ISO27001信息安全管理体系 内审检查表

被审核部门	管理层	审核成员：****	陪同人员：****	审核日期	2021 年 3 月 10 日
审核主题	4.1、4.2、4.3、4.4、5.1、5.2、5.3、6.1、6.2、7.1、9.3、10.1、10.2、A.5.1 、A.6.1 、A.12.2				

检查要素/条款	检查事项	检查记录	符合项	观察项	不符合项
4.1 4.2 4.3 4.4	组织环境	-总经理详细介绍了公司总体情况，包括公司建立的理念，愿景，描述了客户、政府机关、相关协会、团体、法律法规等相关方对公司的期望与要求。具体见信息安全管理手册企业概况。 -总经理明确了公司信息安全管理体系覆盖的物理范围与业务范围。物理范围为：深圳市**********，业务范围为：计算机应用软件的研发及运行维护。	√		
5.1 5.2	领导和承诺 方针	--信息安全方针，信息安全目标和计划得以实施； 信息安全的角色和职责均已明确； 向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性； 提供充分的资源，以建立、实施、运作、监视、评审、保持并改进，决定接受风险的准则和风险的可接受等级；	√		

被审核部门	管理层	审核成员：****	陪同人员：****	审核日期	2021 年 3 月 10 日
审核主题	4.1、4.2、4.3、4.4、5.1、5.2、5.3、6.1、6.2、7.1、9.3、10.1、10.2、A.5.1 、A.6.1 、A.12.2				

检查要素/条款	检查事项	检查记录	符合项	观察项	不符合项
5.3	组织角色、职责和权限	建立信息安全的角色和职责 ——提供《信息安全管理手册》 总经理定义与分配了公司各个部门的不同岗位人员的日常职责与在各管理体系中负担的职责，职责划分基本能够满足要求。 总经理有向组织传达满足信息安全目标、符合信息安全方针、履行法律法责任和持续改进的重要性。	√		
7．1	资源的提供	——主持管理评审，授权管理者代表组织协调建立、实施、运作、监视、评审、保持和改进 ISMS体系。 ——总经理为管理体系顺畅进行提供资源支持，包括设备相应的增加计划，人员增加计划，财务支出支出、培训支持等等。	√		
9.3	ISMS管理评审	——本次是制定体系实施以来的第一次管理评审计划。	√		
A5.1	信息安全方针文件	信息安全方针包含在信息安全管理手册中，由总经理批准、发布并传递给所有相关方。	√		

ISO27001信息安全管理体系 内审检查表

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查要素/条款	核查事项	核查记录	符合项	观察项	不符合项
6.1 8.1 8.2	应对风险和机会的措施 运行的规划和控制 信息安全风险评估	前期策略了风险评估准则、风险评估规范 根据风险评估方法进行了风险评估。	√		
6.2 8.3	信息安全目标和规划实现 信息安全风险处置	制定了信息安全目标：确保每年重大信息安全事件（事故）发生次数为零。 目标通过一年来的运行和保持，得到完成。 信息安全不可接受风险处理计划， 提供“不可接受风险处理检查表”	√		
7.2 7.3 7.4	能力 意识 沟通	人力行政部通过制定培训计划、招聘新员工、聘请外部专家指导等方式确保组织人员有胜任信息安全职责的能力。 人力行政部通过培训、会议、标语宣贯等方式培养员工的信息安全意识。 人力行政部负责与组织内外部各相关方的沟通，沟通方包括客户、政府机关、内部员工等，沟通方式包括公函、会议、电子邮件、电话等等。	√		

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查要素/条款	核查事项	核查记录	符合项	观察项	不符合项
7.5	文件记录信息	公司编制管理手册、SOA适用性声明 1 套，35 个程序文件，信息安全记录 96 个； a) 明确了方针和目标 b) 管理手册、适用性声明； c) 形成 35 个程序 d) 信息安全管理体系运行所必须的程序文件 e) 所需提供的记录 96 个，包括《信息安全风险评估报告》、《信息安全风险处置计划》 f) 目前《适用性声明》	√		
9.2	内部审核	内审情况：2018 年 7 月 12 日实施了内审检查活动，相关的记录完整。	√		
A.6.1.1	信息安全的角色和职责	人力行政部： （1）负责管理体系的建立、实施、保持、测量和改进。 （2）负责文件控制、记录控制、内部审核的组织、管理评审的组织实施和体系的改进。 （3）负责本公司保密工作的管理。 （4）负责安全区域的保卫管理部门，负责安全区域的管理。 （5）负责部门的资产登记及评价、风险评估。	√		

