深圳市特发信息股份有限公司文件

深信息〔2022〕20号

特发信息关于印发《深圳市特发信息股份有限公司信息安全管理办法》的通知

各单位:

《深圳市特发信息股份有限公司信息安全管理办法》于2022年8月11日经公司经营班子会审议通过，现予印发，请遵照执行。原《特发信息信息安全管理暂行办法》（深信息〔2019〕2号）同时废止。

特此通知。

深圳市特发信息股份有限公司

2022年8月19日

深圳市特发信息股份有限公司

信息安全管理办法

第一章 总 则

第一条 目的

为建立和完善与公司信息安全保障体系，保障信息化系统和IT基础设施功能的正常发挥，有效防范信息技术风险，增强网络与信息系统安全预警，应急处置和灾难恢复能力，满足特发信息业务正常开展的要求，根据《特发集团信息安全管理办法（暂行）》及国家有关法律、法规制定本办法。

第二条 总体要求

特发信息的信息安全管理坚持“管理与技术并重”的原则，既要做好规划设计，建章立制，加强管理，落实责任，也要增强技术手段，培养技术人才，切实提高技术防范能力与水平。信息安全规划设计与实施要与特发信息信息化总体发展水平相适应，既“管用”，又“够用”。坚持“动态检测、持续改进”原则，对重要信息系统和IT基础设施进行动态检测和加固，持续不断提高安全防护水平。

第三条 适用范围

本办法适用于特发信息本部,各经营单位参照执行。

第四条 术语与定义

信息安全管理: 指计算机网络及信息系统（简称信息系

统）的硬件、软件、数据及环境受到有效保护，信息系统的连续、稳定、安全运行得到可靠保障。

终端用户： 由各部门信息化设备的用户构成，负责各自使用的信息化设备的安全（如病毒码、系统升级更新等）。

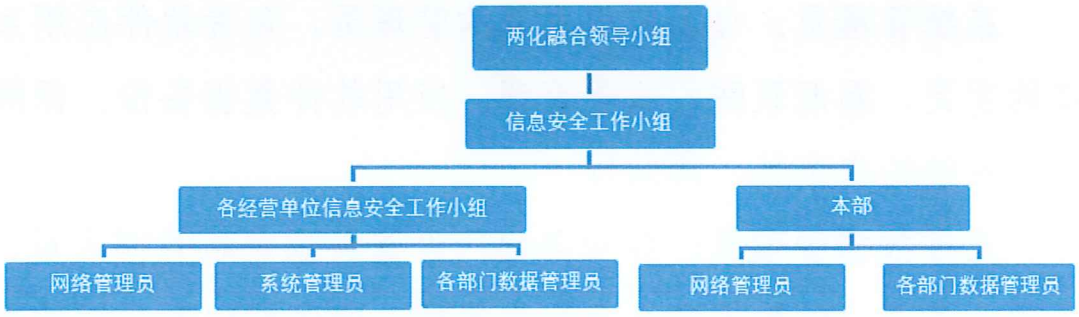
网络设备: 包括服务器、路由器、交换机、集线器，防火墙、UPS 等设备。

计算机病毒： 计算机程序的一种、在一定条件下会不断地自我复制和扩散、影响计算机的正常运行。一般是人故意设计的破坏性程序。

备份： 为应对文件、数据丢失或损坏等可能出现的意外情况，将电子计算机存储设备中的数据复制到大容量存储设备中。

第二章 信息安全组织保障体系

第五条 组织架构与主要职责



两化融合领导小组： 为公司信息安全管理最高决策机构，负责公司信息安全的组织协调和统筹规划工作，审核并批准信息系统安全决策，对跨事业部或公司级重要安全改进进行决策。

信息安全工作小组：由办公室 IT 人员及各经营单位 IT 管理人员组成，是公司信息系统安全管理机构，在授权范围内协助管理层工作，就公司信息系统建设、安全管理出具相应工作报告和专业意见，为两化融合领导小组提供决策参考。

各经营单位信息安全领导小组：由经营单位分管信息化工作的领导任组长，负责公司的总体信息安全要求的落实，及本单位信息安全的组织协调工作，并制定本单位信息安全管理制度，健全工作机制，落实管理责任。

办公室：负责制定信息安全管理制度，指导各经营单位信息安全管理工作，同时负责本部桌面端病毒预防，本部日常上网的行为安全、防火墙等网络设备日常安全加固。保障本部网络及网络设备的可靠性、连续性

