信息安全手册
Information Security HandBook

确保内外网隔离，严禁内外用一机；
处理涉国密信息，要用专用保密机。
防病毒和防木马，安全补丁及时打；
实时保护要启动，定期扫描毒可控。
口令不要怕复杂，数字字母结合佳；
长度至少八位数，定期更换牢记住。
接收邮件要谨慎，注意留意发件人；
不明附件勿打开，莫名链接勿点击。
使用安全移动盘，查杀病毒首当先；
重要文档加密码，数据文件常备份。
网页挂马威胁多，各种插件要确认；
恶意软件遍网络，不明网站莫访问。
基础知识和操作，大家一同来学习；
防护措施记心间，信息安全在身边。

目 录

第一章　信息安全基础知识篇

1、什么是信息安全?

国际标准中对信息安全的定义是：信息本身的机密性(Confidentiality)、完整性(Integrity)和可用性(Availability)的保持，即防止未经授权使用信息、防止对信息的不当修改或破坏、确保及时可靠地使用信息。

通俗的说，信息安全就是:

- 确保信息系统持续、可靠、稳定运行
- 防止信息丢失、篡改和泄密。

2、信息安全防护目标

- 确保管理信息系统和电力二次系统安全稳定运行
- 确保信息内容安全

3、信息安全防护策略

- 管理信息系统安全防护策略
  - **双网双机** 管理信息网划分为信息内网和信息外网，内外网间采用逻辑强隔离装置进行隔离，内外网分别采用独立的服务器及桌面终端
  - **分区分域** 在公司信息系统划分为管理信息大区与生产控制大区的基础上，依据定级情况的业务系统类型，进行安全域划分，以实现不同安全域的独立化、差异化防护
  - **等级防护** 以实现等级保护为基本出发点进行安全防护体系建设
  - **多层防御** 在分域防护的基础上，各安全域的信息系统划分为边界、网络、主机、应用四个层次进行纵深防御的安全防护措施设计
- 电力二次系统安全防护策略
  - **安全分区** 发电企业、电网企业和供电企业内部基于计算机和网络技术的应用系统，原则上划分为生产控制大区和管理信息大区，生产控制大区可以分为控制区（又称安全区Ⅰ）和非控制区（又称安全区Ⅱ）
  - **网络专用** 电力调度数据网是为生产控制大区服务的专用数据网络，承载电力实时控制、在线生产交易等业务

- **横向隔离** 采用不同强度的安全设备隔离各安全区，在生产控制大区与管理信息大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置，隔离强度应接近或达到物理隔离
- **纵向认证** 采用认证、加密、访问控制等技术措施实现数据的远方安全传输以及纵向边界的安全防护

4、信息安全威胁及产生的后果

◆ 信息安全面临的威胁:

- 人为的无意失误——如操作员误操作、用户弱口令。
- 人为的恶意攻击——如越权访问信息、信息数据侦听。
- 信息系统本身缺陷——如系统硬件故障、软件故障。
- 物理环境影响——如电力故障、自然灾害。
- 管理不当——如权限管理不当。
- 病毒木马——如蠕虫、间谍软件。

◆ 威胁产生的后果:

- 信息系统遭受攻击
- 敏感信息泄露或丢失
- 数据被窃取或远程监控
- 信息被恶意添加、删除或修改
- 计算机病毒（木马）的传播
- 信息系统被非授权或越权访问

5、信息安全防护重点

6、常见的信息安全事故及处理

常见的信息安全事故:

- 信息发布和服务网站遭受攻击和破坏
- 应用系统数据丢失或停止服务故障
- 非法入侵，或有组织的攻击
- 大面积病毒爆发、蠕虫、木马程序、有害移动代码
- 网络、设备、操作系统和基础软件故障
- 自然灾害或人为外力破坏

一旦发生信息安全事故，应立即启动信息系统应急预案，并按预案处置流程进行事件报告、应急处置。

7、国家秘密、公司秘密的等级

国家秘密的密级从高到低依次分为**“绝密”**、**“机密”**、**“秘密”**三级。

涉及公司秘密的信息包括**商业秘密**和**工作秘密**。

- 商业秘密在载体上标识为**“商密一级”**、**“商密二级”**
- 工作秘密标识为**“内部事项”**或**“内部资料”**

8、涉密信息的处理及存储

涉及国家秘密的信息必须在保密计算机中进行处理，保密计算机必须与信息内网、信息外网等信息网络实现物理隔离。信息内网和信息外网的计算机均不得处理涉及国家秘密的信息。

记载国家秘密信息的纸介质、磁介质、光介质等秘密载体，均要存放在保险柜内，与其他普通载体分开管理。

严禁普通移动存储介质和涉及国家秘密的介质在保密计算机和信息内外网计算机之间交叉使用。

8、信息安全认识误区

误区一：电脑病毒靠“杀”