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查要素/条款	核查事项	核查记录	符合项	观察项	不符合项
		（6）负责涉密信息上网、涉密计算机运行、检修、报废的监督管理。 （7）对信息安全日常工作实施动态考核，将信息安全管理作为企业管理的重要工作内容。 （8）负责协调各部门的定岗定编工作；提出相关岗位人员配置的建议。 （9）制定员工培训与开发计划，建立培训与开发体系包括人员聘用管理、任职培训、保密协议签署、员工的能力、专业技能培训、学历教育培训、综合素质培训等，并制订相应管理制度。 （10）建立和完善薪酬体系；制订员工福利政策；员工绩效管理 ；协助行政管理部制订员工绩效管理的相关制度，并组织实施。 （11）负责员工各项保险和住房公积金帐户的申报和管理；负责员工考勤、休假管理。 （12）负责员工劳动合同管理、员工离职管理、员工人事档案管理。 （13）本部门人员必须遵守公司信息安全的相关规定以及本岗位相关的保密要求。			
A.6.1.2	信息安全职责的分配	《信息安全管理手册》，公司在信息安全管理职责明细表里明确了信息安全职责。 公司设立信息安全管理者代表，全面负责 ISMS的建立、实施与保持工作。	√		

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查要素/条款	核查事项	核查记录	符合项	观察项	不符合项
A7.1.1 A7.1.2 A7.2.1 A7.2.2 A7.2.3 A7.3.1	审查 任用条款和条件 管理职责 信息安全教育和培训 纪律处理过程 任用终止或变更职责	人力行政部负责初始录用员工进行能力、信用考察，每年对关键信息安全岗位进行年度考察，对于不符合安全要求的不得录用或进行岗位调整。 在《劳动合同》中明确规定了保密的义务及违约的责任。 10 月份开展了信息安全相关的培训，查看《培训签到表》 具备《信息安全奖惩制度》，并按制度执行。 具备《人力资源管理程序》，并按制度执行。	√		
A.8.1.1 A.8.1.2 A.8.1.3 A.8.1.4	资产清单 资产所有权 资产的可接受使用 资产的归还	公司对资产进行了评估。包括软件/系统、数据/文档、硬件/设施及人力资源。 对每一项信息资产，根据《信息安全风险管理程序》识别出了重要资产及高风险的项目。其中高风险的资产有公司软件源代码等。自此之后公司完成了风险处理计划、检查、残余风险评估报告，以及验证。 有《重要信息资产清单》，信息资产包括数据、软件、硬件、服务、文档、人员、经验。 ——《信息资产清单》、《重要信息资产清单》都定义了责任部门或责任人 ——提供了资产归还的记录表。	√		
A.8.3.1 A.8.3.2 A.8.3.3	可移动介质的管理 介质的处置 物理介质传输	提供可移动介质授权使用清单 1 份。 ——有申请部门、申请人、部门审核人、申请介质类型、申请使用数量、申请使用时间、行政审核人、行政批示、经办人。	√		

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日	
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18					
核查要素/条款	核查事项	核查记录		符合项	观察项	不符合项
		——目前无介质处置。				
A.9.1.1 A.9.1.2	访问控制策略 网络和网络服务的访问	网络划分为三个网段，内网使用固定IP，入网需要申请，并绑定MAC地址。 现场查《网络安全配置表》符合要求。 提供了《开通外网申请表》符合		√		
A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6	用户注册及注销 用户访问开通 特殊访问权限管理 用户秘密鉴别信息管理 用户访问权限的复查 撤销或调整访问权限	对于任何权限的改变(包括权限的创建、变更以及注销，须由管理员操作。 提供金蝶K3系统用户列表1 份。 特权分配仅以它们的功能角色的最低要求为据，有些特权在完成特定的任务后应被收回，确保特权拥有者的特权是工作需要的且不存在富裕的特权。 各系统管理员应对被授权访问该系统的用户口令予以分配、规定不使用简单口令，口令必须至少要含有 6 位以上字母+数字。 查：普通用户只能访问被授权的服务，对计算机系统的访问权都被限制。		√		
A.9.3.1	使用秘密鉴别信息	公司范围的计算机登录口令要求 6 位以上。抽查了 4 台 PC机，口令符合要求		√		
A.9.4.1 A.9.4.2 A.9.4.3	信息访问控制 安全登录规程 口令管理系统	——用户不得访问或尝试访问未经授权的网络、系统、文件和服务。 ——现场测试，审核员通过访问网络上的 PC机，有用户名，密码，试图随意输入密码 3 次，均无法登陆。		√		

