2023年防护棚方案是不是危大(实用5篇)

为了确保事情或工作得以顺利进行，通常需要预先制定一份完整的方案，方案一般包括指导思想、主要目标、工作重点、实施步骤、政策措施、具体要求等项目。怎样写方案才更能起到其作用呢？方案应该怎么制定呢？以下是小编给大家介绍的方案范文的相关内容，希望对大家有所帮助。

防护棚方案是不是危大篇一

除此之外，在铁道工程建设里，有很多的新的科学时间都很广的被应用，关于其边坡防护的相关工程技术也随着社会科技的不断发展而在社会的各个阶层都深受重视。

其边坡生态防护技术在经济、环境、社会等各个生活领域中有拥有强大的效益。

本文主要对铁路边坡生态防护技术的发展前景、功能、技术原理、主要类型进行了叙述。

引言：铁道工程边坡的生态防护根据其实际的性质和侧重点不同可分为工程防护和生态防护。

就公工程防护来说，在地质状况不是很好的状态下，利用各种措施，如：挡土墙、喷混凝土等来达到使边坡得到一定的保护并使其能够达到稳定的状态。

在此之前，在铁路工程建设的施工过程中，对于边坡来说只是做了粗略的防护，只对其本身的条件考虑了太多，并没有对其周边的生态环境有所考虑，从而造成了其周边的环境造成了一定的破坏，使周边的植物也受到了一定的影响，不仅如此，在观赏上也影响了其周围的美化，尤为重要的是，其施工阶段会产生大量的噪音，噪音污染对周围的居民的生活有多影响，也会造成不必要的麻烦。

另一类就是生态上的防护，其主要是指在铁路边坡形成以后，对铁路边坡周围的生态环境进行一定的保护，甚至进行一定的改进，这样不仅改善了铁路周边的自然环境，而且周围的一些植物对噪音和光都有一定的吸收和遮挡作用，此外，还可以对周围的植物面貌有所改进，从而使铁路工程和环境绿化工程能够很融洽的结合。

为了保护环境，维护生态的平衡，随着社会日新月异的发展，环境的绿化和保护也日益的受到社会各界的关注，这一趋势的势不可挡的，也是社会发展过程中和边坡工程发展中的必然趋势。

因此，此边坡生态保护工程是其他普通的铁路工程边坡技术无法替代的。

防护棚方案是不是危大篇二

沿海地带是台风的多发地区，我施工单位为确保施工人员的生命安全、保证企业的财产不受损失，所以对施工现场作出以下防台措施：

1、在接到台风预报时立即部署防台措施；

2、及时对全体职工传达上级防台通知，使职工了解台风的动向和来临时间。

1、由项目部防台小组组织对施工现场进行全面检查，确保万无一失；

2、各班组认真检查各种施工材料的堆放稳固，对稍有疑惑的地方进行清理整治；

3、架工班对外架的整体性能和外架与建筑物的刚性连接进行彻底的检查，对存在有安全隐患的地方立即整改。

4、施工现场专业防护小组对防护棚进行加固处理，具体加固措施为设置剪刀撑和用铁丝拉防护棚四角固定在地面。

5、塔吊操作人员在台风来临前停止所有吊装工作，吊臂的停放位置及固定点按塔吊的操作规程进行。

6、电工在接到防台通知后，立即对施工现场敷设的电路电线进行检查，电箱的放置是否牢固可靠，对有安全隐患的.地方立即整改，并在台风来临前切断所有施工用电，台风过后，先对施工现场的电路电线进行检查，确认正常后方可送电。

