绥德网络货运监管服平台

网络安全建设实施方案

单位名称：绥德京卡物联数据技术有限公司

实施单位：绥德京卡物联数据技术有限公司

目 录

随着信息化的高速发展，信息安全已成为网络信息系统能否正常运行所必须面对的问题，它贯穿于网络信息系统的整个生命周期。是保障系统安全的重要手段，通过安全检测，我们可以提前发现系统漏洞，分析安全风险，及时采取安全措施。为保证我单位信息系统能够正常安全运行，单位通过以下方面进行安全加固。

第一章　物理安全保护措施

物理安全是信息系统安全中的基础，如果无法保证实体设备的安全，就会使计算机设备遭到破坏或是被不法分子入侵，计算机系统中的物理安全，首先机房采用“门禁系统”配合“监控系统”等控制手段来控制机房出入记录有效的控制接触计算机系统的人员，由专人管理周记录、月总结。确保计算机系统物理环境的安全；　其次采取设备线路准确标记、计算机设备周维护、月巡检以及机房动力环境监测短信报警等安全措施，确保计算机设备的安全。另外，通信线路是网络信息系统正常运行的信息管道，物理安全还包括通信线路实体的安全。检测网络信息系统物理安全的主要方法采用现场检查、方案审查等。

第二章　网络安全保护措施

网络的开放性带来了方便的可用性，但也使其更容易受到外界的攻击和威胁。入侵者可以利用系统中的安全漏洞，采用恶意

程序来攻击网络，篡改、窃取网络信息，从而导致网络瘫痪、系统停止运行。在网络维护过程中，我们采用防火墙、杀毒系统等防护设备严格的与网络攻防行为对抗，保障网络安全。

2.1 网络结构安全保护措施

网络信息系统为了保证内部网络拓扑信息不被非法获得，在不对性能造成影响的前提下，采用 VPN 虚拟专用网络并以多重身份认证系统隔离内部网络； 在网络信息系统内部采用使用加密设备以及划分 VLAN 的方法来防止非法窃听； 采取监控、隔离的措施来保护重要的服务器。

2.2 网络系统设备安全保护措施

网络系统的网络设备配备防火墙、入侵检测系统、以及行为审计系统等。

1） 防火墙。防火墙的抗攻击能力特别强，它是不同网络以及网络安全域信息交换的唯一出入口，功能包括： 网络数据包过滤功能、访问控制功能、网络访问行为功能以及安全审计、安全告警功能；

2） 入侵检测系统。入侵检测系统可以它可以协助系统对付网络攻击，主动保护自己免受攻击，使信息安全基础的结构更加的完整。入侵检测系统功能包括： 实时监测网络上的数据流，分析处理和过滤生成的审计数据； 联动功能和自动响应功能是否正

常； 身份认识功能是否合理有效，什么权限的授权人员才有资格设置入侵管理规则，才能查阅、统计、管理以及维护日志记录，其他人不能任意的更改或删除日志记录。

3） 病毒防范系统。病毒防范系统功能包括： 病毒防范功能、病毒特征库更新功能以及审计数据生成与管理。病毒防范系统安全检测包括： 能控制病毒侵入途径，控制并阻断病毒在系统内传播； 系统能在病毒侵入时应及时的隔离、清除病毒，在日志上详细记录病毒时间的发生及处理过程； 病毒特征库定期更新，定期统计和分析病毒的相关日志记录，及时的对病毒防范策略进行调整。

4） 安全审计系统。审计数据是系统根据设置的审计规则产生的，审计系统功能包括： 审计查阅功能、选择性审计功能。只有授权人才有权查阅审计系统的日志记录； 采取加密保护措施来确保日志的安全，任何人不得随意更改日志记录。

2.3 网络系统可用性保护措施

网络系统的可用性是网络信息系统安全要求的重要组成部分，保证网络系统安全的技术手段有： 网络冗余、技术方案验证、网络管理和监控等方面。其中，网络冗余是解决网络故障的重要措施，备份重要的网络设备和网络线路，实时监控网络的运行状态，一旦网络出现故障或是信息流量突变可以及时的切换分配，确保网络的正常运行。我们适当的采用网络监控系统、网络管理

