河南水利与环境职业学院信息安全总体策略

一、安全策略概述

（一）范围

信息安全关系到单位所有类型信息的存贮、处理或传输以及与其相关的硬件、软件及固件。本策略适用于单位所有部门的所有系统（以下简称系统）及相关人员。

（二）目标

信息安全的目标是确保系统的连续性，并通过一系列预防措施将系统可能受到的损害降到最低，将信息安全事故产生的影响降到最小。信息安全管理应在确保信息和计算机资产受到保护的同时，确保信息能够在允许的范围内正常运行使用。对每种资产的保护程度由以下四个基本要素决定：机密性、完整性、可用性、可审计性。

同时，本策略的目的也让单位员工能够了解信息安全问题以及个人的责任，并严格遵守本安全策略。促进信息安全策略的实现和普及是每个员工应尽的责任和义务。依照本安全策略，需要制定信息安全相关的岗位及职责要求。

（三）遵循

单位所有员工都有责任学习、理解并遵守本策略，以保障单位信息安全工作。对违反本策略的行为，根据事件性质和违规的严重程度，采取相应的处罚措施。信息安全管理部门应根据违规的严重程度向相关领导提出建议惩罚措施。除

本策略中涉及的要求之外，单位所有部门及员工同样需要遵守相关国家法律和法规的要求。

信息安全总体策略由信息安全领导小组负责制定和解释，并每年组织一次对总体策略的修订和维护，由信息安全领导小组办公室在全单位发布。

（四）安全组织机构

1．信息安全组织机构

建立信息安全组织机构的目标是管理单位的信息安全。单位必须建立专门的信息安全领导小组，指定专职的信息安全管理员，不得与其它系统管理员、数据库管理员、应用系统管理员等管理人员角色重叠。

信息安全是全单位信息安全组织机构必须共同承担的责任。必须建立信息安全领导小组，由主管领导任组长，领导小组应能够：

（1）为单位的信息安全工作提供清晰的指导方向，可见的管理支持，明确的信息安全职责授权；

（2）审查、批准信息安全策略和岗位职责；

（3）审查关键安全事件；

（4）审查、批准信息安全保障能力的控制措施和管理机制；

（5）保证必要的资源分配，以实现数据有效性以及信息安全管理体系的持续发展。

信息安全管理相关部门必须为建立和维持信息安全管理体系，协调相关活动，承担如下职责：

（1）调整并制定所有必要的信息安全管理制度、规程以及实施解释等；

（2）提议并配合执行信息安全相关的实施活动，如风险评估、资产分级分类等；

（3）主动采取单位内的信息安全措施，如安全意识培训及教育等；

（4）配合执行新系统或服务的特殊信息安全措施；

（5）审查对信息安全策略的遵循性；

（6）审查、监控、协调对信息安全相关事件的评估和响应；

（7）配合并参与安全评估事项；

（8）定期向单位信息安全领导小组报告信息安全工作情况。

2.信息安全岗位及职责划分

安全岗位和职责的分配应该根据单位的具体情况，补充详细的环境、系统或服务的描述，这些描述必须明确定义个人资产（包括物理的和信息的）的职责和安全规程，单位具体的安全岗位及职责划分参见《信息化工作岗位设置及其职责》文件。

为了避免任何对个人责任的误解，每个管理者的职责范围必须被明确规定，以下几点需要重点强调：

（1）应该识别和定义与每个业务应用系统相关的各种资产和安全过程；

（2）管理者应该明确与其相关的管理责任，并且形成文件；

（3）应明确定义授权级别，并形成文件。

（五）术语表及其定义

资产：对单位有价值的任何东西。

数据：为适用于人们或自动处理方式进行交流、阐述或处理而采用形式化方法表示的事件、概念或指令。

信息：依据数据通常表达的意思，当前赋予数据的意义。

用户：利用信息技术的个人或组织。

可用性：确保当请求者需要时信息和关键服务可用。

机密性：保护敏感信息免受非授权泄露或明文被中途拦截。

完整性：确保信息和计算机软件的精确和完整。

可审计性：能确定行为责任的能力。

控制措施：管理信息安全风险的方法，包括策略、制度、规程划组织机构。可以是行政、技术、管理、法律等方面的方式方法。

信息安全：信息的机密性、完整性和可用性的保护。

系统：人、硬件设备、系统软件、应用软件和使用或处理的数据（或信息）的组合。

安全事件：任何已经发生的或可能发生导致单位信息安全受到损害的事件，或是违反单位信息安全相关规定的行为。

信息处理设施：任何信息处理系统、服务或基础设施、或放置它们的场所。

信息安全管理：管理机制，使信息安全得以执行。

二、资产分类与控制

信息资产是用来处理、存贮信息的硬件和软件以及为这些硬件和软件提供支撑服务的资产（例如能量提供、电缆、房屋等）。为了保护信息，必须识别这些资产并定义它们所需的保护类别和等级。