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日		
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18						
核查要素/条款	核查事项	核查记录			符合项	观察项	不符合项
A.9.4.4 A.9.4.5	特殊权限实用工具软件的使用 对程序源代码的访问控制	——所有计算机用户在使用口令时应遵循以下原则：所有活动帐号都必须有口令保护，所有系统初始默认口令必须更改等。 ——没有安装实用工具。 ——公司没有软件开发，只有网站服务采用托管形式，由第三方公司负责运营。 ——提供《网站维护协议》，合同有效日期从 2014 年 4 月 30 日至 2015 年 4 月 29 日，条款一，规定服务方所应承担的业务与遵守的规定；条款五，规定了双方的法律责任与处理办法					
A.10.1.1 A.10.1.2	使用密码控制的策略 密钥管理	公司的密码控制是由银行提供的加密机。 由银行专员到公司内导入密钥。			√		
A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6	物理安全周边 物理入口控制 办公室、房间和设施的安全保护 外部环境威胁的安全防护 在安全区域工作 交接区安全	——现场查公司大门设有接待处 ——现场查《外来人员来访登记表》，登记信息包含：来访人员姓名，时间，单位，身份证，事由，被访人			√		

被审核部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查要素/条款	核查事项	核查记录	符合项	观察项	不符合项
A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8 A.11.2.9	设备安置和保护 支持性设施 布缆安全 设备维护 资产的移动 组织场外设备和资产的安全 设备的安全处置或在利用 无人值守的用户设备 清空桌面和屏幕策略	——公司机房外包给第三方进行管理。 ——提供服务器每周检查记录。 ——现场查公司目前没有组织场所外的信息处理设备使用。 ——含有敏感信息的设备在报废或该做他用时，由使用部门应利用安全的处置方法将设备中存储的敏感信息清除并保存清除记录。对旧机器的硬盘砸坏，物理破坏后。公司目前未发生设备处置。 ——提供电子设备领用签字单。有申请人、 主管签字和日期。 ——桌面均能保持干净	√		
A.12.1.1 A.12.1.2 A.12.1.2 A.12.1.4	文件化的操作规程 变更管理 容量管理 开发、测试和运行环境分离	——程序文件34 个 ——现场了解目前没有信息系统的变更。 ——提供服务器容量监控记录。有服务器、硬件配置、总容量、已用空间、剩余空间。每日通过手工登录，通过服务器阵列备份通用备份，按照容量管理程序文件记录 。 ——现场查公司目前无软件开发和测试活动，目前使用的信息系统由供应商负责安装测试，	√		

部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查 要素/条款	核查事项	核查记录	符合项	观察项	不符合项
A.12.2.1	控制恶意软件	——使用 360 杀毒软件、金山杀毒软件。 ——资产编号 00007 刘*，00015 李**，00001 陈* 台式机，使用 360 杀毒，360 卫士。	√		
A.12.3.1	信息备份	——没有对综合管理部将设计开发资料进行数据备份			√
A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4	事态记录 日志信息的保护 管理员和操作员日志 时钟同步	——现场查公司通过门卫进行进出登记记录，保安 7*24 小时值班，进入办公大楼有前台，前台负责公司职员的考勤，现场查有打卡机，同时负责外来人员监控。 ——现场查只有系统管理员有权察看日志，服务器均开启管理员和操作员日志。 ——现场查公司的电脑设置为与 Internet 时间自动校对，未连接网络的电脑定期校对电脑时间。	√		
A.12.5.1	在运行系统上安装软件	——对软件在作业系统的执行进行严格控制，在新软件安装或软件升级之前，应经主管部门负责人审核同意后方可进行。计算机终端用户除非授权，否则严禁私自安装任何软件。现场查目前安装软件统一管理安装。	√		
A.12.6.1 A.12.6.2	技术脆弱性的控制 限制软件安装	计算机安装了 360 安全卫士，自动扫描系统漏洞，抽查公司人员电脑安全状况，人力行政部申意的电脑未存在高危漏洞未分析处置和及时修补。 ——系统应用程序的使用进行限制和严格控制，并规定授权的使用者等，只有经过授权的系统管理员才可以使用实用工具，现场查服务器上没有安装实用工具。	√		

