信息安全管理手册

文 件 编 号：ISMS-2022

版/次：V1.0

主编：张少辉 审核：张少辉 批准：郭发玉

2022 年 10 月 12 日发布 2022 年 10 月 13 日实施

修订记录

序号	修订日期	页码	版/次	修订内容	修订人
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					

前言

为了证明本公司有能力稳定的提供满足顾客和适用的法律法规要求的产品，通过信息安全管理体系有效运行，在公司内部达到持续改进、缺陷预防、减少变差和浪费，最终达到顾客满意的目的，结合公司体系策划和实际运行情况，特制定本管理手册。

本文件由欧玛（中国）汽车部件有限公司总经办归口管理。

主要起草单位：总经办/信息安全体系组

主要起草人：总经办/张少辉

主要审核人：管理者代表/张少辉

主要批准人员：总经理/郭发玉

本文件版本号：V1.0

本手册首次发布。

管理手册

0.1 发布令

为提高欧玛（中国）汽车部件有限公司的信息安全管理水平，保障我公司业务活动的正常进行，防止由于信息系统的中断、数据的丢失、敏感信息的泄密所导致的公司和客户的损失，我公司开展贯彻TISAX（Trusted Information Security Assessment Exchange）标准中的信息安全工作，建立、实施和持续改进文件化的信息安全管理体系，制定了公司的《信息安全管理手册》。

《信息安全管理手册》是企业的法规性文件，是指导企业建立并实施信息安全管理体系的纲领和行动准则，用于贯彻企业的信息安全管理方针、目标，实现信息安全管理体系有效运行、持续改进，体现企业对社会的承诺。

《信息安全管理手册》符合有关信息安全法律、法规要求及TISAX（Trusted Information Security Assessment Exchange）标准信息安全要求和企业实际情况，现正式批准发布，自2022.10.13起实施。企业全体员工必须遵照执行。

全体员工必须严格按照《信息安全管理手册》的要求，自觉遵循信息安全管理方针，凡不遵循信息安全，可能出现信息系统的中断、数据的丢失、敏感信息的泄密所导致的企业和客户的损失，所以说信息安全非常重要，所有员工均应贯彻实施本手册的各项要求，努力实现公司信息安全管理方针和目标。

总经理：郭发玉

签发日期：2022 年 10 月 12 日

0.2 管理者代表授权书

为贯彻执行信息安全管理体系,满足TISAX(Trusted Information Security Assessment Exchange）标准信息安全的要求，加强领导，特任命

张少辉为我公司信息安全管理者代表。

授权代表有如下职责和权限：

1. 确保按照标准的要求，进行资产识别和风险评估，全面建立、实施和保持信息安全管理体系；
2. 负责与信息安全管理体系有关的协调和联络工作；
3. 确保在整个公司内提高信息安全风险的意识；
4. 审核风险评估报告、风险处置计划；
5. 制定审核程序文件；
6. 主持信息安全管理体系内部审核，批准内审报告；
7. 向最高管理者报告信息安全管理体系的业绩和改进要求，包括信息安全管理体系运行情况、内外部审核情况。

本授权书自任命日起生效执行。

总经理：郭发玉

签发日期：2022 年 10 月 12 日

0.3 公司简介

0.3.1 综述

欧玛（中国）汽车部件有限公司由意大利 OMR 集团和河南广瑞集团于 2007 年合资组建，致力于非公路用车所用驱动桥、转向节、悬挂支架、变速箱壳体的研发、制造历时 15 年，成长为国家级专精特新“小巨人”企业、高新技术企业、汽车分行业排头兵企业、中国绿色铸造企业、河南省重点“小巨人”企业、河南省智能车间示范企业、河南省绿色铸造示范企业、新乡市智能制造标杆企业。

公司建有省级企业技术中心，组建了高水平研发团队，严格按照 APQP 程序、SGS 国际规范实施新产品研发，申报各项专利 37 项，拥有自主知识产权核心技术，并与意大利 OMR 国际研发平台、郑州大学等科研机构和高等院校进行定向合作，专注于产学研与科技成果转化的紧密结合。

公司多项产品连年多次荣获中国国际铸件博览会“优质铸件金奖”，得到世界 500 强企业或行业中的龙头企业等众多客户的青睐，与之建立起坚实的合作伙伴关系。公司已成为河南省规模最大的车桥壳体供应企业，市场占有率超过 35%以上，其中大马力轮拖桥壳为国内细分市场冠军产品。

0.3.2 公司详细地址及联系方式：

公司地址：河南省辉县市城西工业园区外环路东

邮编：453600

邮箱：omrc@sina.com

电话：15225973906

网址：http://www.omr-c.com/

0.4 术语

0.4.1.信息系统

指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

0.4.2.计算机病毒

指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

0.4.3.信息安全事件

指导致信息系统不能提供正常服务或服务质量下降的技术故障事件、利用信息系统从事的反动有害信息和涉密信息的传播事件、利用网络所从事的对信息系统的破坏窃密事件。

0.4.4.相关方

关注本公司信息安全或与本公司信息安全绩效有利益关系的组织和个人。主要为：政府、上级部门、供方、用户等。

0.4.5.原型区域

顾客需要保护的车辆、部件和零件，这些车辆、部件和零件尚未向公众展示和/或 OEM 以适当的形式发布，该类产品的设计、制造、检验、存储等相关区域

0.4.6.信息安全术语的英文缩写

TISAX：Trusted Information Security Assessment Exchange 可信信息安全评估交互；

ISMS：Information Security Management Systems 信息安全管理体系；

SOA：Statement of Applicability 适用性声明；

PDCA：Plan Do Check Action 计划、实施、检查、改进。

ISA：Information Security Assessment 信息安全评估；

1 政策和组织

1.1 信息安全政策

1.1.1 信息安全策略

1.1.1.1 信息安全管理方针目标

为防止由于信息系统的中断、数据的丢失、敏感信息的泄密所导致的企业和客户的损失，本公司建立了信息安全管理体系，制订了信息安全方针，确定了信息安全目标。

信息安全管理方针：

增强风险意识，保障信息安全，防止泄密事件，实现持续改进。

为了保证各种信息资产的保密性、完整性、可用性，切实推行信息安全管理，积极预防风险，完善控制措施，提高客户信任度，确保公司业务的连续性，公司依据 TISAX（Trusted Information Security Assessment Exchange）标准信息安全要求，建立信息安全管理体系，并承诺如下：

1) 在公司内各层次建立完整的信息安全管理组织机构及信息安全管理策略，确定信息安全方针、安全目标和控制措施，明确信息安全的管理职责；

2) 识别并满足适用法律、法规和客户等相关方信息安全要求；

3) 定期进行信息安全风险评估，内审，采取纠正预防措施，保证体系的持续有效性；

4) 采用先进有效的设施和技术，处理、传递、储存和保护各类信息；

5) 对全体员工进行持续的信息安全教育和培训，不断增强员工信息安全意识和能力；

6) 制定并保持完善的业务连续性计划，实现可持续发展；

7) 对于基本方针的适用性、充分性，结合实际状况定期评审，必要时予以修订；

8) 如 ISMS 体系发生任何的变更，应将变更的信息告知相关的员工和外部业务合作伙伴。

公司级的信息安全目标如下：

序号	指标名称	目标值	评价周期	目标属性
01	■.系统可用率	99.5%	每月	可用性
02	■.加密软件覆盖率（安全区域）	100%	每季度	保密性
03	■.数据异地灾备率	100%	每季度	完整性
04	■.应急预案演练参与率	100%	每年	可用性
05	■.重要信息泄密数	0	每季度	保密性

