KFB

金发科技股份有限公司企业标准

供应链信息安全管理规定

2024-10-18 发布　　2024-11-01 实施

金发科技股份有限公司标准化办公室 发布

目　录

1　范围 1
2　规范性引用文件 1
3　术语定义 1
3.1　供应商 1
3.2　生产商 1
3.3　贸易商 1
4　职责与权限 1
4.1　信息安全组 1
4.2　采购部 2
4.3　业务部门 2
5　信息安全管理策略及要求 2
5.1　供应商选择与评估 2
5.2　信息分类保护 2
5.3　访问控制 2
5.4　系统维护及安全配置 2
5.5　数据安全 3
5.5.1　基本要求 3
5.5.2　外部人员数据使用 3
5.6　系统实施/服务管理要求 3
6　供应商审计与监督 3
7　信息安全培训 3
8　信息安全责任定义及事件处置处理 3
8.1　信息安全责任划分 3
8.2　安全事件应急处置 4
附 录 A 5
附 录 B 13
附 录 C 14

前　言

为规范供应链信息安全，防范信息泄露、篡改、破坏等风险，保障公司资产和客户隐私安全，维护公司声誉和业务连续性。。

本标准由金发科技股份有限公司信息中心提出。

本标准由金发科技股份有限公司信息中心归口。

本标准由金发科技股份有限公司信息中心信息起草。

本标准主要起草人：袁健

本系列标准审核人：周盛佳

本系列标准批准人：顾均勇

本标准于 2024 年 10 月首次发布，其修订履历如下表所示：

文件修订记录表

序号	版本	修订内容	修订人	审核	批准	修订时间
1	A	新增标准	袁健	周盛佳	顾均勇	2024/09/01

供应链信息安全管理要求

1 范围

本标准规范了供应商在为金发科技股份有限公司及其下属子公司提供服务期间的信息安全要求，防范信息泄露、篡改、破坏等风险，保障公司资产和员工隐私安全，维护公司声誉和业务连续性。

本标准适用于金发科技股份有限公司及其下属子公司的供应商。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

金发科技信息安全管理规定

金发科技信息系统应急响应流程

供应商管理规范

管理供应商分类评估及应用流程

3 术语定义

3.1 供应商

指向公司提供物资的经营者，包括物资的生产商和贸易商。

3.2 生产商

指具有所有物资的生产资质且从事生产活动，通过生产商品并卖出的从而赚取利润的企业。

3.3 贸易商

指无所供应物资的生产资质，仅通过商品交易，赚取商品流通环节中的上下游差价或收取相应的佣金的企业。

4 职责与权限

4.1 信息安全组

制定供应链信息安全策略，审批信息安全计划，协调重大信息安全事件的处理，监督信息安全工作的执行情况。执行供应链信息安全策略，制定具体的信息安全管理制度和操作规范，组织信息安全培训和演练，定期检查和评估信息安全状况，及时发现和处置信息安全隐患。

对供应链信息安全工作进行审计和监督，确保信息安全管理制度和操作规范的执行效果，对发现的问题提出改进建议，并跟踪整改情况。

4.2 采购部

负责本部门的信息安全日常管理，监控信息安全风险，及时报告信息安全事件，配合信息安全进行信息安全检查和评估工作，确保本部门员工遵守信息安全政策和规定，执行信息安全组对供应商提出的问题进行整改与跟踪。

4.3 业务部门

负责本部门的信息安全日常管理，监控信息安全风险，及时报告和处理信息安全事件，配合信息信息中心进行信息安全检查和评估工作。

5 信息安全管理策略及要求

5.1 供应商选择与评估

SRM系统作为供应商的唯一入口，涉及提供工业服务（包含信息工程服务、维保IT）、商业服务（包含差旅、酒店、票务、签证、人力服务）、物流服务、关务服务、技术服务的供应商在准入时需要填写信息安全调查问卷，问卷内容包含安全管理体系、安全开发流程、数据保护措施等方面的评估，考察供应商基本的信息安全建设情况。

a) 在选择供应商时，评估其信息安全能力和合规性，选择符合要求的供应商。
b) 每年应对涉及信息化建设、系统数据交互的供应商进行信息安全评估，确保其持续符合公司要求。
c) 在与供应商签订合同时，明确信息安全要求和责任，包括保密条款、数据保护条款等。
d) 对违反信息安全协议的行为进行处罚和索赔。