目前大多数的杀毒软件都扮演着“事后诸葛亮”的角色，即电脑被病毒感染后杀毒软件才去发现、分析、清除，这种被动防御的消极模式不能彻底解决计算机安全的问题；同时，杀毒软件有时良莠不分，会把合法数据也当作病毒清除，很容易造成信息的丢失和损毁。因此对待电脑病毒应当以**“防”**为主，防患于未然。

误区二：文件被删除后不可恢复

不少人认为被删除的文件从“回收站”清空后就永远消失，事实上，一些特殊软件或技术完全可以实现将被删除或损坏的数据进行恢复。因此要妥善保管好数据存储介质，以防信息泄漏。

误区三：网络共享文件是安全的

网络共享文件存在漏洞，很有可能被恶意人员利用和攻击，因此共享文件应予以关闭，若必需使用，共享文件应该设置高强度口令，并设置文件权限为只读。

10、信息安全行为十严禁

- ◆ 严禁将涉及国家秘密的计算机、存储设备与信息内外网和其他公共信息网络连接；
- ◆ 严禁在信息内网计算机存储、处理国家秘密信息；
- ◆ 严禁在连接互联网的计算机上处理、存储涉及国家秘密和企业秘密的信

息;

- 严禁信息内网和信息外网计算机交叉使用;
- 严禁普通移动存储介质在信息内网和信息外网上交叉使用;
- 严禁扫描仪、打印机等计算机外设在信息内网和信息外网上交叉使用;
- 严禁在普通传真机上发送涉及国家秘密、企业秘密的文件;
- 严禁在电话、手机等通讯工具中谈论涉及国家秘密、公司企业秘密的事项;
- 严禁携带涉及国家秘密、公司企业秘密的计算机和存储介质离开公司;
- 严禁在办公计算机上使用盗版光盘和来历不明的盘片.

第二章　信息安全操作篇

1、防病毒和防木马

- **病毒**

病毒是一段特殊的计算机程序，具有类似生物病毒的行为特性，如自我复制、传染性、破坏性和变异性等。

感染病毒后常见现象

- ◆ 网络拥塞，经常断线或根本无法使用网络
- ◆ 计算机运行速度变慢，出现 CPU 或内存高使用率现象
- ◆ 经常出现系统错误或系统崩溃或无故重启
- ◆ 磁盘上生成未知文件，空间急剧减少
- ◆ 应用程序图标改变，打开应用程序无故报错
- ◆ 无法启动浏览器，无故关闭或跳转到非定制页面

- **木马**

木马程序是一种基于远程控制的黑客工具，它潜伏在电脑中，受外部用户控制以窃取电脑信息，它具有隐蔽性和非授权性的特点。

中木马后常见现象

- ◆ 硬盘在无操作的情况下频繁被访问
- ◆ 用户帐号口令被盗取
- ◆ 系统无端搜索软驱、光驱
- ◆ 计算机运行速度变慢，出现 CPU 或内存高使用率现象

- **清除病毒木马**

- ◆ 使用企业级防病毒系统查杀病毒木马

在信息内外网分别部署网络版防病毒软件系统，定期对防病毒软件特征码和软件版本进行升级。

- ◆ 开启防病毒软件实时更新功能

计算机必须安装防病毒软件，开启所有监控功能，定期检测运行状况，

定期对计算机进行全盘扫描。

◆ 使用专用工具进行彻底清除

2、操作系统安全

1）经常检查更新并安装操作系统补丁

2）删除多余用户

3）开启屏幕保护

3、口令安全

1）不安全的口令:

◆ 姓名、生日、电话号码等个人信息

◆ Password、root、admin 等默认口令

◆ 123456、与用户名相同的口令等弱口令

2）安全的口令:

◆ 长度至少达到 12 个字符

◆ 由大小写字母、数字和其它字符混合组成。

3）口令安全遵循原则:

◆ 不在多个系统中使用同一口令

◆ 定期更换口令，周期不超过 3 个月

◆ 严格保管用户名（帐号）和口令

4、邮件安全

公司邮件分为内网邮件系统和外网邮件系统，内外网邮件系统相互隔离，二者之间不能互相发送和接收邮件。

发送和接收邮件要做到以下几点:

◆ 信息内网邮件不得发送涉及国家秘密信息

◆ 信息外网邮件不得发送涉及国家秘密和企业秘密（含商业秘密和工作秘密）信息

- 不直接打开、阅读来历不明的电子邮件
- 对可疑后缀如.exe、.com、.pif、.scr、.vbs 为后缀的附件文件，不要轻易下载打开
- 邮件发送和接收前都应使用防病毒软件对邮件附件进行病毒查杀，确保附件及内容无病毒

5、安全移动存储介质

安全移动存储介质主要用于公司员工在工作中产生的涉及公司秘密信息的存储和内部传递（包括商密一级、商密二级和工作秘密），也可用于内网非涉密信息与外部计算机的交互，涉及公司企业秘密的信息必须存放在保密区。

禁止使用普通存储介质存储涉及公司企业秘密的信息。禁止将安全移动存储介质中涉及公司企业秘密的信息拷贝到外网计算机，禁止在外网计算机上保存、处理涉及公司企业秘密的信息。