公司信息安全由总经办负责，总经办负责人负责管理、协调各部门保障信息安全。监

督、检查、分析和评价信息安全运行的有效性，并将结果报告给管理层。

1.1.1.2 信息安全管理体系手册管理

管理者代表负责组织编制《信息安全管理手册》，总经理负责批准。

总经办负责按《文件管理程序》的要求，进行《信息安全管理手册》的登记、发放、回收、更改、归档、作废与销毁工作；

《信息安全管理手册》手签名版的仅有一本，存档于总经办。手册电子版由总经办挂到公司内网企业号，对公司所有人员授权公开查阅，内网已设置权限，只能查阅，不能下载，也不能修改；当利益相关方提出要求时，应根据信息安全等级和信息传输的要求提供给利益相关方。

手册描述的过程适合公司的活动、产品及服务的实际，所有部门和全体员工必须严格遵守本手册中的规定。管理体系程序文件及相关的控制指导书必须与本手册相一致，任何人不得将包括本手册的体系文件内容全部或部分向外界泄露或供他人使用。为保证管理体系的有效运行，授权管理者代表负责本手册的贯彻实施和解释；手册的管理和日常监督授权总经办负责。

当依据的 TISAX（Trusted Information Security Assessment Exchange）标准信息安全要求有公司的结构、内外部环境、法律法规、VDA ISA 标准、关键顾客要求等发生重大改变时，将对变化的影响范围进行审查，由总经办组织对《信息安全管理手册》进行换版，必要时将通知相关方。

1.2 信息安全组织

1.2.1 信息安全管理边界

为了建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系（简称 ISMS），确定信息安全方针和目标，对信息安全风险进行有效管理，确保全体员工理解并遵照执行信息安全管理体系文件、持续改进信息安全管理体系的有效性，特制定本手册。本信息安全管理体系手册按照 TISAX 的要求，覆盖 VDA ISA5.1 标准信全部内容。本公司的业务不涉及原型零部件，因此本手册删减原型保护和数据保护的相关条款要求，详见附录 5：《VDA ISA 适用性声明（VDA ISA5.1）》。

公司 ISMS 范围为：TISAX Participant Handbook.v2.5 中 2.0 标准范围，包括公司汽车桥壳、转向节等零部件的制造相关的信息安全管理活动。

企业名称：欧玛（中国）汽车部件有限公司

地理区域为：河南省辉县市

评估内容和等级：Information Security/AL3、Prototype Protection/AL3；

公司按照 TISAX 信息安全要求，执行 ISMS 体系的控制。

公司建立《信息安全管理体系手册》和相关文件，建立了全面的信息安全要求，均由领导批准并实施。

总经办每年依据 VDA ISA 评估表，组织信息安全小组对公司内部进行信息安全管理自评估（内部审核），验证 ISMS 的运行符合性、有效性，并将结果汇报给管理层。

总经办根据 VDA ISA 编制 SOA,对 VDA ISA 问卷的所有问题确定适用的控制措施。

公司的管理层每年需对 ISMS 运行的有效性进行评审（如管理评审），至少一次。

1.2.2 信息安全责任组织

本公司总经理为信息安全最高责任者。总经理指定信息安全管理者代表。

各部门负责人为本部门信息安全管理责任者，全体员工都应按保密承诺的要求自觉履行信息安全保密义务；公司的信息安全组织架构见附录 1《欧玛（中国）汽车部件有限公司组织架构图》；各部门、人员有关信息安全职责分配见下表：

部门/负责人	职责和分工
总经理	信息安全负责人； 负责本单位网络与信息安全重大事项的决策和协调； 负责对公司的管理层进行任命，负责 ISMS 职责和权限分配； 为信息安全管理体系的策划、实施、运行和改进提供必要的资源； 并对全公司信息安全工作负责； 定期举行管理评审，评审体系运行状况；
管理者代表	详见 0.2 管理者代表授权书
总经办	1、识别公司的信息安全资产，分析重要的信息安全资产；对信息资产分类管理；对各种信息资产进行标识；负责可移动介质的管理；根据公司的内部外部因素，分析风险和机会，制定措施处置高风险，制定措施控制低风险； 2、负责网络和网络服务访问；负责用户注册、访问权限开通、访问权限管理、访问的撤销或调整；制定安全登录规程；控制特殊软件工具的使用；控制源代码程序的访问； 3、制定文件化的操作规程；变更管理；负责容量管理；负责保证开发、测试、运

部门/负责人	职责和分工
	行环境分理；负责对恶意软件的检测、预防和回复；负责信息的备份；负责事态记录；日志信息保护；负责管理员和操作员日志评审；负责时钟同步管理；负责管理系统上安装的软件；负责对信息系统脆弱性制定措施处理相关的风险；负责软件安装限制的管理；负责系统验证审计的要求和审计工作； 4、负责网络控制；负责信息传递（电子消息发送、）控制；定期评审信息保护措施 5、负责对第三方开发的软硬件系统的测试、验收； 6、制定信息安全连续性计划；实施信息安全连续性计划；验证、评审和评价信息安全连续性计划；信息处理设备的冗余部署； 7、收集信息安全管理数据，统计、分析和评价信息安全管理体系的绩效。法律法规及合同要求的识别并保持最新；保护知识产权和所有权的软件使用符合法律法规和合同的要求；保护记录，满足法律法规的要求；保护个人信息、使用密码控制符合协议、法律和法规； 8、定期按 TISAX 要求开展自评并汇报给管代和最高管理者，负责自评问题改进闭环。 9、制定信息安全事件的规程；向相关方报告信息安全事件的情况；评估信息安全事件并响应；信息安全事件的总结； 10、依据信息安全管理体系的绩效数据、管理评审的决策，分析数据，确定信息安全管理改进方向，确定改进目标，制定改进措施，跟踪改进的措施实施，评价结果； 11、公司与信息安全相关人员的招聘、培训、任用、离职过程的管理；公司与信息安全相关人员的培训过程的管理； 12、负责组织实施供应商的选择，包括对供应商信息安全水平的评审； 13、负责方管理并与供应商及合作伙伴签订保密协议； 14、负责向供应商及合作伙伴传达顾客和公司对信息资产的保护要求； 15、负责组织与供应商及合作伙伴的信息沟通、传输、确认； 16、负责监视、评审和审计供应商服务交付； 17、负责服务供应商涉及信息安全的变更管理；

部门/负责人	职责和分工
	18、将顾客和组织的信息安全要求纳入项目管理目标； 19、在相关管理中识别信息资产和保护信息资产； 20、在相关管理中测试信息安全管理的效果； 21、在重要信息资产创建、传输、使用、变更、储存、销毁过程中保护信息安全；对重要数据进行备份、备份测试；
财务部	1、组织建立财务管控体系，建立健全财务管理制度; 2、负责资金收支管理，合理使用、调度集团资金并定期对集团经营情况进行分析; 3、主持财务报表及财务预决算的编制工作，编制月、季、年度财务报告 4、策划纳税方案，按时缴纳各种税款，按时完成税务申报以及年度审计工作; 5、加强日常财务管理和成本控制，合理控制费用支出，负责成本费用的预算、控制、考核及分析; 6、管理财务团队的日常运作，监管、指导下属工作，提升本部门的业务水平; 7、财务用友软件的使用和管理，对财务数据进行管理；
销售部	1、线下展会活动策划、组织与执行； 2、各社交平台公司网站运营； 3、客户、行业、竞争对手分析； 4、企业市场文化宣传； 5、宣传物料设计与制作 ； 6、公司网站的运营和维护；
销售部	1、负责开发新客户，获取顾客信息及顾客对信息保护的要求； 2、负责维护老客户，对客户信息的保护措施； 3、客户需求分析，组织各部门对顾客要求进行评审、确定； 3、负责向组织内部传达顾客的信息安全要求； 4、负责与顾客沟通信息安全管理的成果； 5、负责处理与顾客相关的信息安全事件的沟通和处理； 6、负责监督和管理组织内部顾客的信息资产； 7、客户管理（合同、PO、开票、付款、客户满意度、客户计划、收益分析)；