7、台风来临时，生活区宿舍关闭所有门窗，确保职工安全。

由项目部组织的领导班子成员彻夜值班，配置必要的通讯设备（如对讲机），便于应急时相互联络。

1、应急救援人员应经过培训和必要的演练，掌握救援行动的方法技能和注意事项，熟悉本单位安全生产情况，掌握应急救援器材，设备的性能和使用方法。

2、配备必要的应急救援器材，设备。

3、台风期间救援小组xx小时待命，发生事故及时进行处理。

成立防台应急小组，便于及时处理防台过程中出现的问题，减少不必要的损失。

防护棚方案是不是危大篇三

网络安全防护论文：

一、网络安全概述

网络安全是指网络上的信息和资源不被非授权用户使用。网

络安全设计内容众多,如合理的安全策略和安全机制。网络安全技术包括访问控制和口令、加密、数字签名、包过滤以及防火墙。网络安全,特别是信息安全,强调的是网络中信息或数据的完整性、可用性及保密性。完整性是指保护信息不被非授权用户修改或破坏。可用性是指避免拒绝授权访问或拒绝服务。保密性是指保护信息不被泄漏给非授权用户。

网络安全产品有以下特点:一是网络安全来源于安全策略与技术的多样化;二是网络的安全机制与技术要不断地变化;三是建立有中国特色的网络安全体系,需要国家政策和法规的支持及集团联合研究开发。安全与反安全就像矛盾的两个方面,总是不断地向上攀升,所以安全产业将来也是一个随着新技术发展而不断发展的产业。

二、网络安全存在的威胁因素

目前网络存在的威胁主要有以下方面:

第一,非授权访问,即没有预先经过同意,就使用网络或计算机资源。

第二,信息遗漏或丢失,即敏感数据在有意或无意中被泄漏出去或丢失。

第三,破坏数据完整性,即以非法方式窃得对数据得使用权,删除、修改、插入或重发某些重要信息,以取得有益于攻击者得响应;恶意添加,修改数据,以干扰用户得正常使用。

三、网络安全技术

(一)防火墙

网络防火墙技术是一种用来加强网络之间访问控制,防止外部网络用户以非法手段通过外部网络进入内部网络,访问内部网

络资源,保护内部网络操作环境的特殊网络互联设备。它对两个或多个网络之间传输的数据包如链接方式按照一定的安全策略来实施检查,以决定网络之间的通信是否被允许,并监视网络运行状态。根据防火墙所采用的技术不同,我们可以将它分为3种基本类型:包过滤型、网络地址转换-nat代理型。

1、包过滤型。包过滤型产品是防火墙的初级产品,其技术依据是网络中的分包传输技术。网络上的数据都是以“包”为单位进行传输的,数据被分割成为一定大小的数据包,每一个数据包中都会包含一些特定信息,如数据的源地址、目标地址tcp/udp源端口和目标端口等。防火墙通过读取数据包中的地址信息来判断这些“包”是否来自可信任的安全站点,一旦发现来自危险站点的数据包,防火墙便会将这些数据拒之门外。系统管理员也可以根据实际情况灵活制订判断规则。包过滤技术的优点是简单实用,实现成本较低,在应用环境比较简单的情况下,能够以较小的代价在一定程度上保证系统的安全。但包过滤技术的缺陷也是明显的。包过滤技术是一种完全基于网络层的安全技术,只能根据数据包的来源、目标和端口等网络信息进行判断,无法识别基于应用层的恶意侵入,如恶意的java小程序以及电子邮件中附带的病毒。有经验的黑客很容易伪造ip地址,骗过包过滤型防火墙。

2、网络地址转化-nat网络地址转换是一种用于把ip地址转换成临时的、外部的、注册的ip地址标准。它允许具有私有ip地址的内部网络访问因特网。它还意味着用户不许要为其网络中每一台机器取得注册的ip地址。在内部网络通过安全网卡访问外部网络时,将产生一个映射记录。系统将外出的源地址和源端口映射为一个伪装的地址和端口,让这个伪装的地址和端口通过非安全网卡与外部网络连接,这样对外就隐藏了真实的内部网络地址。在外部网络通过非安全网卡访问内部网络时,它并不知道内部网络的连接情况,而只是通过一个开放的ip地址和端口来请求访问olm防火墙根据预先定义好的映射规则来判断这个访问是否安全。当符合规则时,防火墙认为