部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日		
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18						
核查 要素/条款	核查事项	核查记录			符合项	观察项	不符合项
A.12.7.1	信息系统审计控制措施	——漏洞扫描工具使用JP1，只有信息系统课系统管理员有权限使用。 ——内部使用360 杀毒软件对个人计算机进行病毒查杀			√		
A.13.1.1 A.13.1.2 A.13.1.3	网络控制 网络服务安全 网络隔离	——提供《网络拓扑图》，描述网络结构并表示网络的各组成部分之间在逻辑上和物理上的相互连接。公司内部的计算机，只有授权的可以上外网，其他的都不能访问外网，现场查连网情况未发现异常。 ——公司路由器放置于机房内，目前划分为 3 个网段。 ——为确保公司网络安全，采用逻辑方式进行外部网络隔离，内网与外网物理隔离。现场查财务部内电脑没有连接网络。			√		
A.13.2.1 A.13.2.2 A.13.2.3 A.13.2.4	信息传递策略和规程 信息传递协议 电子消息发送 保密性或不泄露协议	对信息交流应作适当的防范，严禁在无保密措施的通信设备及计算机网络中传递企业秘密。 ——客户通过企业邮箱 Email，通过内部腾讯通。 ——现场查公司的电子邮件目前只用于公司内部信息交换、对外发送公开的报价单。内部通过腾讯通进行交换文件。			√		
A.15.1.1 A.15.1.2	供应商关系的信息安全策略 处理供应商协议的安	——与供应商签订年度协议,有安全保密协议,有双方负责人签字,合同专用章,			√		

部门	综合管理部	审核成员：*****	陪同人员：*****	审核日期	2021 年 3 月 10 日
审核主题	6.1、7.2、7.3、7.4、7.5、8.1、8.2、8.3、9.1、9.2、A.6.1.1 、A.6.1.2 、A.7、A.8、A.9、A.11、A.12、A.13、A.15.A.16 、A.17、A.18				

核查 要素/条款	核查事项	核查记录	符合项	观察项	不符合项
A.15.1.3	全问题 信息和通信技术供应链				
A.15.2.1 A.15.2.2	供应商服务的监视和评审 供应商服务的变更管理	——提供第三方评审记录表。 ——查《采购合同书》规定了对于服务方所提供服务的要求细则重要事项条款：规定了对于服务方违约的处理办法符合。第三方服务的更改，包括更改和加强网络，使用新技术，更改服务设施的物理位置，更改供应商。 ——目前没有第三方服务的变更。	√		
A.16.1.1 A.16.1.2 A.16.1.3 A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.7	职责和规程 报告信息安全事态 报告信息安全弱点 评估和确定信息安全事态 信息安全事件响应 对信息安全事件的总结 证据的收集	安全事情、事故一经发生，事情、事故发现者、责任者应立即向网管报告，网管应及时对事情、事故进行反应处理。所有员工有报告安全事故、事情的义务。 目前没有计算机中病毒情况，未发生安全事件。 各部门及全体员工应按照要求及时识别安全弱点及可能的安全威胁，一旦发现应及时向有关人员或部门报告并记录，主管部门或安全管理负责人应采取有效的预防措施，防止威胁的发生。 填写安全弱点报告在《信息安全事件报告表》中，包括以下内容：1）安全弱点的原因，2）安全弱点的预防处置措施及改进计划，3）安全弱点报告提交给信息安全管理小组；	√		