部门/负责人	职责和分工
其他部门	1、支持以上信息安全相关的管理活动，人事部门的信息资产、控制操作安全、通信安全； 2、积极配合控制和处理信息安全事件，基于风险的思维，对于重要资产实施控制。 a） 遵守信息安全规章制度，遵循操作规范和流程； b） 履行岗位信息安全职责，执行信息安全工作任务； c） 保护信息资产，妥善使用工作所涉及的信息资产； d） 及时上报发生的信息安全事件或发现的信息安全隐患； e） 参与信息安全相关的培训和活动。

总经办对即将上任的人员进行能力评价，让有资格的人员上岗确保完成任务。管理层为各岗位提供工作所必须的资源。

1.2.3 项目管理

根据公司的实际情况对项目管理进行分类，公司的主要的项目分类为业务相关、基础设施建设项目、招聘相关、基础建设等其他支持类项目。在所有项目管理过程中，在项目早期应对识别信息安全的要求并按照《信息安全风险管理程序》（编号：ISMS-A-003）进行风险评估，并确定对信息的保护目标（信息的C,I,A属性），必要时将信息安全目标纳入项目管理目标。当项目发生变化时重复进行风险评估。

1.2.4 外部IT服务供应商管理

总经办编制《相关方信息安全管理程序》，识别与公司相关的IT服务及IT服务供方。在IT服务提供前与IT服务供方确定与服务相关的信息安全要求，并将信息安全的要求增加在服务合同中。在IT服务合同中定义每个组织的责任、责任的分担机制。

现有的IT服务商有网络运营服务商、系统提供服务商等；所有的外部IT服务商都签订合同，规定了对应的保密义务。负责IT的相关人员，都进行信息安全的培训。

1.3 资产管理

1.3.1 信息资产的识别和记录

根据资产的表现形式，将信息资产分为：主要资产（信息、流程、账号/密码、专利、商标等）和支持资产（文档、软件、硬件、服务、通讯设备、移动设备、基础设施等），并为主要资产和支持资产确定负责人，同时为每个关键信息资产都分配各自的支持资产。

信息安全小组每年对信息资产清单进行审核。具体见《信息安全风险管理程序》。

1.3.2 信息资产的分类和管理

公司建立《信息安全风险管理程序》，建立了信息资产分类的方案。资产赋值对资产在保密性、完整性和可用性上的达成程度进行分析，选择对资产保密性、完整性和可用性最为重要（分值最高）的一个属性的赋值等级作为资产的最终赋值结果。资产等级划分为五级，分别代表资产重要性的高低。等级数值越大，资产价值越高。编制《信息处理设施管理程序》，规定了 IT 设备等支持资产的购买、发放、维修、报废等要求。

1.3.3 外部 IT 服务管理

公司的计算机设定权限，员工不能自行安装或卸载软件。所有的软件、IT 服务等，都需要通过 IT 单位进行安装或许可授权后安装。公司规定办公自动化类设备等的采购审批流程，由部门主管审批，分别由 IT 部门、部门经理和总经理等不同级别的领导进行书面批准。

1.4 风险管理

1.4.1 信息安全风险管理

公司建立了《信息安全风险管理程序》，规定了每年评估一次，并且当发生重大信息安全事件时、当重要的信息资产发生重大变化时、IT 单位确定有必要时，要进行风险评估。《信息安全风险管理程序》规定了风险的识别、评估和处置的流程和要求，每个部门建立了风险评估表，识别了风险、分级、控制措施和对应的责任人。根据保密性、完整性、可用性、威胁性、脆弱性等赋值进行风险等级划分。

1.5 评估

1.5.1 信息安全合规性

按照《信息安全风险管理程序》的要求，定期检查验证公司内信息安全政策和制度的遵守情况，核实是否符合信息安全要求，保留审核记录。针对审核中发现的不符合项，按照《内部审核控制程序》要求，推动不符合项的关闭，并保留整改记录（如：法律法规、知识产权、信息安全、网络安全、记录保存）。

1.5.2 ISMS 审查

《内部审核控制程序》规定，针对 ISMS 每三年或发生重大变化时，由体系单位委托第三方咨询公司按照 VDA ISA 检查表的要求实施独立的 ISMS 评估，并对审核的不符合项进行纠正。审核报告作为 TISAX 内审结果，在管理评审时汇报。每年编制内部审核计划，进行内部自评。

1.6 事件管理

1.6.1 信息安全事件处理

公司建立了《信息安全事件管理程序》，对信息安全事件的定义和分类进行了描述，并定义了信息安全事件的处理流程，规定了信息安全事件处置、归档要求，确保信息安全的可追溯性，规定了对应的升级流程，规定中等事故及以下授权由 IT 单位组织处理，重大事故由 IT 单位报总经理决策处理，当对公司产生了重大损失或者关键信息泄密时，由总经理决定是否对网络攻击行为实施报警或起诉。信息安全事件，按照要求登记在《信息安全事件记录》中，确保信息安全的可追溯性。中等以上信息安全事件，按照流程填写《信息安全问题报告》，记录事件，名称、应急处理、原因分析、处理结果等信息。规定了信息安全事件的响应和分析的要求，并制定预防措施，避免类似事件的发生。对于出现重大事件影响到顾客、供应商、政府机关、公益组织等其他相关方声誉或者信息安全时，报公司总经理决策处理后，由销售部等对外对接部门负责对事件的严重度、可能造成的影响度通知到相关方，由相关方提前做出应对措施。

2 人事

2.1.1 敏感工作领域管理

各部门编制了《岗位说明书》，规定各个岗位的职责和权限。人事部根据《岗位说明书》职责要求，对员工进行笔试、面试、复试和体检，由人事经理对合格人员的经历、背景以及以前工作表现情况进行核实，对所有的员工一人一档建档管理。

2.1.2 合同管理

根据《人力资源管理程序》（编号 ISMS-A-009）的要求，由人事部与安全区域、核心岗位人员签订《员工保密协议》，该协议签署后方可上岗。该协议规定了员工的保密内容、保密范围、双方的权利和义务、保密期限、违约责任等内容。

2.1.3 培训管理

按照《人力资源管理程序》（编号 ISMS-A-009）策划信息安全培训活动。在每年的培训计划中纳入信息安全培训课程，并按照计划执行培训，让员工了解信息安全的要求和风险预防。

2.1.4 远程办公管理

建立了《远程工作策略》（编号 ISMS-C-2022），规定了远程办公的操作细则。

在移动办公过程中，非安全区域工作人员禁止访问公司内部资源。安全区域工作人员如需访问公司内部资源，在确保周围物理环境及网络环境的安全下，必须通过 VPN 远程接入，

在接入过程中，不允许同时在网上冲浪，接入完成后，必须及时断开 VPN 连接。在移动办公过程中，只能通过 VPN 访问公司内网共享服务器，VPN 登录时需进行双重验证，在输入静态密码时，也必须输入通过手机短信的一次性动态密码。在移动办公过程中使用设备时，必须防止公司敏感信息被非法窥探。在移动办公过程中，含有敏感或关键业务信息的设备不允许无人值守，必须随身携带或使用物理防护措施来保护设备。