安全移动存储介质维修工作由各单位专业技术人员负责，出现故障的存储设备要妥善保存并按规定及时销毁。

6、重要数据文件备份

对于重要数据和文件，应使用移动存储设备、光盘介质等定期进行备份，避免病毒破坏、人为误删除或磁盘物理性损坏而导致的数据丢失，确保意外发生后可恢复重要数据和文件，一般可以采用本地备份或异地备份。

7、重要文件加密传输

涉及公司商业秘密信息和重要文件必须采用信息加密压缩方式在信息内网进行传送。使用公司已统一采购 WinRAR 正版压缩软件对文件进行加密压缩（可在公司总部门户“服务之窗”栏目中下载），加密口令要求 12 位以上并包含字母数字，同时加密口令要采用不同的传递方式如电话等，在确保安全的前提下传送。

已在信息内网建设有 CA 认证系统的单位，可采用 CA 数字证书，在其有效覆盖范围内的信息内网进行信息加密传递。

对于在信息外网和互联网上传输的非涉及公司秘密和敏感信息的内容，也应采用 WinRAR 加密压缩方式进行传输，进一步提高安全性。

8、日常文件管理

建议将日常文件保存在“本地磁盘（D:）/（E:）/（F:）”等位置

切勿将日常文件保存在“本地磁盘（C:）/桌面/我的文档”等位置，以防操作系统瘫痪或病毒破坏等导致的文件数据丢失。

9、软件下载与安装

办公计算机不得安装、运行、使用与工作无关的软件，不得随意更改或卸载统一配置的软件;从互联网下载的软件,应使用杀毒软件进行病毒查杀后再使用。

10、良好的上网习惯

- 对上网计算机的登录帐号设置具备一定强度的口令
- 及时升级系统补丁
- 安装杀毒软件，打开所有监控功能，定期对上网计算机进行安全漏洞扫描
- 不要访问不熟悉的网站、不要下载安装来历不明的软件

第三章　信息安全防护篇

1、系统漏洞

系统漏洞是指应用软件或操作系统在设计上存在的缺陷或在编写时产生的错误，这个缺陷或错误可以被恶意人员利用，通过植入木马、病毒等方式来发动攻击或控制整个计算机，从而窃取重要资料和信息，甚至破坏系统。

案例：操作系统缓冲区溢出漏洞

攻击者首先利用漏洞扫描工具对重点网段进行扫描，寻找存在缓冲区溢出漏洞的计算机。

攻击者启动漏洞攻击软件实施攻击，以获得目标计算机的系统权限。攻击者利用漏洞获得系统权限后，采用远程登录软件即可以进入目标计算机进行操作。

防范对策：

- 严禁将涉及国家和公司企业秘密的信息内网计算机接入互联网；
- 办公计算机补丁及时升级；
- 安装企业级防病毒软件；
- 安装防木马软件。

2、木马

木马是针对目标计算机实施远程控制的“间谍”软件。

案例：“灰鸽子”木马

攻击者先将木马程序捆绑在一些应用程序中，以电子邮件的形式发送给目标用户。目标用户收到邮件后，在打开应用程序的一瞬间，“木马”便植入计算机并运行，此时将通知攻击者植入成功。于是攻击者便可通过“木马”远程监控目标计算机，任意下载窃取其中的文件资料。下图为“灰鸽子”木马获取银行帐号密码的图示。

防范对策：

- 严禁将涉及国家和公司企业秘密的信息内网计算机接入互联网；

- 不随意打开不明电子邮件，
- 不轻易打开电子邮件附件；
- 计算机必须安装杀毒软件并及时升级更新。

3、嗅探

嗅探是指植入特定功能程序，用以隐蔽探测和记录键盘操作、口令密码等信息的窃密技术。

案例：利用 Sniffer 工具嗅探 FTP 口令

攻击者首先利用漏洞或木马在目标计算机中植入 Sniffer 嗅探工具。当目标计算机重新连接互联网使用 FTP 时，Sniffer 嗅探工具便开始记录明文传输的 FTP 的用户名和口令。（图截小）

防范对策：

- 严禁将涉及国家和公司企业秘密的信息内网计算机接入互联网；
- 用于连接互联网的计算机，任何情况下不得处理涉及国家秘密、商业秘密和个人帐户口令的信息；
- 严禁启用共享文件夹处理信息数据。

4、数据恢复

数据恢复，指磁盘数据在删除或格式化后可利用相关工具进行恢复。

案例：使用数据恢复软件恢复磁盘数据

先将计算机磁盘进行格式化处理，数据删除后，窃密者启动数据恢复软件，对该盘进行格式化恢复，成功恢复原有文件。

防范对策：

- 处理涉及国家秘密、商业秘密的移动存储介质严禁在连接互联网的计算机上使用；
- 涉及国家秘密、公司企业秘密的存储介质淘汰、报废时，必须作彻底的物理销毁；
- 严格将涉密载体当作废品出售。

