成都索贝数码科技股份有限公司

网络安全应急预案

文件编号:	SBISMS11023		
文件版次:	1.1	页次:	1/7
拟订部门:	信息管理部		
发行部门:	信息管理部		
适用范围:	全公司		
拟订日期:	2024 年 11 月 6 日		
生效日期:	2024 年 11 月 6 日		
责 任 人:	梁承龙		

拟定：梁承龙 审核：陈伟 批准：陈伟

文件履历页

版本	发布日期	制/修订原因	修订内容	申请	审核	批准
V1.0	2016.5.30	新制定		尹波	周刚	周刚
V1.1	2024.11.6	更新	应急处置流程内容完善	梁承龙	陈伟	陈伟

1. 目的

确保公司能够快速、有效地响应和处置各类信息安全事件，最大限度地减少事件对公司业务、数据和声誉的影响，维护公司信息资产的安全性。

2. 定义

2.1 术语

网络攻击事件：包括拒绝服务攻击、恶意软件传播、病毒传播、黑客入侵等。

数据安全事件：包括数据泄露、数据篡改、数据丢失等。

信息系统故障事件：包括操作系统崩溃、应用程序故障、硬件故障等。

信息泄露事件：包括非授权访问、恶意泄露信息等。

人员管理事件：包括员工违规行为、内部人员恶意行为等。

物理安全事件：包括数据中心入侵、硬件被盗、物理破坏等。

2.2 信息安全事件分级

信息安全事件按其影响程度可分为以下四级：

一级事件（低危）：事件对公司业务或数据的影响极小，能够通过常规管理手段处置，且不涉及重大法律风险。

二级事件（中危）：事件对公司业务或数据有一定影响，但不会对整体业务造成重大中断，能够通过短期应急响应解决。

三级事件（高危）：事件对公司业务或数据的影响较大，可能导致部分业务中断或数据泄露，需调动公司资源进行全力应急处置。

四级事件（重大）：事件对公司业务或数据造成重大影响，涉及敏感数据泄露、大规模业务中断、法律责任等，需立即启动全面应急响应。

3. 职责

3.1 应急指挥组

应急指挥组负责全局性的决策和指挥，确保各项应急响应措施的有效落实。

组长： 总裁

负责发布和解除应急命令，调动全公司资源。

副组长： 信息管理部负责人

负责技术支持和应急响应的具体执行。

成员：信息管理部、法务部、总工办人员

各成员根据职责分工，协调和提供必要的技术、法律支持。

3.2 应急处置组

应急处置组负责具体的技术处置、恢复、报告工作。

信息管理部：负责技术应急响应工作，如网络隔离、漏洞修复、恢复系统。

研发部：负责开发环境和应用的恢复，确保业务系统正常运行。

法务部：负责事件的法律评估，确保法律合规性，处理可能的数据泄露和法律责任问题。

3.3 信息发布组

信息发布组负责向内部员工、外部公众及监管机构发布事件信息。

总裁办：向外界发布事件的处理结果，处理媒体沟通。

行政部：发布内部通告，确保员工及时了解事件进展，避免误解或恐慌。

4. 网络安全事故处置程序

4.1 事故发生

发现阶段：各部门通过监控、报警、系统异常等方式发现潜在网络安全事

件。

报告阶段：任何部门或人员发现安全事件应立即报告信息管理部，由信息管理部进行初步评估和分类。

4.2 初步评估与响应

信息管理部对报告的事件进行评估，根据事件类型和级别决定是否启动应急响应程序。

低级别（一级）事件：不影响业务或数据安全，采用常规管理措施解决。

中级别（一级至二级）事件：事件可能影响部分业务或数据，需要应急响应。

高级别（三级及以上）事件：严重影响公司业务或数据，需要全面启动应急预案。

4.3 应急响应启动

根据事件等级，启动不同级别的应急响应：

一级事件（低危）：由信息管理部进行常规处置，采取简易的修复措施，如更新病毒库、调整访问控制等。

二级事件（中危）：需要信息管理部、研发部和法务部协作，采取临时隔离、系统修复等措施，必要时向高级管理层报告。

三级事件（高危）：事件影响较大，必须立即启动应急响应计划，集中资源进行处置。

四级事件（重大）：立即启动全面的应急响应，包括外部通报、法律协调、公司全员参与等。

4.4 事件处置

网络隔离：信息管理部对受影响的网络或系统进行隔离，防止事件扩展。

漏洞修复：对系统中的安全漏洞进行修补或升级，确保不存在可被利用的漏洞。

数据恢复：恢复丢失、篡改或泄露的数据，确保业务系统的正常运行。

法律应对：法务部评估事件的法律影响，依据法律法规及时向外部报告，处理可能的合规问题。

4.5 事件结束与复盘

结束确认：在确认所有受影响的系统已恢复并且不再存在安全威胁后，宣布事件处置结束。

总结报告：编写事件总结报告，分析事件原因，评估应急响应效果，提出改进建议。

复盘与优化：对事件处置过程进行复盘，完善应急预案，提升整体应急响应能力。

5. 日常管理

5.1 定期演练

定期进行应急响应演练，确保各部门在真实事件发生时能够迅速有效地响应。

5.2 漏洞扫描与修复

定期对公司网络和系统进行漏洞扫描和修复，确保网络防护措施及时更新。

5.3 安全监控

持续进行网络流量监控和入侵检测，提前发现潜在威胁。

6. 事故发生后的行动

6.1 事件分析

分析事件发生的根本原因，找出安全漏洞和管理短板，优化系统和流程。

6.2 预案更新

根据事件处理经验，更新应急响应预案，确保适应新的威胁环境。