在移动办公过程中，只能通过微信和指定邮箱进行联系，必须防止公司敏感信息被非法窥探。

3 物理安全性和业务连续性

3.1.1 安全区域管理

《安全区域管理程序》（编号 ISMS-A-016）对安全区域进行了定义。现有的安全区域为：公司机房、技术部办公区，对该区域计算机密码每三个月更新一次，在文件中规定安全区域的保密措施并执行。所有涉密人员上岗前应经过保密培训，掌握保密知识技能，签订保密协议，严格遵守保密制度，不得以任何方式泄漏公司秘密。主要的手段有监控、密码、人员管理等。编制《外协车辆人员管理规定》，规定外来人员的管理政策。编制《移动设备管理程序》（编号 ISMS-A-015）定义和实施携带和使用移动 IT 设备和移动数据存储设备的政策，对移动设备进行编号、登记，张贴标签，并设置密码保护。在计算机端设置自动加密软件，自动对所有的信息进行加密保护，包括移动设备上的信息。编制《网络安全管理程序》（编号 ISMS-A-017），规定了网络/基础设施组件的保护要求和访问政策，以防未经授权的访问。编制《用户访问管理程序》（编号 ISMS-A-021），规定进入人员的授权、使用、变更、撤销等管理流程。

3.1.2 信息安全保障

编制《业务连续性管理程序》（编号 ISMS-A-029），识别并记录可能出现的异常情况，包括自然灾害，事故灾难，人为破坏等。规定了异常发生时，应对的措施和流程，确保在特殊情况下的信息防护。《业务连续性管理程序》（编号 ISMS-A-029）规定每年对应急预案进行评审，评审后保留评审记录。规定每年对应急预案进行演练，测试针对危机情况的信息安全措施的有效性。

3.1.3 辅助资产处理

建立《信息安全风险管理程序》（编号 ISMS-A-003），对所有的信息资产进行识别、管控。编制《信息处理设施管理程序》（编号 ISMS-A-019），规定支持资产的运输、储存、维修、丢失、退回及处置。

3.1.4 移动 IT 设备和移动数据存储设备管理

编制《移动设备管理程序》（编号 ISMS-A-015），定义和实施携带和使用移动 IT 设备和移动数据存储设备的政策，对移动设备进行编号、登记，张贴标签，并设置密码保护。

在电脑端设置自动加密软件，自动对所有的信息进行加密保护，包括移动设备上的信息。

4 身份管理和访问管理

4.1 身份管理

4.1.1 身份识别手段应用

需要给员工或访客建立身份档案并授予相关权限时，由部门人员填写申请表，部门负责人进行审批，由 IT 单位根据申请表载明的范围进行授权，保留申请表和授权记录。主要的手段有刷脸、指纹、密码授权等。按照公司各部门岗位工作需要建立信息系统用户，每一个信息系统用户根据使用情况明确责任人，确定用户账户使用的唯一性。严禁设置具有共享权限的用户。员工调岗或离职时，或者访客变动时，IT 单位根据变动记录来更改或撤销权限。进入安全区域，要进部门负责人和 IT 单位的授权，开启门锁方能进入。公司信息系统用户设置默认有效期为 5 年，由系统管理员负责监督。以上详见《用户访问管理程序》（编号 ISMS-A-021）及《外协车辆人员管理规定》。

4.1.2 用户访问安全保障

编制《用户访问管理程序》（ISMS-A-021），规定信息化系统登录的密码策略，规定了不同用户身份的密码设置策略，通过密码访问 IT 系统。普通用户为 6 位密码，管理员用户不低于 10 位，且至少包含三类字符。管理员用户等登陆，需要密码和手机验证码双因素认证。建立《信息安全风险管理程序》（编号 ISMS-A-003），规定高保护需求信息和非常高保护信息的分类和定义。

4.1.3 账户和登录信息管理

建立《用户访问管理程序》（编号 ISMS-A-021），规定了账户创建、修改和删除的要求，不允许设置公司集体账号。供应商所提供账户，由授权的专人管理和登陆，不得将登陆信息外泄。所有系统不允许进行自动登陆，每次都要按照要求验证后方可登陆。且系统在规定的时间内无操作，则自动退出登陆。规定了首次登陆，要强制修改初始登陆密码，禁止使用初始登陆密码登陆。账户的设置，由需求部门人员提出申请，IT 单位创建并授权。

4.2 访问管理

4.2.1 访问权限的分配和管理

通过设置账号权限，来确保只有授权用户才能访问信息和 IT 应用程序。账户的设置，由需求部门人员申请，部门负责人审批后，由 IT 单位创建并授权。详见《用户访问管理程序》（编号 ISMS-A-021）公司规定了对用户获得的权限有正式的文档进行记录，定期审核用户账号和权限，纠正错误的权限分配，关闭无人使用的用户账号，并及时维护相关文档。

5 信息安全/网络保安

5.1 密码应用

5.1.1 加密程序使用

公司所有台式机在分发时，由 IT 单位负责在每台设备上安装安全软件，使用者无法自行卸载。安全软件为公司采购的正版软件。进入安装了加密软件的计算机，由系统自行进行加密。需要解密时，操作者提交解密申请流程，审核者要对解密原因及文件认真审核，确保信息的真实性和安全性后方可解密。《数据安全管理程序》

5.1.2 信息传输管理

操作者如需外发电子文档，根据信息的重要程度或与对方沟通后确定是否制作外发文件，对外发的文件应严格审核。如需密码等信息，通过电话或其他方式，通知文件接收者。内部文件若无特别要求一般加密传输。《电子邮件管理程序》、《信息交换管理程序》

5.2 操作安全

5.2.1 变更管理

信息系统的变更（新的系统、旧系统的升级）编制有《变更管理程序》（编号 ISMS-A-032），评估变更的风险、变更的策划、实施、验证；变更失败的回退计划等。

信息化系统发生变更时，要评价信息安全管控风险和合规性要求。规定了日常性维护需求、审核评审、程序升级维护、程序试运行、和程序正式运行等流程。对变更后的信息系统要进行试运行。当试运行通过后，方可转入正式运行。试运行期间发现升级程序在安全性、业务不适用或不合规时，应立即停止程序升级工作，继续保持原系统运行。升级程序正式运行后，在发现系统有重大 BUG、不符合公司信息安全要求、业务不适用或不合规时，立即停止程序运行，删除补丁程序，退回原有系统版本，确保不影响公司正常业务系统运行。

5.2.2 开发和测试环境

在项目试运行时，原系统和新系统要双规运行，且试运行阶段测试系统不能直接对接

生产环境正式系统，数据隔离，避免开发过程中的错误影响正式生产和公司运行。当试运行通过后，方可正式运行新系统，导入正式生产环境。详见《信息系统应用管理程序》（编号 ISMS-A-022）

在项目试运行时，IT 单位用单独的计算机进行原系统和新系统的双规运行，避免开发过程中的错误影响正式生产和公司运行。当试运行通过后，方可正式运行新系统，导入正式生产环境。

5.2.3 IT 系统保护

公司安装有企业版杀毒软件，IT 人员定期更新病毒库，并设置顾客端杀毒软件程序定期查收。规定各部门在接收外来文件时，必须先进行病毒检测、查杀，确认无毒后方可下载或接收。详见《病毒防范管理程序》（编号 ISMS-A-027），公司现在安装的杀毒软件为火绒杀毒软件及 360 杀毒软件。各用户端全部安装杀毒软件，并防止用户私自卸载或修改设置，并将杀毒软件的安装情况纳入每月综合检查项，定期检查。公司用天锐绿盾软件进行上网行为的监控和管理。