网络管理员：负责各单位的网络安全的规划、管理及其相关的技术支持，公司级网络设备的管理、网络设备数据的备份、网络应用和操作培训。

系统管理员：每个应用系统的管理员，负责软件应用系统的变更、漏洞预防、权限管理、应用软件数据备份。保障软件系统的安全性、连续性。

业务数据管理员：各业务部门设置数据资料管理人员，负责业务部门的数据安全及数据管理，确保部门用户将重要的数据进行了安全的备份。

第六条 专业人才保障

加强信息安全人才队伍建设，合理配置人力，打造适应

企业信息化要求的专业人才队伍，为企业信息化建设提供坚实的人才保障。本部及各经营单位的网络管理员应具备良好的政治素质、职业操守和安全保密意识，除正常的运营维护业务外，未经审批，不得擅自对业务数据和流程进行修订，要对所接触的数据或者信息严格保密。

第七条 投入保障

按照信息化总体规划和年度工作计划安排，把信息安全产品与服务采购、培训等相关经费预算纳入年度信息化建设经费预算，加强资金保障和使用监管，确保信息安全工作必要的资金投入。

第八条 信息安全培训

积极开展培训，针对信息化人员的专业技能培训每年不少于 20 课时，针对终端用户的信息安全知识教育培训每年不少于 4 课时，通过形式多样的培训，努力 培养企业全体员工信息安全防范意识，不断提升安全防范技能和水平。

第九条 信息安全应急

为有效预防、及时控制和妥善处理网络和信息安全类突发事件，加强应急管理工作,健全应急机制，并根据年度应急演练计划，每年至少安排一次应急预案演练，强化全员应急意识，提高公司应急反应速度和实战能力，网络管理员负责做好演练记录和总结。

第三章 信息安全要求

第十条 信息安全管理要求

（一）网络设备及环境的安全管理

1.所有网络设备由网络管理员管理。其安装、维护等操作由网络管理员进行，其他终端用户不得破坏或擅自维修。

2.网络资源配置由网络管理员统一规划管理，接入公司网络的用户计算机的网络配置由网络管理员根据用户计算机MAC地址统一管理分配，包括：用户计算机的IP地址、网关、DNS等信息。未经许可，任何终端用户不得更改网络配置。

3.公司内计算机网络的扩展必须由网络管理员实施，未经许可任何终端用户不得私自连接交换机、集线器等网络设备，不得私自接入网络。网络管理员有权拆除终端用户私自接入网络的设备。

（二）计算机防病毒管理

1.网络管理员有义务指导终端用户防病毒软件安装，并负责防病毒软件的问题处理。

2.终端用户若发现防病毒软件的病毒库未能及时更新，或发现新病毒及其他疑似病毒的情况应及时通知网络管理员处理。

3.因病毒感染造成重大影响，或为防止病毒扩散的情况下，网络管理员有权暂停终端用户的网络使用权。

4.如果有突发性的恶性计算机病毒发生，网络管理员应通过电子邮件发出病毒预警通知及处理办法，终端用户应及时参照执行；终端用户遇到无法处理的计算机病毒时，及时

通知网络管理员。

5.任何人不得制作和传播计算机病毒。

6.各部门接入局域网的计算机不得安装来历不明的软件，必须安装防病毒软件，并及时更新。不得以任何借口删除或卸载防病毒软件。

（三）网络信息安全管理

公司网络仅供员工为了工作、学习使用，禁止以下活动：

1.在网络上发布有损公司形象和职工声誉的信息。

2.攻击公司网络和他人计算机，盗用、窃取他人资料、信息等。

3.利用公司邮件服务分发或转发垃圾邮件。

4.制作、查阅和传播宣扬反动、淫秽、封建迷信等违犯国家法律、企业规程和中国道德与风俗的内容。

5.传播任何非法的、骚扰性的、中伤他人的、辱骂性的、恐吓性的、伤害性的信息。

（四）数据泄密预防

1.公司员工具有信息保密的义务。任何人不得泄漏公司机密、技术资料和其它保密资料。

2.涉及公司秘密的文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄、保存，相关人员都要严格保密，不可随意乱放，如不需要时及时销毁，不得以任何方式向无关人员泄露秘密内容，具体参照《档案管理办法》执行。