访问是安全的,可以接受访问请求,也可以将连接请求映射到不同的内部计算机中。当不符合规则时,防火墙认为该访问是不安全的,不能被接受,防火墙将屏蔽外部的连接请求。网络地址转换的过程对于用户来说是透明的,不需要用户进行设置,用户只要进行常规操作即可。

3、代理型。代理型防火墙也可以被称为代理服务器,它的安全性要高于包过滤型产品,并已经开始向应用层发展。代理服务器位于客户机与服务器之间,完全阻挡了二者间的数据交流。从客户机来看,代理服务器相当于一台真正的服务器;而从服务器来看,代理服务器又是一台真正的客户机。当客户机需要使用服务器上的数据时,首先将数据请求发给代理服务器,代理服务器再根据这一请求向服务器索取数据,然后再由代理服务器将数据传输给客户机。由于外部系统与内部服务器之间没有直接的数据通道,外部的恶意侵害也就很难伤害到企业内部网络系统。

代理型防火墙的优点是安全性较高,可以针对应用层进行侦测和扫描,对付基于应用层的侵入和病毒都十分有效。其缺点是对系统的整体性能有较大的影响,而且代理服务器必须针对客户机可能产生的所有应用类型逐一进行设置,大大增加了系统管理的复杂性。

(二)加密技术

与防火墙配合使用的还有数据加密技术。目前各国除了从法律上、管理上加强数据的安全保护之外,从技术上分别在软件和硬件两方面采取措施推动数据加密技术和物理防范技术不断发展。按作用不同,数据加密技术分为数据传输、数据存储、数据完整性的鉴别和密钥管理技术4种。数据传输加密技术是对传输中的数据流加密,常用的方法有线路加密和端一端加密两种;数据存储加密技术目的是防止存储环节上的数据失密,可分为密文存储和存取控制两种。前者一般是通过加密算法转换、附加密码、加密模块等方法实现;后者则是对用户资格、

格限加以审查和限制,防止非法用户存取数据或合法用户越权存取数据。数据完整性鉴别技术目的是对介入信息的传送、存取、处理人的身份和相关数据内容进行验证,达到保密的要求,一般包括口令、密钥、身份、数据等项的鉴别,系统通过对本验证对象输入的特征值是否符合预先设定的参数。实现对数据的安全保护。密钥管理技术是为了数据使用的方便,往往是保密和窃密的主要对象。密钥的媒体有磁卡、磁带、磁盘、半导体存储器等。密钥的’管理技术包括密钥的产生、分配保存、更换与销毁等各环节的保密措施。

(三)pki技术

pki(publiekeyinfrastucture)技术就是利用公钥理论和技术建立的提供安全服务的基础设施□pki技术是信息安全技术的核心,也是电子商务的关键和基础技术。由于通过网络进行的电子商务、电子政务、电子事务等活动缺少物理接触,因此使得用电子方式验证信任关系变得至关重要。而pki技术恰好是一种适合电子商务、电子政务、电子事务的密码技术,他能够有效地解决电子商务应用中的机密性、真实性、完整性、不可否认性和存取控制等安全问题。一个实用的pki体系应该是安全的易用的、灵活的和经济的。它必须充分考虑互操作性和可扩展性。它是认证机构(ca)□注册机构(ra)□策略管理、密钥(key)与证书(certificate)管理、密钥备份与恢复、撤消系统等功能模块的有机结合。

1、认证机构□ca(certificationauthorty)就是这样一个确保信任度的权威实体,它的主要职责是颁发证书、验证用户身份的真实性。由ca签发的网络用户电子身份证明-证书,任何相信该ca的人,按照第3方信任原则,也都应当相信持有证明的该用户□ca也要采取一系列相应的措施来防止电子证书被伪造或篡改。

2、注册机构□ra(registrationauthorty)是用户和ca的接口,它

所获得的用户标识的准确性是ca颁发证书的基础□ra不仅要支持面对面的登记,也必须支持远程登记。要确保整个pki系统的安全、灵活,就必须设计和实现网络化、安全的且易于操作的ra系统。