详见《网络安全管理程序》（编号 ISMS-A-017），目前，公司计算机大部分为内网，有连接外网需求的，需要单独申请批准。

5.2.4 事件日志记录与分析

编制《信息系统监控管理程序》（编号 ISMS-A-023），规定了事件日志的要求，并规定了事件日志的记录要求，并规定了管理员的权限，避免非法访问和修改。在每月的综合检查中，定期检查事件日志，如有违规行为或明显问题，启动处理流程。规定对高保护需求信息和非常高保护需求信息，都要记录其访问日志。

5.2.5 漏洞识别和解决

编制《信息系统应用管理程序》（编号 ISMS-A-022），规定了客户端、服务器、网络设备、安全设备、应用系统等技术漏洞管理要求。公司在公司的所有应用端安装 360 软件，通过服务器下载系统软件、应用软件及第三方软件的安全补丁，自动对应用端计算机进行漏洞管理。通过漏洞扫描工具获得系统存在的漏洞，通过软件、硬件供应商获得最新的安全补丁，对系统的安全配置进行检测，确认配置存在的风险，对存在的漏洞及风险进行评估，根据评估结果确定整改方案。对信息资产进行漏洞修补完成后，应进行业务测试以确保系统的正常运行。

5.2.6 IT 系统审计

《脆弱性管理程序》（编号 ISMS-A-028）规定了 IT 审核的要求。审核由 IT 审核小组每

年进行一次，确定审核要求和审核范围。审核结果以《信息安全事件报告》的方式向领导层和公司员工公示（必要时）。必要时公司委托第三方公司对公司进行渗透测试。

5.2.7 网络管理

公司内部根据管理需要建设内部局域网，满足内部信息资源方面的应用。规定了网络管理和控制的要求，并按照要求执行。公司现在根据车间和办公楼的划分，进行网络分段管理。通过交换机来实施网络分段，设置分段之间互连的权限。

通过网络行为系统，限制网络连接功能。各网络分段之间可以进行网络互连，但通过交换机设置，可以避免各分段之间的网络风险的传递。以上详见《网络安全管理程序》（编号 ISMS-A-017）。

5.3 系统采购、需求管理和开发

5.3.1 新系统及改进系统开发

公司编制《信息系统应用管理程序》（编号 ISMS-A-022）规定与 IT 系统设计和开发相关的信息安全要求，规定 IT 系统升级的信息安全要求。新系统或升级后的系统，要验证符合规范要求后，方可正式启用。在项目试运行时，原系统和新系统要双规运行，且试运行阶段测试系统不能直接对接生产环境正式系统，数据隔离，避免开发过程中的错误影响正式生产和公司运行。当试运行通过后，方可正式运行新系统，导入正式生产环境。

5.3.2 网络服务要求

《网络安全管理程序》（编号 ISMS-A-017）规定了网络服务的要求，并按照要求实施。公司在国际互联网接入中选择有国家许可资质、有能力的互联网服务商进行互联网接入，确保在互联网接入冗余，选择适合公司互联网使用的带宽服务。至少保证两个互联网服务商接入。现有的网络为移动和电信双运营商接入，且布线位置不同，确保一家运行商出现故障，不影响公司的网络通信。每个互联网服务商必须保证公司网络服务期限内通讯正常，签订网络级别服务协议，出现故障保证 24 小时内予以解决（电话支持、远程支持或现场服务）。上网流量流量通过软件进行监控并记录，并在综合检查中进行检查和分析。

5.3.3 外部 IT 服务退还和安全移除信息资产

《相关方信息安全管理程序》(编号 ISMS-A-011)规定须与供应商签订合同或保密协议，必须规定服务退出时服务商的配合义务，确保公司信息资产安全的全部移除或归还。当需要外部服务退出或变更时，由责任部门提出申请 IT 单位进行风险评估，评审变更或退出的信息安全风险，由总经理审批后执行。IT 单位负责登记并确认在外部 IT 服务提供方处的信息资产，确保安全的移除或归还全部信息资产后变更或终止双方合作协议。

5.3.4 外部 IT 服务共享

与 IT 供应商签订技术协议，规定 IT 服务提供期间服务提供商的责任，并规定在终止 IT 服务时，始终保护自己在外部 IT 服务中的信息，并防止其他组织访问这些信息。如需使用共享 IT 服务外发电子文档，需制作外发文件，要根据文档的安全性对外发文件的阅读口令进行设定，不得无约束制作，审核人要对外发的文件严格审核。详见《相关方信息安全管理程序》（编号 ISMS-A-011）

6 供应商管理

6.1.1 信息安全保障

所有的供应方必须与公司签订合同书或者 SLA，确保了适当级别的信息安全。只有供应商签字，才会加入公司的合格供应商清单，在签订保密协议后发放与业务相关的资料和信息。供应商和合作伙伴须接受信息安全方面的风险评估，供应商和合作伙伴需提供证据证明其信息安全水平足以满足信息保护需求。在适用的情况下，可将与客户签订的合同协议将转交给供应商和合作伙伴，供应商和合作伙伴也有义务将有关适当信息安全级别的任何要求传递给其分包商。相关人事部门应审查供应商和合作伙伴的服务报告和文件，验证服务是否符合合同协议。《相关方信息安全管理程序》

6.1.2 信息交换保密管理

保密协议为公司的信息提供法律保护，尤其是在组织边界之外交换信息的情况下。公司的管理层及业务部门应识别公司的信息资产，并确定信息的保密要求和保密程序。在转发敏感信息之前应与相应的组织或个人签订有效的保密协议。管理层应定期的审查适用保密协议和处理敏感信息的要求和程序。

为确保公司的各类保密协议可用，需定期检查保密协议模板适合法律法规要求。保密协议的模板应包含但不限于以下要求：相关人员或组织；协议涵盖信息的性质；协议的主题；协议的有效期（临时或永久）；债务人的责任；处理合同以外敏感信息的规定；

在保密协议中约定供应商及业务合作伙伴必须提供符合相关信息安全的合规性，还应保留合规性审计权，如独立第三方审查或第二方的审查。

相关部门应制定在临时保密协议有效期内的监测和适当时间开始延长的流程。公司对保密信息的保护要求保护期限至少为 2 年，合同期限结束的 5 年内保密业务仍然有效，对知识产权的保护不因合同的到期而失效。《相关方信息安全管理程序》

7 合规性

7.1.1 法规和合同条款

相关部门按照《信息安全合规性管理程序》（编号 ISMS-A-012）识别法律、监管和合同相关的要求。将识别的法律法、监管和合同在公司内重新定义实施和管理的策略，并将其传达给相应的负责人。

在公司信息安全管理体系运行过程中，要采取相应的措施实施并满足知识产权和使用受版权保护的软件产品的要求。相关部门要定期的对员工培训信息安全合规性为主题的相关要求的措施。在业务过程中需要保留符合合同、监管或法律义务以及业务要求的完整性记录。

7.1.2 个人信息保护

相关部门按照《信息安全合规性管理程序》（编号 ISMS-A-012）识别与个人信息相关的法律法规，根据最新的法律法规要求确定公司的对个人数据的保护措施。各部门根据公司获取的法律法规和其他要求融入本部门管理策略，确认相关岗位、职责及人员，确保措施落地实施。

人事部门是公司个人信息保护的主要负责部门，人事部门应负责制定与个人信息保护相关的管理流程和要求。人事部门应监督公司内部对于个人信息的获取、保存、使用和处理，人事部门应确保掌握和处理个人信息的人员应了解和遵守数据保护的法律和合同要求。