5、口令破解

口令破解是使用穷举法把计算机键盘上的数字、字母和符号按照一定的规则进行排列组合实验直到找到正确的口令。

案例：“暴力破解”口令

攻击者首先启动“暴力破解”口令破译软件，输入目标计算机 IP 地址，对目标计算机进行口令破译。口令越长，组合越复杂，破译难度越大，所需时间越多。一旦找到正确的口令，软件显示破译成功。这时，攻击者就可以利用得到的口令攻击目标计算机。

防范对策：

- 加强口令强度，使用数字、大小写字母和特殊符号组成的高强度口令；
- 口令长度至少 8 位以上，并定期进行修改。

6、 “摆渡”

摆渡，指利用移动存储介质在不同的计算机之间隐蔽传递数据信息的窃密技术。

案例：U 盘“摆渡”，通过互联网或其他途径使 U 盘感染摆渡程序，当目标用户将感染了摆渡程序的 U 盘插入涉密计算机时，在无任何操作和显示的情况下，U 盘内的摆渡程序能按事先设定好的窃密策略将文件从计算机中复制到 U 盘隐藏目录下，同时将自身摆渡程序复制到计算机中。一旦此 U 盘插入上互联网计算机，文件就会被摆渡程序迅速转移至上网计算机中，此时窃密者即可实施远程窃取。

防范对策：

- 严禁移动存储介质在信息内网和信息外网上交叉使用；
- 安装杀毒软件并及时更新升级。

7、预设后门

后门，是指计算机、操作系统、交换机等在设计制造过程中，人为设置的可用于远程维护、信息收集或设备操控的隐蔽功能。与一般漏洞相比，“后门”的隐蔽性更强、破坏力更大。

案例：被攻击者预植了后门程序的计算机一旦接入互联网，后门程序便被激活，攻击者即可利用后门获取该计算机权限，实现远程操纵计算机，从而窃取存于计算机中的涉密信息。

防范对策：

- 严禁将涉及国家和公司企业秘密的信息内网计算机接入互联网；
- 关键信息设备尽量选用国内安全性高的技术产品；
- 加强对引进设备与软件系统的安全检测和漏洞发现，阻断信息外泄的渠道。

8、无线设备

计算机无线设备是指部分或全部采用无线电（光）波这一传输媒质进行连接的装置。无线网卡、无线键盘、无线鼠标和蓝牙、红外接口都属于这类设备。

无线上网使用开放式的无线信道传输，信号暴露在空中，任何具有接收能力的设备都可能获取传输的信息，即使采用加密技术，也可能被破解。

无线键盘、无线鼠标等无线外围设备，因其传输采用开放的空间传输方式，传输信号极易被接收还原，也存在泄密隐患。

案例：安装有 Windows 操作系统并具有无线联网功能的笔记本电脑只要上互联网或被无线互联，就有可能被攻击者通过空口令、弱口令及磁盘共享等漏洞而取得控制权。攻击者可将麦克风打开，使笔记本电脑变成窃听器造成泄密，也可植入病毒木马，窃取计算机中的信息。

防范对策：

- 涉及国家秘密的内网计算机必须拆除具有无线联网功能的硬件模块或对无线联网功能进行有效阻断；
- 严禁使用无线键盘、无线鼠标等无线外围设备。

9、手机窃听

手机通信传输系统是一个开放的地面或卫星无线通信系统，只要有相应的设备，即可截听通话内容。

案例：一些手机，特别是进口和功能复杂手机，制造时易被植入特殊功能程序，具有隐蔽通话功能，可直接用于遥控窃听，甚至将关机或待机的手机转为通话状态，在无振铃、无显示的状态下将周围的声音发射出去，成为窃听器。在这种情况下，任何能使用手机进行通讯的地方，都可窃听通话内容。

防范对策：

- 严禁使用手机谈论涉及国家秘密、公司企业秘密的事项；
- 严禁谈论涉及国家秘密、公司企业秘密的事项时随身携带手机；
- 严禁将手机带入重要涉密场所；
- 严禁在手机上存储、处理涉及国家秘密、公司企业秘密的信息；
- 涉密人员不得随意使用他人赠送的手机。

10、办公设备窃密

在复印机、打印机、传真机、碎纸机等办公设备内加装窃密装置，或利用其存储功能窃取数据信息，也是不可忽视的窃密手段。

防范对策：

- 严禁扫描仪、打印机等计算机外设在信息内网和信息外网上交叉使用；
- 涉密办公设备应当使用国产的，经有关主管部门指定的检测测评机构检测测评合格的设备，或通过有关主管部门鉴定的设备；购买涉密办公设备应到国家保密局指定、有保密资质的定点厂家购买，专人负责使用和保管；如无国产设备可选，使用进口设备须经有关主管部门或其指定的检测机构检测批准；
- 涉密设备的维修必须到有关部门指定、具有保密资质的定点维修部门将涉密信息删除或将涉密部件拆除后维修，如需要更换录有涉密信息的部件，须将旧件带回销毁，禁止折价出售或随意丢弃；
- 退还或淘汰的涉密设备须进行彻底的消密处理，交保密部门统一销毁，禁止作为私用或转借他人。