3.不准在无保密措施的通信设备和计算机上传输和存储机密文件；凡使用计算机存储、传输、处理涉及公司机密信息

时，应采取保密措施，配备必要的保密设备，防止电磁辐射泄密；严格秘密数据载体（存储设备、纸张等）的管理，严格人员的审查。

4. 计算机设备、存储设备、移动设备报废须向网络管理员及办公室申请，由网络管理员统一进行数据不可还原式清除；如设备遗失使用部门应向业务数据管理员及办公室报备评估数据遗失危害。

5. 工作人员调动工作或离退休，应将自己保管的涉及公司机密的文件、资料，登记造册后移交公司，不得私自保存或复印。

（五）系统用户管理

1. 用户口令管理：用户设置含有字母、字符和数字的强度口令，并且定期修改口令。

2. 用户增加流程：新用户入职，需要增加用户账号时，人力资源部填写《用户登记表》，用户部门负责人审批相应的权限并交由系统管理员创建用户。

3. 用户变更流程：用户因工作岗位调动、口令遗忘或其它原因需要变更时，需填写《用户登记表》，用户部门负责人审批，网络管理员根据审批变更的内容在系统中做变更操作。

4. 用户撤销流程：员工因离职需要撤销时，人力资源部办理离职手续时通知网络管理员撤销该用户；其它原因需要撤销权限时，用户部门负责人书面的形式通知网络管理员撤销用户。

（六）系统变更管理

1.系统变更适用于已开发或采购完毕并正式上线、且由软件开发组织移交给应用管理组织之后，所有系统运行支持及系统变更工作。

2.系统变更可分为下面两种类型:

（1）功能性维护。业务部门由于业务发展或业务处理的需要，所产生的对系统的现有功能进行修改、完善的需求。

（2）系统缺陷修复。系统的缺陷会引系统安全事件及引发业务操作中的异常，对系统进行升级或修复的需求。

3. 系统变更工作以任务形式由业务部门和系统管理员协作完成。

4. 系统变更

（1）系统管理员负责接受变更需求，进行分析需求后，编制变更方案报告，必要的时候向系统供应商寻求协助。

（2）业务部门发现系统异常，导致系统无法正常运行，必须迅速处理解决时，问题发现人员应该立即通知系统管理员。系统管理员应立即通知相关业务部门暂停使用系统。并且研究具体解决方案，进行系统变更。紧急问题得到妥善解决后，通知业务部门可以正常使用系统，同时通知业务部门补办各类文档和审批文件。

（3）系统管理员负责对系统变更过程的文档进行归档和版本管理。

（4）变更完成后，系统管理员填写《系统变更验收单》，业务部门签字确认。

（七）系统数据备份管理

1.用户数据的备份基本原则是：“谁使用，谁备份”，业务数据管理员确保部门用户将重要的数据备份进行了安全的备份；网络管理员负责公司级网络系统的数据备份，系统管理员负责系统的数据备份。

2.备份分为：定期备份、临时备份。

定期备份指按照规定的周期对数据进行备份；

临时备份指在特殊情况（如：软件升级、设备更换、感染病毒等）下，临时对信息数据进行备份，临时备份至少保存一个月。

3.数据的定期备份原则上要求进行日备份，月备份，年备份。

公司级系统数据由系统管理员每天备份。部门用户数据由部门的业务数据管理员每月底备份，保留两份拷贝，一份在数据处理现场，以保证数据的正常快速恢复和数据查询，另一份备档在办公室，确保备份数据万无一失。

日备份至少保存十五天，月备份至少保存六个月，年备份至少保存三年，财务相关业务数据备份至少保存十年。

4.根据系统情况和备份内容，可以采取以下备份方式：

（1）完全备份：对备份的内容进行整体备份。

（2）增量备份：仅对备份相对于上一次备份后新增加和修改过的数据。

（3）差异备份：仅备份相对于上一次完全备份之后新增加和修改过的数据。

（4）按需备份：仅备份应用系统需要的部分数据。

（5）数据备份时必须建立备份文件档案及档案库，详细记录备份数据的信息,所有备份要有明确的标识，标识应包括：应用系统名称+备份时间。

第四章　附　则

第十一条 本办法由特发信息办公室负责解释。

第十二条 本办法自颁布之日起施行，原《特发信息信息安全管理暂行办法》（深信息〔2019〕2号）同时废止。

抄送：公司领导。

深圳市特发信息股份有限公司办公室　　2022年8月19日印发