8 原型保护

8.1.1 周边安全

必须防止未经授权访问受保护对象。为此，必须保护环境（例如使用围栏/墙壁）。在不可行的情况下，必须使用合适的材料或设备（如格栅、安全玻璃）保护建筑物的外表面。

8.1.2 外墙的稳定性

建筑物的外壳必须由坚固的结构（如石头、混凝土、钢/其他金属）制成。不得使用商用工具拆卸或打开墙壁部件。

8.1.3 视线保护

在车辆或设计相关零部件加工或储存的所有区域，必须确保视野和视线保护。这包括建筑物的相关玻璃表面和防止通过打开的门/门/窗看到/看到的保护措施。

8.1.4 防止未经授权的访问和访问控制

必须为受保护的区域建立访问概念，规范和记录访问权的分配。这可以通过机械和电子门禁系统实现。

8.1.5 入侵报警系统

在安全的场所，应安装有效的入侵报警系统（例如，符合 DIN EN 50131 或符合 VDS 或类似标准）。

报警跟踪必须由经认证的安全服务/控制中心进行。入侵报警系统的另一种替代方案是由认证的安全服务机构提供全天候的保护。

必须制定并验证警报反应计划。

8.1.6 访客管理

所有访客都必须登记。此外，他们必须在访问之前同意保密协议。必须记录注册和保密协议。应为所有访客发布安全和访客条例。必须遵守有关数据保护的国家立法。

8.1.7 客户分离

不同客户的项目必须在物理上分开。这种分离可以通过移动设备（例如移动隔板或窗帘）实现。此外，不同项目之间应该可以分离。

8.2.1 保密义务

必须与客户签订书面保密协议/义务，该协议/义务在合同法方面有效。

8.2.2 分包商

分包商必须得到原客户的批准，还必须同意接受保密约束。必须提供分包商遵守安全规定的书面证据。

8.2.3 意识

必须定期（至少每年一次）让参与项目的员工和其他人员了解和/或接受信息安全培训，尤其是原型保护方面的培训。这些措施必须以书面形式记录。

8.2.4 安全分类

参与项目的每个人都必须了解项目的当前安全分类和由此产生的安全要求。

8.2.5 访问控制

必须实施并记录控制进入安全区域的流程，该流程定义了访问权的新分配、变更和撤销，以及丢失时的行为准则。

8.2.6 摄影及拍摄管理

必须实施并记录控制进入安全区域的流程，该流程定义了访问权的新分配、变更和撤销，以及丢失时的行为准则

8.2.7 具有视频和照片功能的移动设备

必须制定法规来管理具有视频和/或照片功能的移动设备，这些设备可能会被带到现场

并使用（例如，锁定/密封此类设备）。

8.3.1 运输

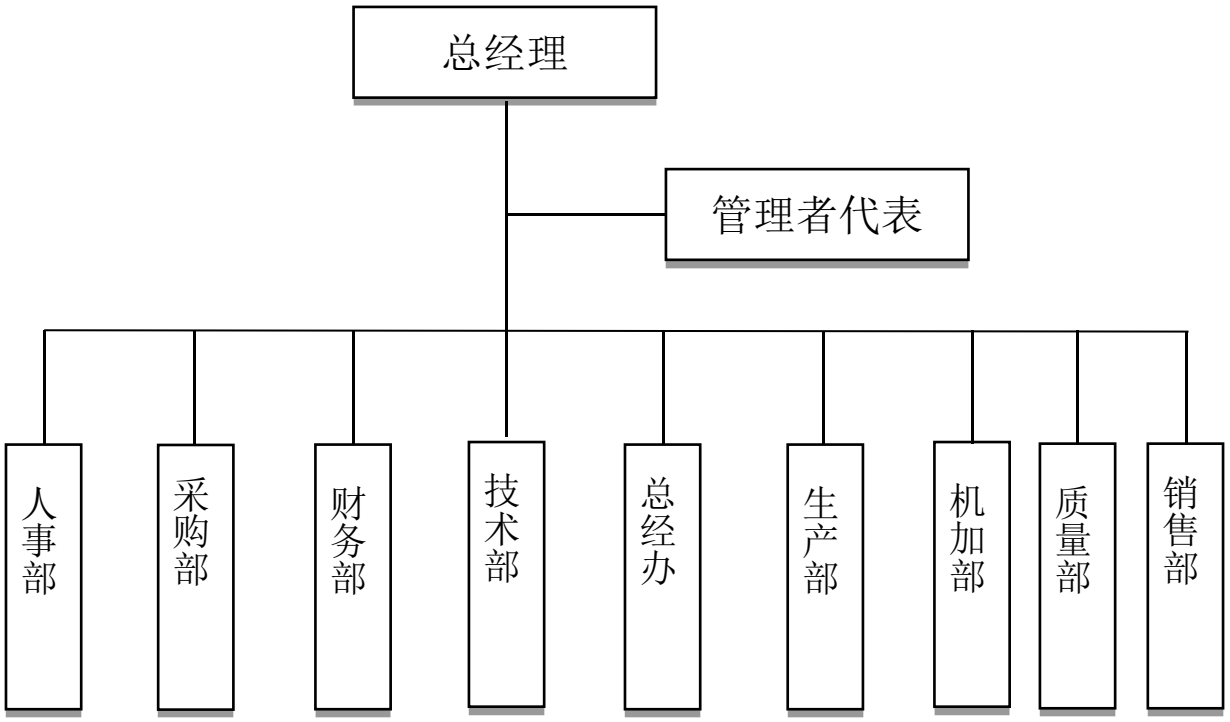
在运输过程中（通过空运、海运、公路运输），必须保护归类为需要保护的车辆、零部件，防止未经授权的查看、未经授权的图像记录和访问。描述并实施了向客户报告任何安全相关事件的流程。需要保护的运输必须按照客户的要求进行。