附录一

国家电网公司信息安全管理暂行办法

第一章　总 则

第一条　为加强和规范国家电网公司（以下简称公司）信息安全工作，提高公司信息系统整体安全防护水平，实现信息安全的可控、能控、在控，依据国家有关法律、法规、规定及公司有关制度，制定本办法。

第二条　本办法所称信息系统是指公司一体化企业级信息系统，主要包括一体化企业级信息集成平台（以下简称“一体化平台”）和八大业务应用。“一体化平台”包含信息网络、数据交换、数据中心、应用集成和企业门户；“业务应用”包含财务（资金）管理、营销管理、安全生产管理、协同办公、人力资源管理、物资管理、项目管理、综合管理业务应用。

第三条　信息安全主要任务是确保信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止信息内容及数据丢失和失密，防止有害信息在网上传播，防止公司对外服务中断和由此造成的一次系统事故。

第四条　在规划和建设信息系统时，信息安全防护措施应按照“三同步”原则，与信息系统建设同步规划、同步建设、同步投入运行。

第五条　本办法适用于公司总部，各区域电网、省（自治区、直辖市）电力公司和公司直属单位（以下简称各单位）的信息安全管理工作。

第二章　安全职责

第六条 公司信息安全管理按照“谁主管谁负责，谁运营谁负责”原则，实行统一领导、分级管理。各单位主要负责人是本单位信息安全第一责任人，各单位信息化领导小组负责本单位信息安全重大事项决策和协调工作。

第七条 信息安全纳入公司安全管理体系，实行专业化管理、归口监督。公司信息工作办公室是信息安全的管理和保障部门，安全监察部是公司信息安全监督部门。

第八条 公司信息工作办公室主要职责：

（一）落实国家有关信息安全法规、方针、政策、标准和规范，联系国家有关部门落实信息系统安全管理相关工作；

（二）组织制定公司信息安全管理规章制度和标准规范；

（三）指导、协调和检查各单位信息安全工作，组织落实公司信息系统等级保护制度，统筹开展公司信息系统风险评估和安全检查工作；

（四）负责重大以下信息安全事件的调查和处理（公司信息系统安全事件描述见《国家电网公司信息系统事故调查与统计规定》）；协助、配合重大及以上信息安全事件的调查和处理；

（五）负责建立公司信息系统应急体系；

（六）配合开展涉密计算机网络和系统立项、设计和建设的监督、审核，配合开展计算机信息系统安全和保密监督检查；

（七）负责规范公司信息系统安全产品的测评和选型工作。

第九条 公司安全监察部主要职责：

（一）负责将信息安全纳入公司安全生产管理体系，实施公司信息安全全过程监督；

（二）负责重大及以上信息系统安全事件的调查和处理；

（三）负责归口统计网络与信息安全事件。

第十条 国家电力调度通信中心主要职责：

（一）负责制定电力二次系统管理制度，制定电力二次系统安全

防护策略；

（二）负责电力二次系统应急处理预案的制定与审查；负责电力二次系统信息安全事件的调查和处理；

（三）协助完成国家有关部门对公司电力二次系统开展的信息安全检查、等级保护制度落实等各项工作。

第十一条 各单位主要职责：

（一）负责贯彻落实国家有关信息安全法规、方针、政策、标准和规范，贯彻落实公司信息系统安全相关规章制度和技术标准；

（二）负责建立健全本单位信息安全标准制度和规范体系；

（三）在公司信息职能管理部门指导下，落实本单位信息系统等级保护制度、信息系统风险评估和安全检查等工作；

（四）按公司信息系统应急体系要求建立本单位信息系统应急体系，组织本单位信息系统安全突发事件的应急处理；

（五）负责明确本单位信息系统安全运行维护部门或机构，落实信息系统安全运行维护日常工作，具体落实信息安全等级保护和安全策略。

（六）组织本单位信息安全的宣传和培训。

第十二条 业务应用部门主要职责：

（一） 配合开展业务应用系统安全等级定级工作；

（二） 配合开展业务应用系统安全测评、安全检查和风险评估等工作；

（三） 负责或配合开展业务应用使用人员的有关信息安全和保密培训工作；

（四） 协助开展业务应用人员办公计算机安全管理。

第三章 管理措施

第十三条 安全管理制度

要不断建立健全信息安全管理制度体系，通过操作规程实现安全管理和操作人员的标准化作业；定期或不定期对信息安全管理制度进

行检查和审定，对存在不足或需要改进的安全管理制度及时进行修订。

第十四条 安全管理机构

要明确安全管理机构，设立系统管理员、网络管理员、安全管理员等岗位，并明确各岗位职责；避免一人多岗，关键事务岗位应配备多人共同管理。应加强信息安全管理人员之间、信息职能部门和业务部门之间的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题。