5.2 信息分类保护

a) 根据信息的敏感程度和价值，将信息分为不同等级（如绝密、机密、秘密、内部、公开等），并采取相应的保护措施。
b) 对敏感信息进行加密存储和传输，确保信息的机密性和完整性。
c) 每年对敏感信息进行风险评估和重新分类，确保信息保护措施的针对性和有效性。

5.3 访问控制

a) 实施严格的访问控制策略,供应商需访问金发科技信息系统的需要对用户进行身份验证和权限管理。
b) 账号需采用多因素认证方式（如用户名+密码+动态验证码等），提高用户身份验证的安全性。
c) 每季度应对供应商使用金发科技信息系统的账号进行权限审查,确保权限的合理性和权限最小化原则。

5.4 系统维护及安全配置

a) 每季度对涉及到供应商使用的信息系统进行安全配置和漏洞扫描，及时修复安全漏洞。
b) 加强网络设备、服务器、存储设备等硬件设施的安全防护，确保物理安全和网络安全。
c) 对重要系统进行冗余备份和容灾备份，确保系统的可靠性和可用性。

5.5 数据安全

5.5.1 基本要求

a) 定期对重要数据进行备份和恢复测试，确保数据的可靠性和可用性。
b) 实施数据脱敏和匿名化处理，保护客户隐私。
c) 对数据进行加密存储和传输，确保数据的机密性和完整性。
d) 每年对数据进行风险评估和重新分类，确保数据保护措施的针对性和有效性。

5.5.2 外部人员数据使用

a) 外部人员的账号信息的申请和数据的使用须由公司对接人协助,须遵循权限最小化原则提供账号权限和数据信息。
b) 现场或项目相关的外部人员数据的使用应借用公司加密电脑或使用移动加密客户端进行访问，数据使用完毕后，项目负责人应及时进行销毁，并回收公司电脑、移动加密客户端等支持查看加密文件的工具。
c) 涉密数据的使用需由项目负责人通过部门长批准后方可使用。
d) 外部人员离场后，项目负责人应立即通过企业微信/邮箱等方式，通知对应系统管理员，对账号进行回收。

5.6 系统实施/服务管理要求

a) 实施安全需求分析，明确软件需满足的信息安全要求。
b) 在设计阶段考虑安全架构和防护措施，如数据加密、访问控制等。
c) 遵循安全的编码规范，避免常见的安全漏洞。
d) 进行全面的安全测试，包括渗透测试、代码审查等，确保软件无安全漏洞。
e) 如需使用第三方服 务或组件，应对第三方进行严格的安全审查，确保其符合安全要求。

6 供应商审计与监督

a) 每年根据5.1供应商分类中的供应商分类进行抽查，对其信息安全落实情况进行审计，确保其遵守公司信息安全政策和规定。
b) 金发科技各业务部门对发现的信息安全问题，需及时通知供应商进行整改，并跟踪整改效果。
c) 信息中心信息安全组对供应商的信息安全状况进行定期评估和报告。

7 信息安全培训

a) 信息中心-信息安全组每年度对集团采购、销售进行信息安全意识培训，提高员工对供应链安全的认知与集团信息安全的策略要求，并根据培训的效果进行评估，调整培训计划及内容。
b) 新员工在上岗前，需参与公司组织的信息安全培训，确保其了解公司的信息安全政策和规定。
c) 供应商每年度应对其员工进行至少一场全员信息安全意识培训。