3、策略管理。在pki系统中,制定并实现科学的安全策略管理是非常重要的这些安全策略必须适应不同的需求,并且能通过ca和ra技术融入到ca和ra的系统实现中。同时,这些策略应该符合密码学和系统安全的要求,科学地应用密码学与网络安全的理论,并且具有良好的扩展性和互用性。

4、密钥备份和恢复。为了保证数据的安全性,应定期更新密钥和恢复意外损坏的密钥是非常重要的,设计和实现健全的密钥管理方案,保证安全的密钥备份、更新、恢复,也是关系到整个pki系统强健性、安全性、可用性的重要因素。

5、证书管理与撤消系统。证书是用来证明证书持有者身份的电子介质,它是用来绑定证书持有者身份和其相应公钥的。通常,这种绑定在已颁发证书的整个生命周期里是有效的。但是,有时也会出现一个已颁发证书不再有效的情况这就需要进行证书撤消,证书撤消的理由是各种各样的,可能包括工作变动到对密钥怀疑等一系列原因。证书撤消系统的实现是利用周期性的发布机制撤消证书或采用在线查询机制,随时查询被撤消的证书。

(四)网络防病毒技术

在网络环境下,计算机病毒有不可估量的威胁性和破坏力,一次计算机病毒的防范是网络安全性建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消毒三种技术。

预防病毒技术,即通过自身的常驻系统内存,优先获得系统的控制权,监视和判断系统中是否有病毒存在,进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可

执行程序、引导区保护、系统监控和读写控制。

检测病毒技术,即通过对计算机病毒的特征进行判断的技术,如自身校验、关键字、文件长度的变化等。

消毒技术,即通过对计算机病毒的分析,开发出具有删除病毒程序并恢复原文的软件。

网络反病毒技术的具体实现方法包括对网路服务器中的文件进行频繁的扫描和监测;在工作站上用防毒芯片和对网络目录及文件设置访问权限等。

四、安全技术的研究现状和动向

我国信息网络安全研究历经了通信保密、数据保护两个阶段,正在进入网络信息安全研究阶段,现已开发研制出防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。对我国而言,网络安全的发展趋势将是逐步具备自主研制网络设备的能力,自发研制关键芯片,采用自己的操作系统和数据库,以及使用国产的网管软件。我国计算机安全的关键在于要有自主的知识产权和关键技术,从根本上摆脱对国外技术的依赖。

网络安全技术在21世纪将成为信息网络发展的关键技术,21世纪人类步入信息社会后,信息这一社会发展的重要战略资源需要网络安全技术的有力保障,才能形成社会发展的推动力。在我国信息网络安全技术的研究和产品开发仍处于起步阶段,仍有大量的工作需要我们去研究、开发和探索,以走出有中国特色的产学研联合发展之路,赶上或超过发达国家的水平,以此保证我国信息网络的安全,推动我国国民经济的高速发展。

防护棚方案是不是危大篇四

学校校园网是为教育及学校管理而建立的计算机信息网络,

目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了促进我校信息化建设和应用，提高我校现代化水平，保护校园网络系统的安全，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理制度。

第一章总则

本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

1、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

2、学校装备中心及其所辖的网络管理中心(以下简称网络中心)负责相应的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

3、任何单位和个人，未经网络中心同意，不得擅自安装、拆卸或改变网络设备。

4、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

5、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

6、使用校园网的全体师生有义务向网络中心和有关部门报告违法行为和有害信息。

第二章网络安全管理

1、校园网由学校装备中心统一管理及维护。连入校园网的各部门、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，建立网络事故报告并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。网络教室不准对社会开放。

5、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监控：

(1)校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

(2)加强对学生开放互联网以及全校教职工上网的监管。

(3)专用的财务工作电脑和重要管理数据的电脑原则上不要接入网络工作。

8、网络中心统一在每台计算机上安装防病毒软件，各部门要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

9、禁止私自安装、卸载程序，在校园网上，禁止使用盗版软件，不允许玩电子游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

10、严禁在校园网内使用来历不明、引发病毒传染的软件或文件;对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、杀毒。