第十五条 人员安全管理

应严格信息安全从业人员录用过程，审查其身份、背景、专业资格，关键岗位应签署保密协议；及时终止离岗员工的所有访问权限；严格外部人员访问程序，对允许访问人员实行专人全程陪同或监督，并登记备案。

第十六条 等级保护

应严格按照国家有关部门要求，开展公司网络与信息系统定级、审批、备案工作。针对确定的网络与信息系统安全等级，要根据等级保护有关要求，落实必要的管理和技术措施，严格执行等级保护制度 。

第十七条 建设管理

新建信息系统涉及安全防护措施建设，应明确安全需求，确定安全等级，结合公司安全防护总体策略，进行安全防护方案设计；根据国家有关规定和坚持鼓励使用国产化产品原则，开展安全产品采购；开展必要的产品预先选型测试；加强软件开发管理，确保开发环境与实际运行环境物理分开；应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；对测试不符合要求的，在整改后要重新测试。系统试运行前，要开展相关安全培训。

第十八条 运维管理

（一）环境和资产管理：要严格执行信息机房管理有关规范，确保机房运行环境符合要求，严格机房出入管理。要编制网络与信息系

统资产清单，建立资产管理制度，根据资产重要程度对资产进行标识。

（二）设备和介质管理：要对信息系统软硬件设备选型、采购、使用等实行规范化管理，建立相应操作规程，对终端计算机、工作站、便携机、系统和网络等设备实行标准化作业。强化存储介质存放、使用、维护和销毁等各项措施。

（三）网络和系统管理：要按照最小服务配置和最小授权原则，对安全策略、安全配置、日志和操作等方面做出具体规定，明确各个角色的权限、责任和风险；详细记录日常操作、运行维护记录、参数设置和修改等内容，严禁任何未经授权的操作；定期开展运行日志和审计数据分析工作，及时发现异常行为。及时根据需要进行软件升级更新，并在更新前做好备份；定期进行漏洞扫描，及时发现安全漏洞并进行修补；及时安装补丁程序，在安装补丁前做好测试和备份工作。

（四）恶意代码防范管理：

要及时升级防病毒软件，加强全员防病毒木马的意识，不打开、阅读来历不明的邮件；要指定专人对网络和主机进行恶意代码检测并做好记录，定期开展分析；加强防恶意代码软件授权使用、恶意代码库升级等管理。

（五）变更管理：

要严格系统变更、系统重要操作、物理访问和系统接入申报和审批程序，建立健全变更管理制度。保证所有与外部系统的连接均得到授权和批准，进行必要的安全隔离，配置严格的访问控制策略，开展必要的安全评估。

（六）密码管理：

要建立和执行密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

（七）监控和安全管理中心：

要对信息网络与系统运行状况等进行监测和报警；定期对监测和报警记录进行分析，根据需要采取必要的应对措施；应建立安全管理

中心，对安全设备、恶意代码、补丁升级、安全审计等安全设施进行集中管理。

（八）安全事件管理：

要严格按照有关信息系统事故调查规定，及时报告信息系统事故情况，认真开展信息系统事故原因分析，坚持“四不放过”原则，有效落实整改，确保类似事故不再发生。严格执行有关公司网络与信息系统安全运行情况通报制度，做好定期、节假日和特殊时期的网络与信息系统安全运行情况报送工作。

第十九条 安全评估

要严格执行公司有关信息安全风险评估管理规定，切实将信息安全风险评估工作常态化和制度化，及时落实整改，及时消除信息系统安全隐患。根据国家和公司要求，定期开展信息安全检查工作，做好特殊时期安全检查和安全保障工作。

第二十条 应急机制

要不断完善应急预案，加强培训和演练，确保人力、设备、技术和财务等应急保障资源可用。

第二十一条 备份与容灾

要建立备份与恢复管理相关安全管理制度，严格控制数据备份和恢复过程，妥善保存备份记录，执行定期恢复程序。认真做好容灾方案可行性研究，切实根据需要开展容灾系统建设。

第二十二条 网络信任体系

要切实加强网络信任体系建设规划工作，不断完善公司安全认证系统相关技术标准和功能规范。强化信任体系应用工作，做好信息系统统一身份认证，以及重要信息的加密和签名工作。

第二十三条 培训和考核

要切实加强员工信息安全培训，提高全员信息安全意识；强化信息安全人员专业技能培训，做到培训工作有计划、有总结，培训效果有评价。要对关键岗位人员进行全面、严格的安全审查和技能考核，

对在信息安全工作中做出显著成绩的单位和人员应给予奖励和表彰。对违反国家法律、法规和公司有关规定，造成一定不良影响和后果的，要追究其责任。

第四章　技术措施

第二十四条　总体防护策略

公司信息安全坚持“分区、分级、分域”总体防护策略，切实执行信息安全等级保护制度要求，有效落实公司信息安全防护方案，做好各区之间安全隔离，落实管理信息内、外网之间实施强逻辑隔离的措施；根据信息系统定级水平，科学合理地做好安全域划分和安全域之间隔离工作。