（一）信息分类

用于指明防护信息的需求和优先级。

1.资产分类分级

信息资产，包括计算机和网络，应当依据其价值和敏感性以及机密性、完整性和可用性原则进行分类。信息安全管理部门应当根据部门的业务特点制定本系统内具体的资产分类与分级办法，并根据分级与分类办法制定明晰的资产清单。分类分级如下：

（1）秘密信息。对系统有价值的和敏感的信息划分为秘密信息，根据需要，数据必须被保护以防止被泄漏、破坏或修改。

（2）关键信息。系统用于保持正常业务持续进行的信息划分为关键信息，对关键信息必须进行备份并作为系统应急预案的一部分进行存储，以保证在这些信息受到破坏的情况下，系统业务正常进行和及时恢复。对备份信息必须进行保护以免破坏和非授权修改。

（3）仅在内部使用信息。来自外部资源（报纸、杂志、调查、书籍等）的信息划分为仅在内部使用信息，这些信息的使用、再出版要遵守版权。

（4）普通信息。其他信息划分为普通信息，这些信息，尽管不属于上述类别，可能很容易被篡改和破坏。因此，对普通类的信息也需要进行安全考虑。

2.资产的保护

信息资产的防护等级应当与它们的分类一致。

3.分类标记

处理敏感信息的系统的输出应当依据其分类进行物理标记。

4.文档分类

文档和其他物理信息资产应该根据它们的类别进行适当的使用、储存和销毁。系统输出所使用的分类准则与其相关文档的分类准则必须保持一致。

（二）资产的可审计性

信息资产应能够被识别、说明并指定责任人，制定并保存信息资产的详细目录。对于关键资产应当明确信息责任人，并为其分配执行和维护等相应权限。与系统相关的资产如下：

1.信息资产

包括数据库、数据文件、电子数据表、命令执行文件、手册以及支撑程序和人等。

2.逻辑设备

包括系统、应用软件和开发工具等。

3.物理设备

包括计算机设备、移动电话、各种类型的媒介、家具和房屋等。

三、人员信息安全策略

为避免信息遭受人为过失、窃取、欺骗、滥用的风险，应当识别单位每项工作的信息安全职责并补充相关的规定文件。对信息和系统的访问进行授权和取消应依据“必须知道”的原则。全体单位员工都应该了解系统的网络与信息安全需求。单位需要为员工提供足够的培训以达到该信息安全要求，并为其提供报告安全事件和威胁的渠道。

（一）工作定义及资源的安全

员工从事或离开工作岗位时必须进行信息安全考虑，相关的安全事项应包括在工作描述中。内容如下：

1.对涉及访问秘密或关键信息，或处理这些信息的系统工作人员应进行严格审查和挑选。

2.根据安全岗位和职责来描述工作。

3.对系统具有特殊访问权限的员工应该签署相关协议，保证不会滥用权限。

4.当员工离开单位时应该移交系统的访问权限，或员工仅在单位内部变动工作时也应该重新检查调整其访问权限。

（二）用户培训

1.单位员工应了解相关系统的安全需求，并对如何安全使用信息以及相关的系统和工具进行培训。应对单位员工就信息安全策略和相关管理规定进行培训，使他们熟悉信息安

全的实施并加强安全意识。

2.管理人员应该保证全体员工明确其与系统信息安全策略相关的职责，在开始执行策略时向其介绍相关安全需求。

3.在对员工授权项信息技术服务进行访问前，必须对其进行培训，确保他们正确使用相关的信息工具和设备。

（三）事件报告

1.建立有效的信息反馈渠道，以便于员工发现安全威胁、事件和故障时，能及时向有关人员报告。

2.信息安全管理者的职责之一就是确保该渠道的合理性，确保能够及时报告安全事件。

（四）外部访问者

应该控制外部访问者访问系统的权限。外部访问者不能对单位工作区、信息或系统进行未经授权的访问。对于需要访问机密、关键信息或处理信息的系统的访问者，应与他们签署保密协议。

（五）员工调转和解聘

单位应将员工、用户职责或聘用状况的变更及时通知相关的系统管理人员。在员工离开岗位之前，单位应：

1.为即将离职的员工重新分配职责和信息资产责任权限；

2.确保指定的继任者能够从该员工处获得与该岗位相关的资料和信息；

3.收回所有单位文档、分发的钥匙和借走的办公设备(例如台式计算机、笔记本电脑、存储设备、文件等)；

4.必须取消即将离任员工进入敏感信息处理区域的权限，删除其相关访问权限。

（六）信息处理设备使用管理的策略

1.单位应向所有单位员工、合同工和临时工提供足够的警告信息，禁止滥用系统计算资源；

2.单位仅为员工提供工作所需的信息处理设备；

3.单位禁止使用系统资源访问含有非法信息或内容的网站；

4.单位应确保所有对系统网络和计算资源的使用（包括访问互联网）都必须遵守单位的安全策略和标准及所有适用的本地法律；

5.如果发现员工使用单位系统连接到包含有色情、种族歧视及其他不良内容的网站，必须立即断开这个网站。能够连接到某个网站本身并不意味着允许员工访问这个站点。以下是单位禁止的行为：