8.3.2 停车和储存

被归类为需要保护的车辆、部件和零件的停放和储存只能在经批准的场所，并在遵守客户进一步要求的情况下进行（如防水帆布）。

附录 1：×××有限公司组织架构图

ISMS 组织架构图

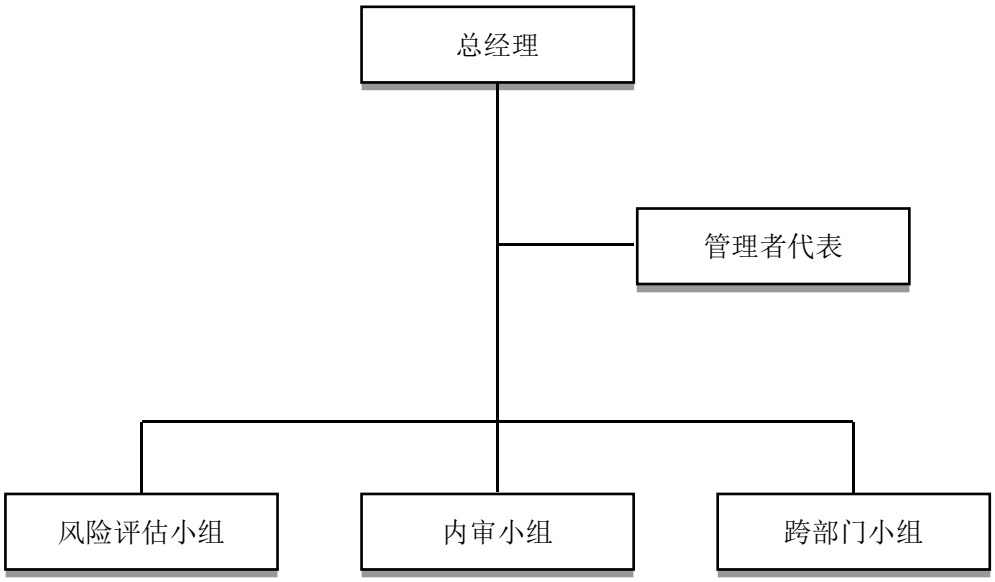


各部门的职责见本手册 1.2.2 条款，信息安全组织对各部门的职责描述。

编制/日期： 2022 年 10 月 12 日　　批准/日期： 2022 年 10 月 13 日

附录 2：信息安全管理实施架构图

为了避免利益冲突，实现职责分离。公司需要成立风险评估小组、内审小组等独立的信息安全组织。具体的职责分配如下；



序号	单位/部门	信息安全职责
1	总经理	公司 ISMS 第一负责人，负责本公司网络与信息安全重大事项的决策和协调，并对全公司信息安全工作负责。定期举行管理评审，评价 ISMS 体系运行的有效性，并为 ISMS 运行提供必要的资源。
2	管理者代表	详见本手册 0.2 条款管理者代表授权书；
3	风险评估小组	负责组织 ISMS 建立过程中的风险评估、风险处置；负责 ISMS 管理中信息安全目标、过程控制、持续改进的变更风险管理；
4	跨部门小组	负责残余 ISMS 的各项活动，如 ISMS 信息资产识别、风险评估、程序文件编制和评审，在各自岗位推动体系在企业内实施；
5	内审小组	负责组织按照 TISAX（VDA ISA）自评表进行定期自评，策划内审方案、组织实施内部审核、向管理层提交内审报告，并对问题进行闭环；

附录 3：信息安全管理体系目标

序号	目标项目	计算方法	统计频次	数据来源	负责部门
1	系统可用率	=（总服务时间-服务异常中断时间）/服务时间×100%	月	服务器故障记录	人事部
2	加密安全软件覆盖率	=安装加密软件计算机数量/计算机数量×100%	季	计算机台账、 加密软件安装明细；	人事部
3	数据异地灾备率	=异地灾备系统数/信息化系统数量×100%	季	异地备份记录；	人事部
4	应急预案演练参与率	=实际参加人员数/应参加人员数×100%	年	应急演练记录；	人事部
5	重要信息泄密次数	=实际重要泄密次数；	季	年度重要泄密次数统计；	人事部
6	信息安全意识培训完成率	=实际培训次数/计划培训次数×100%	半年	信息安全培训计划、培训记录	人事部
7	招聘计划达成率	=实际到岗人数/计划招聘人数×100%	季	员工确认单	人事部
8	保密协议覆盖率	=签订保密协议的人数/公司总人数×100%	季	签订的保密协议、花名册	人事部

附录 4：信息安全管理体系文件清单

序号	文件名称	程序文件编号	版本
001	文件管理程序	ISMS-A-001	V1.0
002	记录管理程序	ISMS-A-002	V1.0
003	信息安全风险管理程序	ISMS-A-003	V1.0
004	内部审核管理程序	ISMS-A-004	V1.0
005	纠正与预防措施管理程序	ISMS-A-005	V1.0
006	管理评审控制程序	ISMS-A-006	V1.0
007	监视和测量管理程序	ISMS-A-007	V1.0
008	商业秘密管理程序	ISMS-A-008	V1.0
009	人事管理程序	ISMS-A-009	V1.0
010	信息安全惩戒管理程序	ISMS-A-010	V1.0
011	相关方信息安全管理程序	ISMS-A-011	V1.0
012	信息安全合规性管理程序	ISMS-A-012	V1.0
013	信息安全内部组织管理程序	ISMS-A-013	V1.0
014	信息安全事件管理程序	ISMS-A-014	V1.0
015	移动设备管理程序	ISMS-A-015	V1.0
016	安全区域管理程序	ISMS-A-016	V1.0
017	网络安全管理程序	ISMS-A-017	V1.0
018	数据安全管理程序	ISMS-A-018	V1.0
019	信息处理设施管理程序	ISMS-A-019	V1.0
020	个人计算机管理程序	ISMS-A-020	V1.0
021	用户访问管理程序	ISMS-A-021	V1.0
022	信息系统应用管理程序	ISMS-A-022	V1.0
023	信息系统监控管理程序	ISMS-A-023	V1.0
024	信息交换管理程序	ISMS-A-024	V1.0
025	软件管理程序	ISMS-A-025	V1.0
026	介质管理程序	ISMS-A-026	V1.0
027	病毒防范管理程序	ISMS-A-027	V1.0
028	技术薄弱点管理程序	ISMS-A-028	V1.0
029	信息业务连续性管理程序	ISMS-A-029	V1.0
030	电子邮件管理程序	ISMS-A-030	V1.0
031	项目管理控制程序	ISMS-A-031	V1.0
032	变更管理程序	ISMS-A-032	V1.0
033	远程工作的策略	ISMS-C-2023	V1.0
034	个人信息管理策略	ISMS-C-2023	V1.0

附录 5：DA ISA 适用性声明（VDA ISA5.1）

标准条款	控制问题	控制目标	是否选择	选择理由	控制描述	控制文件
1.1.1	多大程上的信息安全策略可用？	控制	是	信息安全体系规定和公司实际需求	公司管理层策划信息安全管理策略；	信息安全管理手册
1.2.1	组织内部对信息安全的管理程度如何？	控制	是	信息安全体系规定和公司实际需求	管理层项柱子组织内部推行信息安全管理体系；	信息安全管理手册
1.2.2	信息安全职责分配的程度如何？	控制	是	信息安全体系规定和公司实际需求	最高管理层负责向下分配信息安全管理职责和权限；	信息安全管理手册
1.2.3	项目在多大程度上考虑了信息安全要求？	控制	是	信息安全体系规定和公司实际需求	公司的任何项目中，增加信息安全的要求和信息安全的目标；	信息安全风险管理程序
1.2.4	在多大程度上定义了外部 IT 服务提供商和自身组织之间的责任？	控制	是	信息安全体系规定和公司实际需求	与外部 IT 服务提供商之间签订合同，明确各自的职责；	相关方信息安全管理程序
1.3.1	信息资产的识别和记录程度如何？	控制	是	信息安全体系规定和公司实际需求	识别组织的信息资产清单，对信息资产进行标识。	信息安全风险管理程序
1.3.2	根据保护需求，信息资产的分类和管理程度如何？	控制	是	信息安全体系规定和公司实际需求	将信息资产分为主要资产和支持资产，对主要资产分配各自的支持资产；	信息安全风险管理程序
1.3.3	在何种程度上确保只有经过评估和批准的外部 IT 服务用于处理组织的信息资产？	控制	是	信息安全体系规定和公司实际需求	对于的外部的IT服务经过申请、审核、批准后在内部使用。在使用功能过程中监控服务质量。	相关方信息安全管理程序
1.4.1	信息安全风险的管理程度如何？	控制	是	信息安全体系规定和公司实际需求	将组织识别的信息资产分析潜在的风险，威胁和脆弱性的方面分析风险，确定控制措施。	信息安全风险管理程序
1.5.1	在多大程度上确保了程序和流程对信息安全的遵守？	控制	是	信息安全体系规定和公司实际需求	定期对信息安全体系运行的有效性进行评价，发现不符合及时纠正。	内部审核管理程序
1.5.2	ISMS 在多大程度上由独立实体审查？	控制	是	信息安全体系规定和公司实际需求	在组织内部展开的独立的审核组织，组织内部定期的开展 ISMS 审计；	内部审核管理程序
1.6.1	信息安全事件的处理程度如何？	控制	是	信息安全体系规定和公司实际需求	制定信息安全事件的处理流程，对于突发的信息安全事件采取相应的措施。	信息安全事件管理程序
2.1.1	在多大程度上确保敏感工作领域的合适员工？	控制	是	信息安全体系规定和公司实际需求	确定公司的敏感工作领域，识别敏感区域工作的岗位，确定管理措施。	安全区域管理程序
2.1.2	在多大程度上，所有员工都必须遵守信息安全政	控制	是	信息安全体系规定和公司实际需求	新员工入职时培训信息安全要求、操作安全、网络安全等。培训公司的信息安全方针、信息	人事管理程序