系统这些网络管理和监控手段，运用网络故障发现、网络异常报警等功能来确保网络运行的安全。才用深信服全网监测设备实时监控网络设备运行状态。

第三章　应用系统安全措施

3.1 遵守有关制度

互联网应用信息系统必须遵守互联网信息安全管理系统的有关法律法规、规章制度和管理办法。

3.2 用户权限管理

系统用户操作权限按照用户角色限制，严禁授予无关操作权限。要对注册用户进行审核审批、授权，系统对用户 口令要进行加密管理，防止泄露。

3.3 系统漏洞修复

每个系统都有漏洞，不论你在系统安全性上投入多少财力，攻击者仍然可以发现一些可利用的特征和配置缺陷。发现一个已知的漏洞，远比发现一个未知漏洞要容易的多，这就意味着多数攻击者所利用的都是常见的漏洞。采用适当的工具，就能在黑客利用这些常见漏洞之前，查出网络的薄弱之处。修复系统漏洞是一项日常性工作，发现漏洞，及时修复。

第四章　运行安全措施

信息系统的安全与运行密不可分，网络信息系统的运行安全主要包括以下几个方面的内容：

4.1 备份与恢复

为了使数据保持一致和完整，我们对网络系统的数据进行备份，以此来确保整体网络系统数据的安全。备份和恢复的检测方案是：

1）　如果系统的硬件或存储媒体发生故障，使用系统自带的备份功能，进行单机备份，然后将数据存储到其他存储设备；

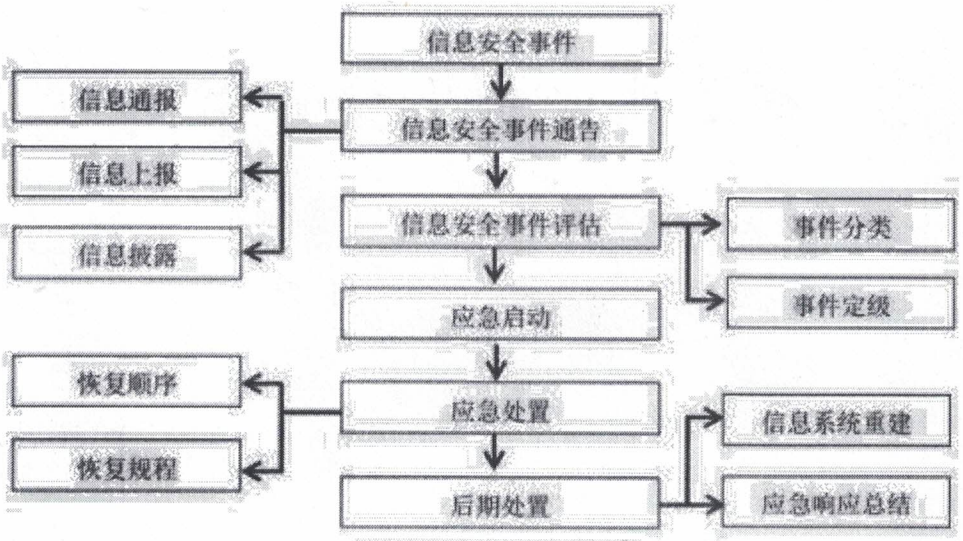
2）　在建立系统时进行设备备份冗余备份。局域网内存在备份服务器，备份的数据保存在本地和异地；　为了确保备份的高效性，要采用磁带机加存储的方法共同执行的方法；　采用 RAID 等技术，确保备份的容错性。

4.2 恶意代码

恶意代码是指没有作用却会带来危险的代码。恶意代码本身是程序，通过执行可能会利用网络信息系统的漏洞来攻击和破坏系统。处理恶意代码我们采用：　系统审查所有从外界获取的文件；在一定范围内建立防恶意代码体系，具有防恶意代码工具，在造成损失之前彻底清除恶意代码。

4.3 应急响应

应急响应的目的是在发生紧急事件或是安全事件时，确保系统不中断或紧急恢复。如图，信息安全事件处理流程。



信息安全事件处理流程

应急响应方案应包括的措施有：

1） 与多家网络公司合作能够在发生安全事件或是紧急事件时及时的做出影响分析，并组成应急小组，在法定时间内对发生的事件做出响应；

2） 具有完善的应急计划和多种切实可行的备选方案，有由外地和本地专家组成的应急小组，在法定时间内对发生的事件做出响应。