8 信息安全责任定义及事件处置处理

8.1 信息安全责任划分

	甲方	乙方

安全管理	告知供应商公司安全管理要求，确保了解并遵守公司的信息安全政策和规定。	对员工进行信息安全管理要求的培训，确保员工具有安全意识和技能。
数据保护	1、在提供数据时，采用加密传输，降低数据泄密的风险。 2、定期对供应商的信息安全控制措施进行审计和评估，及时发现并纠正潜在的安全隐患。	1、在使用数据时，应在授权的范围内使用，并确保数据的完整性和安全性。 2、对自身的信息安全风险进行评估和管理，制定风险应对措施，如建立应急响应机制和数据泄露预案。 3、合作终止，应清理其存储的数据，需继续承担保密义务，不得泄露合作期间获取的敏感信息。
系统安全	定期评估供应链中的信息安全风险，并制定应对措施。	1、保护其信息系统安全性，定期对其系统进行风险评估，防止被攻击或泄露。
合规性	确保供应商的信息安全实践符合法律法规的要求，以降低法律风险。	供应商应遵守所有相关的信息安全法律法规和标准，如GDPR、HIPAA等。
软件服务	定期进行系统漏洞扫描和渗透测试，及时修复发现的安全问题。	确保提供的产品和服务不包含恶意代码或漏洞。
沟通协作	建立定期沟通机制，及时分享信息安全方面的最新信息和最佳实践。通过协作共同提升整个供应链的信息安全水平。	

8.2　安全事件应急处置

如发生信息安全事件，参照《金发科技信息系统应急响应流程》执行相关流程。

附 录 A
（规范性附录）
信息安全评估表

Information Security Assessment Checklist 信息安全评估表			
No. 序号	Assessment Elements 评审要素	Achieved Score 评分	Comment & Evidence 注释&证据
1	Security Management 安全管理		
1.1	Basic policies and promotion system for information securityanization? - Have you clarified the rules that information security should follow. - Is there a system for regularly appointing positions such as CISO to oversee information security as an organization to monitor security status. 信息安全的基本政策和体系 - 是否明确了关于信息安全应该遵守的规则 - 是否有任命统括信息安全的职务（CISO 等）等定期作为组织来掌握安全状况的体制？		
1.2	Is there a designated person responsible for Information Security? - Have an information organization structure and establish an information security management representative (The management representative appointed letter) 是否指定信息安全负责人? - 有信息组织机构以及制定信息安全管理者代表（管理者代表颁布令）		
1.3	Is there regular information security awareness training and activities conducted? 是否定期开展信息安全意识培训及活动		

1.4	Is there a confidentiality agreement signed by employees in key positions? - Define key positions (R&D Department,sales department, project department, production department, etc.); - Confidentiality management regulations/list of key positions - Personnel in key positions have signed confidentiality agreements 是否签订关键岗位员工保密协议？ - 有定义关键岗位（研发部、销售部、项目部、生产部等） - 保密管理规定/关键岗位清单 - 关键岗位人员有签署保密协议		
2	Internal management system 内部管理制度		
2.1	Is there an internal information security related system? - Information security management system: information security manual, information security strategy, confidential information management system, etc. 是否有内部信息安全相关制度？ - 信息安全管理体系制度：信息安全手册、信息安全策略、保密信息管理制度等		
2.2	Does the management system cover: personnel, physical environment, data files, equipment security (routing, switching, computers, servers)? - Personnel management system, physical environment management system, data asset management system, terminal equipment management system, network security equipment management system 管理制度是否涵盖：人员、物理环境、数据文件、设备安全（路由、交换、电脑、服务器）？ - 人员管理制度、物理环境管理制度、数据资		