标准条款	控制问题	控制目标	是否选择	选择理由	控制描述	控制文件
	策？				安全目标；	
2.1.3	员工在多大程度上了解和培训了信息处理带来的风险？	控制	是	信息安全体系规定和公司实际需求	每年给员工培训信息安全意识，当员工有泄密事件时，按照相关制度进行处理和教育。	人事管理程序
2.1.4	远程工作在多大程度上受到监管？	控制	是	信息安全体系规定和公司实际需求	制定远程工作管理策略，对员工培训远程工作的信息安全意识	远程工作策略
3.1.1	在多大程度上管理了保护信息资产的安全区域	控制	是	信息安全体系规定和公司实际需求	确定公司的安全区域，确定安全区域的访问控制策略；	安全区域管理程序
3.1.2	在特殊情况下，信息安全的保障程度如何	控制	是	信息安全体系规定和公司实际需求	制定信息业务连续性管理程序，每年开展信息安全保障的演练；	信息业务连续性管理程序
3.1.3	支持资产的处理在多大程度上得到了管理	控制	是	信息安全体系规定和公司实际需求	识别公司的支持资产，对于支持资产的风险进行评价，制定控制措施。	信息处理设施管理程序
3.1.4	移动IT设备和移动数据存储设备的管理程度如何	控制	是	信息安全体系规定和公司实际需求	识别公司的移动设备，编制移动设备管理程序，对于公司的移动设备按照移动设备管理程序管理。	移动设备管理程序
4.1.1	身份识别手段的使用在多大程度上得到管理	控制	是	信息安全体系规定和公司实际需求	管理公司的身份信息，每个人有自己唯一的身份信息。不允许泄露给其他人。	用户访问管理程序
4.1.2	用户访问网络服务、IT系统和IT应用程序的安全程度如何	控制	是	信息安全体系规定和公司实际需求	制定用户访问管理程序，对于网络服务、IT系统和IT应用程序的权限进行授权，定期的审查访问权限。	用户访问管理程序
4.1.3	用户帐户和登录信息的安全管理和应用程度如何	控制	是	信息安全体系规定和公司实际需求	对IT系统用户账户进行审查，定期的已经离职或者转岗的人员权限进行审查。	用户访问管理程序
4.2.1	访问权限的分配和管理程度如何	控制	是	信息安全体系规定和公司实际需求	公司的访问分为物理访问和系统访问，对系统访问和物理访问策划授权的流程。	用户访问管理程序
5.1.1	在多大程度上使用了受管理的加密过程？	控制	是	信息安全体系规定和公司实际需求	公司安全区域的电脑都设置可密码。安全区域的访问均使用门禁。所有的终端都需加密。	口令控制策略
5.1.2	在传输过程中，信息的保护程度如何？	控制	是	信息安全体系规定和公司实际需求	公司的重要信息在传输是进行加密。	信息交换管理程序
5.2.1	变更管理到什么程度？	控制	是	信息安全体系规定和公司实际需求	编制信息系统应用管理程序，公司所有的信息安全变更按照程序管控。	信息系统应用管理程序
5.2.2	开发和测试环境与操作环境的分离程度如何？	控制	是	信息安全体系规定和公司实际需求	在公司信息技术机房配备一个测试用机，在新系统上线前在测试机上进行测试。	信息系统应用管理程序
5.2.3	在多大程度上保护IT系统不受到恶意软件？	控制	是	信息安全体系规定和公司实际需求	编制病毒防范管理程序，IT管理人员定期的对IT系统的进行杀毒，更新病毒库。	病毒防范管理程序
5.2.4	在多大程度上记录和分析了事件	控制	是	信息安全体系规定和公司实	每季度对服务器的访问情况进行审查，查看系统日志，分析信	信息安全监控策略

标准条款	控制问题	控制目标	是否选择	选择理由	控制描述	控制文件
	日志？			际需求	息安全事件。	
5.2.5	在多大程度上识别和解决了漏洞？	控制	是	信息安全体系规定和公司实际需求	IT 管理人员扫描系统漏洞，解决系统漏铜。	监视和测量管理程序
5.2.6	IT 系统在多大程度上进行了技术检查？	控制	是	信息安全体系规定和公司实际需求	寻找资源，定期对 IT 系统进行审查。	监视和测量管理程序
5.2.7	组织网络的管理程度如何？	控制	是	信息安全体系规定和公司实际需求	制定网络安全管理程序，按照程序监控网络的行为。	网络安全管理程序
5.3.1	IT 系统的新开发或进一步开发在多大程度上考虑了信息安全？	控制	是	信息安全体系规定和公司实际需求	在 IT 系统的开发过程中，审查开发服务方的信息安全输入要求。	信息系统应用管理程序
5.3.2	对网络服务的要求定义到什么程度？	控制	是	信息安全体系规定和公司实际需求	与网络服务商签订协议，监控网络服务的质量。	相关方信息安全管理程序
5.3.3	外部 IT 服务中信息资产的返还和安全移除在多大程度上受到监管？	控制	是	信息安全体系规定和公司实际需求	与供应商签订保密协议，在外部 IT 服务终止前将信息资产返还。	相关方信息安全管理程序
5.3.4	在多大程度上保护了共享的外部 IT 服务的信息？	控制	是	信息安全体系规定和公司实际需求	与供应商签订保密协议，了解和要求共享的外部 IT 服务的信息保护。	相关方信息安全管理程序
6.1.1	供应商和合作伙伴之间的信息安全保障程度如何？	控制	是	信息安全体系规定和公司实际需求	与供应商签订保密协议，监督和审查供应商保密的执行情况。	相关方信息安全管理程序
6.1.2	合同约定的信息交流保密程度如何？	控制	是	信息安全体系规定和公司实际需求	与供应商签订保密协议，按照保密协议的要求进行数据传输。	相关方信息安全管理程序
7.1.1	在多大程度上确保遵守监管和合同规定？	控制	是	信息安全体系规定和公司实际需求	制定合规性管理程序，每年对公司的法规、顾客要求、记录保存等合规性进行审查。	信息安全合规性管理程序
7.1.2	在实施信息安全时，在多大程度上考虑了对个人数据的保护？	控制	是	信息安全体系规定和公司实际需求	制定人信息保护要求，定期的审查合规性。	信息安全合规性管理程序
8.1	物理和环境安全；	保护	是	公司有原型产品的生产车间，客户对原型零部件有保护要求；	原型件研发阶段，将原型车间特殊管控。车间周边及环境部署信息安全的设施，实施相应的信息安全管理；	原型样件保护规程
8.2	组织要求；	保护	是	公司有原型产品的生产车间，对原型车间的工作人员应有信息安全的要求；	识别原型区域的管理要求及工作岗位，对相关人员分配职责，对人员进行管理和培训；监控相关人员的工作行为；	原型样件保护规程

标准条款	控制问题	控制目标	是否选择	选择理由	控制描述	控制文件
8.3	车辆、部件及部件的搬运；	保护	是	公司生产的原型零部件需要供应给客户，运输安全需要保护；	选用客户同意的运输供应商，对运输车辆及运输过程进行控制；	原型样件保护规程
8.4	对试验车辆的要求；	保护	否	N/A	无	无
8.5	对活动和枪拍摄的要求；	保护	否	N/A	无	无