第二十五条　物理安全

要根据国家和公司有关规定，对机房建筑设置符合要求的避雷装置、灭火和火灾自动报警系统；采取防雨水措施，防止雨水、水蒸气结露和地下积水；设置温、湿度自动调节设施，控制机房温、湿度在设备运行所允许范围之内。计算机系统供电应与其它供电分开，并保证双路供电，设置稳压器和过电压防护设备，并提供 8 小时以上的 UPS 备用电力供应；电源线和通信电缆应隔离，避免互相干扰；采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

第二十六条　网络安全

（一）网络结构划分：网络核心交换机、路由器等网络设备要冗余配置，合理分配网络带宽；建立业务终端与业务服务器之间的访问控制；根据需要划分不同子网；对重要网段采取网络层地址与数据链路层地址绑定措施。

（二）网络访问控制：采用防火墙或入侵防护设备（IPS）对内网边界实施访问审查和控制；对进出网络信息内容实施过滤，对应用层常用协议命令进行控制，网关应限制网络最大流量数及网络连接数。严格拨号访问控制措施。

（三）网络安全审计：应严格网络安全审计工作，网络安全审计

系统应定期生成审计报表，自动进行备份；审计记录应受到保护，避免删除、修改或破坏。

（四）边界检查和入侵防范：加强内部用户私自访问外部网络行为的检测工作，要能够及时发现，准确定位，有效阻断；对重要网段，应采用入侵检测系统进行监控，对入侵事件及时提供报警。

第二十七条 系统安全

（一）身份鉴别：对操作系统和数据库系统用户进行身份标识和鉴别，具有登录失败处理，限制非法登录次数，设置连接超时功能；用户访问不得采用空账号和空口令，口令要足够强健，长度不得少于8位。

（二）系统访问控制：应严格限制匿名用户的访问权限；实现操作系统和数据库系统特权用户访问权限分离，对访问权限一致的用户进行分组，访问控制粒度应达到主体为用户级，客体为文件、数据库表级。

（三）资源控制：控制单个用户的多重并发会话和最大并发连接数，限制单个用户对系统资源、磁盘空间的最大或最小使用限度，当系统服务水平降低到预先规定的最小值时，应能检测和报警。

（四）系统安全审计：应严格系统安全审计工作，系统安全审计系统应定期生成审计报表，自动进行备份；审计记录应受到保护，避免删除、修改或破坏。

第二十八条 数据安全

重要和敏感信息实行加密传输和存储；对重要信息实行自动、定期备份；对门户网站页面，要具有防篡改机制和措施。

第二十九条 用户安全

严格用户帐号及口令管理，使用强健复杂口令，定期更换口令，杜绝使用空口令；定期开展用户终端计算机数据备份工作，及时安装系统补丁程序，及时更新杀病毒程序，加强移动存储介质管理。

第五章 附 则

第三十条 本办法由国家电网公司信息工作办公室负责解释。

第三十一条 各单位可根据本办法制定实施细则，报国家电网公司备案。

第三十二条 本办法自印发之日起执行。

附录二

国家电网公司办公计算机信息安全和保密管理规定

第一章 总 则

第一条 为加强国家电网公司（以下简称公司）办公计算机信息安全和保密管理，依据国家有关制度和条例，制定本规定。

第二条 本规定主要就公司信息内外网办公计算机信息安全与保密管理的职责及管理要求做出具体规定。

第三条 信息内外网办公计算机分别运行于信息内网和信息外网，实现网络强隔离与双网双机。信息内网定位为公司信息业务应用承载网络和内部办公网络；信息外网定位为对外业务应用网络和访问互联网用户终端网络。

第四条 信息内网办公计算机及其外设可涉及公司企业秘密，但严禁存储、处理涉及国家秘密的信息，严禁接入与互联网联接的信息网络。信息外网办公计算机及其外设不能存储、处理涉及国家秘密及公司企业秘密的信息。计算机外设是指与计算机相连的打印机、扫描仪、复印机、多功能一体机、摄像装置等外部设备。

第五条 涉及国家秘密的信息系统（涉密信息系统）按照国家《计算机信息系统保密管理暂行规定》（国保发[1998]1 号）、《涉及国家秘密的信息系统审批管理规定》（国保办发[2007]18 号）、《信息安全等级保护管理办法》（公通字[2007]43 号）等文件的要求进行管理。严格执行“涉密不上网、上网不涉密”纪律，严禁将涉及国家秘密的

计算机、存储设备与信息内外网和其他公共信息网络连接，严禁在信息内网计算机存储、处理国家秘密信息，严禁在连接互联网的计算机上处理、存储涉及国家秘密和企业秘密信息；严禁信息内网和信息外网计算机交叉使用；严禁普通移动存储介质和扫描仪、打印机等计算机外设在信息内网和信息外网上交叉使用。公司系统各单位涉密信息系统和涉及国家秘密的计算机要向本单位保密委员会和公司保密委员会办公室备案。

第六条 涉及国家秘密安全移动存储介质的安全保密管理按照公司有关保密规定执行。涉及公司企业秘密的安全移动存储介质管理按照公司办公计算机安全移动存储介质管理规定执行。

