之间的网络传输和通信应能辨识数据的有效性和新鲜性等，并具有数据过滤功能；

d) 基础设施侧视频监控设备应具有码流签名功能；

e) 基础设施侧语音、视频等发布类系统或设备应采用校验码技术、特定的文件格式协议或等同强度手段保证数据完整性。

8.4 入侵防范

入侵防范技术要求包括：

a) 基础设施侧设备应拆除或封闭不必要的 USB、光驱、无线等接口。若确需使用，通过技术手段

实施严格访问控制；

b) 基础设施侧设备应具抵御远程非法控制的能力；

c) 应能监测到广播、电子指示等基础设施侧设备的非法接入并报警；

d) 承载照明控制、通风控制、消防控制、船闸控制等系统运行的网络，应和其他网络实现物理隔离。

9 计算中心安全技术要求

9.1 物理和环境安全

物理和换届安全技术要求包括：

a) 机房应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房应具备访问控制、防盗窃和防破坏等措施；

c) 机房应设置避雷、火灾自动消防、防静电、防水和防潮等装置；

d) 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；

e) 应用确保系统电力的持续供应；

f) 应采用电磁防护措施，防止外界电磁干扰、设备寄生干扰和线路相互干扰等；

g) 确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内。

9.2 云计算平台架构安全

赟计算平台架构安全技术要求包括：

a) 实现不同云租户虚拟网络之间的隔离；

b) 保证云计算平台管理流量与云租户业务流量分离；

c) 云租户能根据业务需求自主设置安全策略集并加载安全服务；

d) 确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限；

e) 保证分配给虚拟机的内存空间仅供其独占访问；

f) 能够对应用系统的运行状况进行监测，并在发现异常时进行告警；

g) 能监测到虚拟机与宿主机之间的异常流量，并进行告警；

h) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

i) 针对重要业务系统提供加固的操作系统镜像；

j) 当进行远程管理时，管理终端和云计算平台边界设备之间建立双向身份验证机制；

k) 保证云服务方对云租户系统和数据的操作可被云租户审计；

l) 能监测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

m) 虚拟机所使用的内存和存储空间回收时应能得到完全清除。

9.3 数据备份与恢复

数据备份与恢复技术要求包括：

a) 应定期备份关键业务数据；
b) 云租户应在本地保存其业务数据的备份；
c) 应提供查询云租户数据及备份存储位置的方式；
d) 应具备将业务系统及数据迁移到其他云计算平台和本地系统的技术手段。

9.4 入侵防范

入侵防范技术要求包括：
a) 应检测、防止或限制从外部发起的对计算中心的攻击行为；
b) 应检测和限制从内部发起的对计算中心的攻击行为；
c) 当检测到攻击行为时，记录攻击源地址、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

10 网络与通信安全技术要求

10.1 物理和环境安全

物理和环境安全技术要求包括：
a) 网络与通信设备应具备防盗、防雷、防火、防水等物理安全防护能力和报警功能；
b) 网络与通信设备应能保证持续的电力供应；
c) 网络与通信设备应具备抵御电磁、通信等干扰的能力。

10.2 网络架构安全

网络架构安全技术要求包括：
a) 应保证网络设备的处理能力和带宽资源满足交通业务信息通讯高峰期的需要；
b) 应提供通信线路、关键网络设备的硬件冗余，保证交通信息系统的可用性；
c) 应合理划分安全域、子网或网段，通过采用可靠的技术隔离措施等方式保证交通信息网络结构安全；
d) 应避免将重要交通信息网络区域部署在网络边界处且没有边界防护措施。

10.3 通信传输安全

通信运输安全技术要求包括：
a) 应能够采用校验码技术或密码技术保证交通运输信息通信过程中数据的完整性；
b) 应采用密码技术保证交通运输信息通信过程中敏感信息字段或整个报文的保密性；
c) 应能够在通信前基于密码技术对交通运输信息通信的双方进行验证或认证；
d) 应可按照业务服务的重要程度为交通运输数据设置优先级并据此分配带宽，优先保障高优先级的重要业务。

10.4 边界防护

边界防护技术要求包括：
a) 应保证跨越边界的交通运输业务访问和数据流通过边界防护设备提供的受控接口进行通信；

b) 应能够对非授权设备私自联到交通运输业务内部网络的行为进行限制或检查，并对其进行有效阻断；
c) 应能够对交通运输业务内部用户非授权联到外部网络的行为进行限制或检查，并对其进行有效阻断；
d) 应确保有线网络与无线网络边界之间的通信经过无线接入网关设备；
e) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。

10.5 集中管控

集中管控技术要求包括：

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
b) 应能够建立一条安全的交通运输信息传输路径，对网络中的安全设备或安全组件进行管理；
c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析；
e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
f) 应能对网络中发生的各类安全事件进行识别、报警和分析。

10.6 访问控制

访问控制技术要求包括：

a) 进行网络或通信设备的远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
b) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
c) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
d) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
e) 应能根据会话状态信息为进出的交通运输数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。

10.7 入侵防范

入侵防范技术要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的对交通运输信息网络的攻击行为；
b) 应在关键网络节点处检测和限制从内部发起的对交通运输信息网络的攻击行为；
c) 应采取技术措施对交通运输信息系统的网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；
d) 当检测到攻击行为时，记录攻击源地址、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
e) 无线接入设备应能够对非授权用户终端接入的行为进行检测、记录、定位；
f) 应具备对针对无线接入设备的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位。