11、任何部门和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

12、未经网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

13、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

14、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线

路设备及附属设备，不准擅自把计算机设备外借。

15、各部门必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通知网络中心处理。

16、各部门应认真做好本部门计算机的养护和清洁卫生工作。

第三章网络用户安全守则

1、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害国家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

2、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作;任何部门和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

3、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把账户借给他人使用，增强自我保护意识，经常更换口令，保护好账户和ip地址。严禁用各种手段解决他人口令、盗用账户和ip地址。

4、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

第四章处罚或赔偿办法

违反本制度规定，有下列行为之一者，学校可提出警告、停止其上网，情节严重者给予行政处分，直至提交纪检司法部

门处理，损坏的照价赔偿。

1、查阅、复制或传播下列信息者：

(1)煽动分裂国家、破坏国家统一和民族团结、违反四项基本原则的;

(2)煽动抗拒、破坏宪法和国家法律、行政法规的实施;

(3)捏造或者歪曲事实，故意散布谣言或传谣，扰乱社会秩序;

(4)公然侮辱他人或者捏造事实诽谤他人;

(5)宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

3、盗用他人帐号或私自转借、转让用户帐号造成危害者;

4、故意制作、传播计算机病毒等破坏性程序者;

5、上网信息审查不严，造成严重后果者;

6、使用任何工具破坏网络正常运行或窃取他人信息者;

7、有盗用ip地址、盗用帐号和口令、解决用户口令等危及网络安全运行与管理的恶劣行径者。

防护棚方案是不是危大篇五

为保证我厂设备正常运转，确保冬季内的顺利安全生产，特制定本预案，具体内容如下：

1、加强对设备的防寒防冻工作，机电、生产班组加强对主厂房及附近的管道、闸阀的检查及维护，对裸露在外的管道及闸阀进行保暖处理。

2、生产班组在交接班时及日常生产过程中做好备用设备及停开的设备放水工作；裸露在室外的各个闸阀要保证有较小的水量，以防冻裂。

3、主厂房、外围皮带走廊、产品仓和原煤仓、新老筛分楼的门窗要关严，破损窗户及时修复或封堵，作好室内保暖工作。

4、日常生产中，停车时间超过两小时以上的，停用设备要求每两小时空车运转一次；各个泵及管道要进行放水，保持冷却泵正常开启。

5、冬季生产中，外部现场严禁用水冲刷地面、皮带走廊及楼梯，防止地面结冰，危及行人安全。

6、厂内员工在上下楼梯时，禁止将手插进口袋内不扶扶手，原煤仓、产品仓、矸石仓外楼梯严禁行人通过。

7、介质、絮凝剂、凝聚剂以及所需备品备件准备要充足，避免因雨雪天气造成以上物品无法按时送到而影响正常生产的问题。

8、各门帘要在冬季到来之前全部悬挂完毕，对各个区域暖气管路进行全面排查，有问题及时处理，确保正常供暖。

9、准备充足的’胶皮管等物品，如有管路冻结能够及时处理。

在生产过程中，如遇设备或管道冻住事故，不能强行启动设备，应用胶皮管子接暖气进行化冻，完全化冻后方可启动设备。

1、对各岗位的暖气进行全面排查，确保每个岗位暖气都能正常取暖。

2、随时检查厂房各门窗情况，及时提醒职工做好自身保暖工作。

1．各班组长及值班领导是本单位防冻防寒工作的第一责任人，对本队防冻防寒工作负责。

2．本厂生产现场不设任何形式的烤火炉及电气取暖设备。私自使用的按厂相关规定追究责任人责任。

3．对没有按照本预案进行防冻防寒责任落实的班组及个人，当发生冻坏设备的事件后，按相关制度规定追究其责任。

4．对违反规定上下楼梯不扶扶手及走各个精煤仓及矸石仓外楼梯的职工按制度严格处理。

5、对于易发生高空坠冰的区域要设立警示牌、必要时设立隔离带，防止高空坠落冰块砸伤职工。印发之日起正式实施。