	产管理制度、终端设备管理制度、 网络安全设备管理制度		
2.3	Is there an annual information security audit carried out? - Information security audit report 是否有年度信息安全评审？ - 信息安全评审报告		
3	Access Control 访问控制		
3.1	Are there sound password setting rules: password strength, regular replacement? - Account password management system: including password policy (difference between ordinary users and special permissions), as well as the frequency and triggering conditions of regular reviews - Facility password policy configuration (production system, office system, AD domain, etc.) 是否有完善的密码设定规则：密码强度、定期更换？ - 账户密码管理制度：包括，密码策略（普通用户和特殊权限的区别）、 以及定期评审的频次和触发条件 - 设施密码策略配置（生产系统、办公系统、AD 域等）		
3.2	Is there anti-virus software and administrator rights control for office computers? - Anti-virus management system: including whether the management of anti-virus software includes definition requirements for installation, uninstallation, virus		

	database, rule database, and regular scanning of anti-virus software - Employee computers cannot uninstall anti-virus software - match the computer asset serial number 是否有办公电脑杀毒软件及管理员权限管控？ - 防病毒管理制度，包括：杀毒软件的管理是否包括杀毒软件的安装、卸载、病毒库、规则库、 定期扫描的定义要求 - 员工电脑针对杀毒软件不可以卸载 - 匹配电脑资产序列号		
3.3	Are software and vulnerability patches updated in a timely manner? - Patch management system: whether it includes patch management, patch sources, patch classification, patch testing, patch release, etc. - Patching records - Patch test records 软件及漏洞补丁是否及时更新？ - 补丁管理制度：是否包括，补丁的管理、补丁的来源、补丁的分类、补丁的测试、补丁的发布等 - 打补丁的记录 - 补丁测试记录		
3.4	Is key information stored locally and is there any uploaded backup? - The backup management system has corresponding requirements - there are different backup strategies for different categories of information - Backup records 关键信息是否本地存储，有无上传备份？ - 备份管理制度有相应的要求-针对不同类别的信息有不同的备份策略 - 备份记录		
4	Data processing 数据处理		

4.1	Do you encrypt sensitive data in general? 您是否有对敏感数据进行加密？		
4.2	Is there an important data access application process and records? - Access control management system - Important data application process records - system access 是否有重要数据访问申请流程及记录? - 访问控制管理制度 - 重要数据申请流程记录-系统访问		
4.3	Are there regular data backup and records? - Data backup strategy, including corresponding backup strategies for different categories of data. 是否有数据定期备份及记录? - 数据备份策略，包括针对不同类别的数据有相应的备份策略.		
5	Protection of Personally Identifiable Data 个人身份数据的保护		
5.1	Are information security management systems (such as personnel systems, financial systems, security systems, etc.) able to adequately protect personally identifiable data? - Systems involving personal information: restrictions on access to personal information systems, restrictions on on-demand export of output, export of personal information data content in accordance with the purpose, and desensitization requirements for personal information display. 信息安全管理系统(例如人事系统，财务系统，安防系统等)是否已能充份保护个人身份数据? - 涉及个人信息的系统：针对个人信息系统的		

	访问做限制、输出按需导出的限制、 导出遵循按照目的去导出个人信息数据内容，同时个人信息展示进行脱敏要求		
6	Physical-and Environmental Security 物理环境安全		
6.1	Do you have access control for your IT room? - Physical security management system, including: definition of critical areas and requirements for restricted access, - In and out records 机房是否有访问控制要求？ - 物理安全管理制度，包括：关键区域的定义以及限制出入限制的要求， - 进出记录		
6.2	Is there a division of critical and non-critical areas and different safety control measures? - Physical security management system, including: definitions of critical areas and non-critical areas, security requirements for physical facilities in critical areas, and requirements for access restrictions - Key areas: intelligent access control, surveillance, fire protection, entry and exit registration, regional camera requirements 是否有关键区域及非关键区域的划分及不同的安全管控措施? - 物理安全管理制度，包括：关键区域与非关键区域的定义、关键区域的物理设施安全防范要求以及访问限制的要求		

