ISO27001:2022 信息安全管理体系认证准备资料清单		
1、人力资源安全		
序号	**名称**	**备注**
1	花名册	全体员工
2	人事资料	全体员工
3	保密协议	全体员工
4	人员访问权限清单	权限包括:可使用的网络、可使用的软件、可使用的系统可使用系统的权限、可进入的物理区域、可访问的信息文件、电脑账户名称(ID)
5	离职资料	离职交接，最近半年
6	涉密人员及涉密事项清单	要注明涉密事项，及使用电脑编号及 ID
7	涉密人员任职条件要求及权利义务	
8	涉密员工背景调查及证书	背量调查包括:员工履历核查、学术及专业资质核查、个人身份核查、信用核查、犯罪核查。
9	信息安全培训计划	
10	信息安全培训记录信息安全违规处罚记录	
11	离职资料	暂无
2、资产管理		
序号	**名称**	**备注**
1	信息资产清单	1、信息资产包括:电脑、路由器、打印机、复印机、传真机、电话、机房中的设施、移动硬盘(U 盘)2.所有信息资产必须编号，写明负责人(IT)及使用人员 3.要列明信息资产中所存放的信息是什么，如:合同、技术资料、安装的软件、安装的系统等。4.要列明信息资产的用途是什么，如:办公用、软件开发用等。 5.信息资产必须必须张贴信息资产标签，标签上要写明: 信息资产编号、负责人(IT)、使用人。
2	业变信息资产清单	存放重要信息或涉密信息的信息资产重愿信息资产清单中的项目内容上。重要信息资产必须在限值区域(保密区域)使用，所配套的打印机、复印机、传真机应为专用
3	笔记本电脑成可以用办公目设备/介质。如:移动硬盘(0 盘)、文件	1.信息资产中不要有笔记本电脑，因信息安全不提倡远程或移动办公。 2.移动硬盘(U 盘)必须为公司所有，在使用时必须经过同意，并登记:不得使用私人移动硬盘(U 盘)只有指定的几台电脑有 USB 接口，其他电脑中的 USB 接 3.]必须为堵死或未安装状态，使用移动硬盘(U 盘)只能在指定的这几台电脑上使用。
4	信息传递记录	信息在传递时要有收发记录，并注明:1.用途 2.并注明临时性拷贝还是永久性拷贝 3.要有拷贝后的处理措施 4.要有处理人签字 5.要有人审批 6.要注明日期和时间。
5	介质处置记豉	粉碎报废
6	信息资产移动记录	若发生
7	信息资产处置记录	报废、废止等

8	信息分类及信息标记	1.信息分类的重要度一般分为 5 类:国家秘密事项、企业秘密事项、敏感信息事项、一般事项和公开事项。(企业可自主制定)2.要在可传递的信息上标记信息分类。可传递的信息包括:打印出来的纸质内容，U 盘内容或其他信息。3.信息管理要求:国家秘密事项、企业秘密事项、敏感信息事项、一般事项和公开事项是怎么管理的要求，如:接触人员要求、传递管理要求、拷贝要求等。
3、访问控制		
序号	**名称**	**备注**
1	网络拓扑图	公共环境、研发环境、测试环境及运行环境网络环境要分开
2	各区域密码配置一览表	要显示:设备名称(无线 AP)、密码安全选项(WPA2-个人)、选择的密码(AES)及理由(可兼容更多的笔记本电脑网卡，安全性比较高)
3	人员访问权限清单	权限包括:可使用的网络、可使用的软件、可使用的系统可使用系统的权限、可进入的物理区域、可访问的信息文件、电脑账户名称(ID)
4	系统账号及权限审批表	新进员工个人 ID 及访问权限需要审批
5	系统账号及权限调整审批表	离职员工权限撤销或权限调整人员需要审批
6	系统权限复查记录	每半年检查一次
7	用户访问日志	登录了哪台电脑、使用了哪些软件、传递了哪些文件、有哪些聊天信息等
8	非法/暴力访问记录	输入密码错误的记录、输入三次密码错误后锁机，并通知 IT、尝试解锁暴力访问记录
9	源代码访问授权人员清单	包括:姓名、职位、ID 及权限
10	源代码访问记录	1.若源代码存在云端，则可以自动生产访问、修改、删除记录。
	用户访问复查记录	2.在运行系统中不得保留源代码。检查记录，防止有人越权访问
11	密码变更记录	检查记录，防止有人越权访问
12	网络拓扑图	每三十天变更一次
4、物理和环境安全		
序号	**名称**	**备注**
1	公司平面图	权限包括:可使用的网络、可使用的软件、可使用的系统、可使用系统的权限、可进入的物理区域、可访问的信息 1 文件、电脑账户名称(ID)
2	布缆图	
3	人员访问权限清单	
4	限制区域进出记录	需要包含进入原因及携带物品，需有陪同人、出门检查及审批。
5	屏幕保护和清理桌面	1.电脑屏幕应在不适用 30 秒内锁屏。 12.电脑桌面上不得存放涉密信息。
5、操作安全		
序号	**名称**	**别称**
1	文件服务器磁盘空间使用率监控表	要满足冗余要求
2	杀毒软件清单	至少两种杀毒软件，要注明杀毒软件更新时间
3	病毒查杀记录	每月至少一次
4	病毒攻击及防范记录	每月至少一次
5	信息安全事件处理记录	当发生违规操作或病毒攻击时的处理记录
6	信息备份策略	
7	信息备份记录	
8	时钟同步	所有电脑上的时间必须为一致的

		电脑上只允许安装办公软件，不得安装 QQ/微信、游戏等其
9	限制软件安装	他软件，信息传输必须使用指定软件传输，并列入信息资
		产清单
6、通讯安全		
序号	**名称**	**备注**
1	网络安全管理	限制内网接入、使用正规外网、使用正规邮箱服务商
7、系统获取开发和维护		
序号	**名称**	**备注**
1	正版编程软件的使用并定期更新	
2	计算机软件开发记录	
3	计算机软件验收记录	
8、供应商关系		
序号	**名称**	**备注**
1	合格供应商清单	包括:云服务供应商、网络供应商、IT 硬件设备供应商等
2	供应商评估记录	
9、信息安全事件管理		
序号	**名称**	**备注**
1	信息安全事件处理记录	当发生违规操作或病毒攻击时的处理记录