# 附件3：

## 鄂尔多斯市智能网联汽车网络安全管理规范（试行）（征求意见稿）

**第一条** 为规范我市智能网联汽车网络安全管理要求，安全有序推进智能网联汽车在我市发展，维护国家安全和社会公共利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《智能网联汽车准入和上路通行试点实施指南（试行）》《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》等法律法规要求，结合本市实际情况，制定本规范。

**第二条** 落实网络安全主体责任。各相关企业要建立网络安全管理制度，明确负责人和管理机构，落实网络安全保护责任。强化企业内部监督管理，加大资源保障力度，及时发现并解决安全隐患。加强网络安全宣传、教育和培训。

**第三条** 全面加强网络安全防护。各相关企业要采取管理和技术措施，按照车联网网络安全相关标准要求，加强汽车、网络、平台、数据等安全保护，监测、防范、及时处置网络安全风险和威胁，确保数据处于有效保护和合法利用状态，保障车联网安全稳定运行。

加强智能网联汽车的网络安全防护能力。智能网联汽车生产企业要依据行业管理要求开展整车网络安全架构设计，保障车辆网络安全。保障车内系统通信安全，具备安全认证、分域隔离、访问控制等措施，防范伪装、重放、注入、拒绝服务等攻击。具备车载信息交互系统、汽车网关、电子控制单元等关键设备和部件安全防护和安全检测能力。提供对诊断接口（OBD）、通用串行总线（USB）端口、充电端口等的访问和权限管理。满足强制性标准《汽车整车信息安全技术要求》等国家相关标准规范。

加强路侧智能交通基础设施网络安全防护能力。相关智能网联路侧终端设备企业应开展终端网络安全架构设计。提供终端内系统通信安全保障，强化安全认证、访问控制等措施，防范伪装、重放、注入、拒绝服务等攻击。加强路侧单元等关键设备的安全防护和安全检测。加强网络接入端口的访问控制和权限管理。

**第四条** 落实网络安全漏洞管理责任。智能网联汽车、路侧智能交通基础设施终端生产企业或使用主体应落实安全漏洞管理责任。相关企业应根据《网络产品安全漏洞管理规定》有关要求，明确本企业漏洞发现、验证、分析、修补、报告等工作程序。发现或获知汽车、智能终端产品存在漏洞后，应立即采取补救措施，并向国家指定的网络安全威胁和漏洞信息共享平台报送漏洞信息。对需要用户采取软件、固件升级等措施修补漏洞的，应当及时将漏洞风险及修补方式告知可能受影响的用户，并提供必要技术支持。

**第五条** 提升全流程道路交通安全保障能力。相关单位须具备智能网联汽车运行安全以及智能交通设施相关网络安全风险防控、隐患排查、应急处置等事前、事中、事后全流程保障能力。

**第六条** 提升车联网网络安全防护与管理能力。各相关企业要严格落实网络安全分级防护要求，加强网络设施和网络系统资产管理，合理划分网络安全域，做好访问控制管理，做好网络边界安全防护，采取防范木马病毒和网络攻击、网络侵入等危害车联网安全行为的技术措施。自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患。

**第七条** 提升车联网通信安全防护与管理能力。各相关企业要建立车联网身份认证和安全信任机制，强化车载通信设备、路侧通信设备、服务平台等安全通信能力，采取身份认证、加密传输等必要的技术措施，防范通信信息伪造、数据篡改、重放攻击等安全风险，保障车与车、车与路、车与云、车与设备等场景通信安全。鼓励相关企业、机构接入国家级车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互认互通。

**第八条** 提升车联网安全监测预警能力。车辆生产企业、运营主体须建设车联网网络安全监测平台，开展网络安全威胁、事件的监测预警通报和安全保障服务。各相关企业要建立网络安全监测预警机制和技术手段，对智能网联汽车、车联网服务平台及联网系统开展网络安全相关监测，及时发现网络安全事件或异常行为，并按照规定留存相关的网络日志不少于6个月。

**第九条** 提升车联网安全应急处置能力。智能网联汽车生产企业、车联网服务平台运营企业要建立网络安全应急响应机制，制定网络安全事件应急预案，定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照《公共互联网网络安全突发事件应急预案》等规定向有关主管部门报告。

**第十条** 提升车联网网络安全防护定级备案能力。智能网联汽车生产企业、车联网服务平台运营企业要按照车联网网络安全防护相关标准，对所属网络设施和系统开展网络安全防护定级工作，并向市公安局备案。对新建网络设施和系统，应当在规划设计阶段确定网络安全防护等级，市公安局负责定级备案审核工作。

**第十一条** 提升车联网相关平台网络安全管理能力。车联网服务平台运营企业须采取必要的安全技术措施，加强智能网联汽车、路侧设备等平台接入安全，主机、数据存储系统等平台设施安全，以及资源管理、服务访问接口等平台应用安全防护能力，防范网络侵入、数据窃取、远程控制等安全风险。涉及在线数据处理与交易处理、信息服务业务等电信业务的，应依法取得电信业务经营许可。认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

**第十二条** 提升汽车在线升级服务（OTA）安全保障和漏洞检测评估能力。智能网联汽车生产企业要建立在线升级服务软件包安全验证机制，采用安全可信的软件。开展在线升级软件包网络安全检测，及时发现产品安全漏洞。具备在线升级服务安全校验能力，采取身份认证、加密传输等技术措施，保障传输环境和执行环境的网络安全。具备在线升级服务全过程的网络安全监测和应急响应，定期评估网络安全状况，防范软件被伪造、篡改、损毁、泄露和病毒感染等网络安全风险。

**第十三条** 提升应用程序安全管理能力。智能网联汽车生产企业、车联网服务平台运营企业要建立车联网应用程序开发、上线、使用、升级等安全管理制度，提升应用程序身份鉴别、通信安全、数据保护等安全能力。具备车联网应用程序安全检测能力，及时处置安全风险，防范恶意应用程序攻击和传播。

**第十四条** 本规范自印发之日起施行。