	- 关键区域：智能门禁、监控、消防、出入登记、区域摄像要求		
6.3	Are unauthorized photography prohibited in key areas? - Physical security management system, including: prohibition of photography in key areas - Physical inspection of key areas to see if there are icons indicating that photography is prohibited 是否关键区域未经授权禁止拍照行为? - 物理安全管理制度，包括：关键区域的禁止拍照行为 - 物理巡查关键区域的是否有禁止拍照的图标提示		
6.4	Do you have a home office policy? 是否有家庭办公的管理要求		
7	Response to incidents and accidents 事件事故应对		
7.1	In the event of an information security related incident or accident, is there a response plan in place to quickly respond, reduce impact, and prevent recurrence? - Have you prepared for the occurrence of accidents, such as creating a corresponding step book for the leakage, loss, or theft of confidential information. - Is there a system (CSIRT) equipped to quickly respond to network events such as information leaks or possible system failures.		

	- Can records and evidence of communication and operational terminal events on the network accessing important information and information systems be cut off as needed. 机房是否有访问控制要求？ - 像是制作机密信息泄露、丢失、被盗时的对应步骤书等，是否做好了事故发生时的准备 - 是否配备了在信息泄露或有可能发生系统故障等网络事件时能够迅速对应的体制（CSIRT） - 取得访问重要信息和信息系统的网络上的通信和操作终端的事件的记录\证据,根据需要能进行切断		

生效日期：2024 年 10 月 18 日

附 录 B
（规范性附录）
改善行动表

Improvement Actions 改善行动									
Standard 标准	No 编号	Observations/Findings 观察/不符合项	Improvement Actions 改善行动	Responsibility 负责人	Target Date 目标日期	Closure Date 关闭日期	Status 状态	Verified by 确认人	Remarks 备注
Note: Supplier shall provide the corrective actions of non-conformance items within 10 working days after receiving the audit report from Johnson Electric. 注:供应商应在收到审核报告后，在十个工作日内对不合格项回复改善措施。									

生效日期：2024 年 10 月 18 日

附 录 C
（规范性附录）
供应商准入信息安全评估表

No. 序号	Assessment Elements 评审要素	Achieved Score 评分
1	Basic policies and promotion system for information securityanization? - Have you clarified the rules that information security should follow. - Is there a system for regularly appointing positions such as CISO to oversee information security as an organization to monitor security status. 信息安全的基本政策和体系 - 是否明确了关于信息安全应该遵守的规则 - 是否有任命统括信息安全的职务（CISO 等）等定期作为组织来掌握安全状况的体制？	
2	Is there regular information security awareness training and activities conducted? 是否定期开展信息安全意识培训及活动	
3	Are there sound password setting rules: password strength, regular replacement? - Account password management system: including password policy (difference between ordinary users and special permissions), as well as the frequency and triggering conditions of regular reviews - Facility password policy configuration (production system, office system, AD domain, etc.) 是否有完善的密码设定规则：密码强度、定期更换？ - 账户密码管理制度：包括，密码策略（普通用户和特殊权限的区别）、 以及定期评审的频次和触发条件 - 设施密码策略配置（生产系统、办公系统、AD 域等）	
4	Do you encrypt sensitive data in general? 您是否有对敏感数据进行加密？	

5	In the event of an information security related incident or accident, is there a response plan in place to quickly respond, reduce impact, and prevent recurrence? - Have you prepared for the occurrence of accidents, such as creating a corresponding step book for the leakage, loss, or theft of confidential information. - Is there a system (CSIRT) equipped to quickly respond to network events such as information leaks or possible system failures. - Can records and evidence of communication and operational terminal events on the network accessing important information and information systems be cut off as needed. 机房是否有访问控制要求？ - 像是制作机密信息泄露、丢失、被盗时的对应步骤书等，是否做好了事故发生时的准备 - 是否配备了在信息泄露或有可能发生系统故障等网络事件时能够迅速对应的体制（CSIRT） - 取得访问重要信息和信息系统的网络上的通信和操作终端的事件的记录\证据，根据需要能进行切断	

生效日期：2024 年 10 月 18 日