第七条 本办法适用于公司总部和公司各单位（以下简称各单位）的办公计算机的信息安全和保密管理。

第二章　管理职责

第八条 公司办公计算机信息安全和保密工作按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”原则，各单位及各部门负责人为单位和部门的办公计算机信息安全和保密工作的责任人。

第九条 各单位保密委员会全面负责办公计算机保密工作，负责办公计算机保密管理的决策、协调、监督、检查和培训教育工作。

第十条 各单位信息化管理部门负责办公计算机的信息安全工作，配合保密委员会做好办公计算机保密的技术措施指导、落实与检查工作。

第十一条 办公计算机使用人员为办公计算机的第一安全责任人，严格执行公司办公计算机的信息安全和保密管理规定，未经本单

位运行维护人员同意并授权，不允许私自卸载公司安装的安全防护与管理软件，确保本人办公计算机的信息安全和内容安全。

第十二条 国网信通公司具体负责总部办公计算机信息安全和保密措施的落实、检查实施与日常维护工作。

第十三条 办公计算机日常运行维护由公司信息运行维护队伍承担，禁止外包给公司系统外的其他单位。

第三章 管理要求

第十四条 办公计算机要按照国家信息安全等级保护的要求实行分类分级管理，根据确定的等级实施必要的安全防护措施。信息内网办公计算机部署于信息内网桌面终端安全域，信息外网办公计算机部署于信息外网桌面终端安全域，桌面终端安全域要采取安全准入管理、访问控制、入侵监测、病毒防护、恶意代码过滤、补丁管理、事件审计、桌面资产管理等措施进行安全防护。

第十五条 加强办公计算机信息安全和保密管理：

（一） 要对信息内外网办公计算机、外设及软件安装情况进行登记备案，定期核查；办公计算机不得安装、运行、使用与工作无关的软件，不得安装盗版软件；

（二） 严禁办公计算机“一机两用”（同一台计算机既上信息内网，又上信息外网或互联网）。信息内外网办公计算机要进行明显标识；

（三） 信息内网办公计算机不能配置、使用无线上网卡等无线设备，严禁通过电话拨号、无线等各种方式与信息外网和互联网络互联；

（四） 接入信息内外网的办公计算机 IP 地址由运行维护部门统一分配，并与办公计算机的 MAC 地址进行绑定；

（五） 定期对信息内外网办公计算机企业防病毒软件、木马防范软件的升级和使用情况进行检查，确保不被病毒、木马感染，不得随意卸载统一安装的防病毒（木马）软件；

（六） 定期对信息内外网办公计算机补丁更新情况进行检查，确保补丁更新及时；

（七） 定期对信息内外网办公计算机及应用系统口令设置情况进行检查，避免空口令，弱口令；

（八） 采取措施对信息外网办公计算机的互联网访问情况进行记录，记录要可追溯，并保存六个月以上；

（九） 采取措施对信息内外网邮件收发中的信息涉密情况进行检查；

（十） 定期对信息内外网办公计算机涉及国家秘密和企业秘密的情况进行检查；

（十一） 办公计算机要妥善保管，严禁将办公计算机带到与工作无关的场所。

第十六条 各单位要应用公司统一推广的信息内网计算机桌面终端管理系统，加强对信息内网办公计算机的安全准入、补丁管理、运行异常、违规接入、安全防护等的管理，部署安全管理策略，进行安全信息采集和统计分析。

第十七条 加强对办公计算机外设管理：

（一） 计算机外设要统一管理，统一登记和配置属性参数；

（二） 严禁私自修改计算机外设的配置属性参数，如需修改要报知计算机运行维护部门，按照相关流程进行维护；

（三） 严禁计算机外设在信息内外网交叉使用；

（四） 计算机外设的存储部件要定期进行检查和清除。

第十八条 办公计算机维护和变更要求：

（一） 办公计算机及外设维护要及时报计算机运行维护部门，由运行维护部门负责维护；

（二） 信息内网办公计算机及外设和存储设备在变更用途，或不再用于处理信息内网信息，或不再使用时，要报计算机运行维护部门，由运行维护部门负责采取有效手段删除存储部件中涉及企业秘密的信息。

第十九条 人员要求：

（一） 加强对办公计算机使用人员的管理，开展经常性的信息安全和保密教育培训，提高办公计算机使用人员的信息安全和保密意识与技能；

（二） 办公计算机使用人员离岗离职，有关部门要及时报运行维护部门对其办公计算机进行涉及企业秘密信息的清理，并取消其办公计算机及应用系统的访问权限。

第四章 附 则

第二十条 违反本规定泄露公司企业秘密的办公计算机使用人员，情节较轻的由本单位予以批评教育，情节严重的按公司相关规定进行处理。

第二十一条 各单位可根据本规定，结合实际，制定完善本单

位办公计算机信息安全和保密管理的具体办法。

第二十二条 本规定由信息化工作部负责解释并监督执行。

第二十三条 本规定自颁布之日起执行。