（1）使用单位系统网络故意从事影响他人工作和生活的行为；员工应避免可能威胁单位计算机系统和数据文件的安全性、完整性、可用性和功能的行为；

（2）通过单位系统的网络服务传输任何非法的、有威胁的、滥用的的材料；严禁员工在任何属于单位系统的设备或备份媒体上存储这些材料；

（3）使用单位系统的计算机工具、设备和互联网访问服务来从事用于个人获益的商业活动；任何员工出于个人获益目的使用单位系统的设备都会被认为是违反纪律的行为；

（4）使用单位系统服务来参与任何政治或宗教活动；

（5）未经授权，在计算机中更改、拷贝、安装、处理或使用任何类型的计算机软件和硬件；

（6）保留、传播、下载、处理或显示攻击性的或淫秽的材料；如果在单位系统计算机中发现这类材料应立即删除，并将对责任人进行惩罚；

（7）在单位系统网络中传播包含有淫秽内容的笑话（或其他材料）；使用单位系统设备或工具来储存或传输这些材料；

（8）故意传播感染了病毒的文件或程序的行为；

（9）从其它非法的外部计算机向单位系统网络内的计算机传输数据；

（10）保留、拷贝或传播任何违反规章或法律条例的信息、数据或材料；

（11）未经授权进行尝试欺骗任何主机、网络或帐号的验证或其他安全措施的行为，例如访问员工不应访问的数据、探察其他网络的安全性（例如运行 IP 扫描器或类似的工具）和网络通讯，或非授权监控任何计算机系统；

（12）试图干扰任何用户、主机或网络的服务(如拒绝服务攻击)；

（13）使用任何程序、脚本或命令干扰任何其他用户的终端或登录对话，例如使用用于获取其他用户登录信息和口令的程序。

（七）处理从互联网下载的软件和文件

1.使用病毒检测软件对所有通过从非单位系统来源下载的软件和文件进行检查。

2.必须经过授权后才能使用用于信息安全检测的工具。一般来讲，只有信息安全管理部门的工作人员才可以使用这类工具。

3.在授权使用漏洞检测软件或其他可以用于破坏系统安全的工具之前，信息安全管理部门必须研究和确认使用这些工具的必要性。

（八）员工保密协议

所有员工必须在开始工作前，签订单位保密协议。

（九）知识产权

1.尊重互联网知识产权。

2.单位员工在被雇佣期间使用单位资源开发或设计的产品，无论是以何种方式涉及业务、服务或研发的资产，都是单位的资产。

四、物理和环境安全

物理的信息和其他用于存储、处理或传输信息的资产，例如硬件、磁介质、电缆等，对于物理破坏来说是易受攻击。应该将资产放置于恰当的环境中并在物理上保护他们免受安全威胁和环境危害

（一）安全域

应将支持关键或敏感业务活动的信息技术设备放置在安全域中。安全域需考虑如下因素：

1.物理安全边界控制，安全域防护等级应当与安全域内的信息资产安全等级一致；

2.适当的进出控制措施保护；

3.访问权限应该被严格控制；

4.为安全域提供中间传递空间，以避免直接将物品传递到该区域；

5.不应该放置需要经常使用的设备；

6.要保护信息机密性或关键信息不受非授权访问，防止信息由于灾难事件带来的损伤或破坏；在非正常工作时间这些信息应该是不可见和不可访问的；

7.资产的销毁应该通过管理手段适当地授权。

（二）设备安全

对支持关键或敏感业务过程（包括备份设备和存储过程）的设备应该适当地在物理上进行保护以避免安全威胁和环境危险。需考虑如下因素：

1.设备应该放置在合适的位置或加强保护，将被水或火破坏、干扰或非授权访问的风险降低到可接受的程度；

2.对支持关键业务过程的设备应该进行保护，以免受电源故障或其他电力异常的损害；

3.对计算机和设备环境应该进行监控，检查环境的影响因素如温度和湿度是否超过正常界限；

4.对通讯和电力线应该保护，以防被侦听和中断；

5.对设备应该按照生产商的说明进行有序地维护；

6.安全规程和控制措施应该覆盖单位设备的安全性要求；

7.设备包括存储介质在废弃使用之前，应该删除其上面的数据。

（三）物理访问控制

1.定义单位信息处理设施运营范围内物理安全的职责，并分配责任到个人；

2.建立访问控制程序，控制并限制所有对单位系统计算、存储和通讯系统设施的物理访问；

3.出入控制来保护安全场所，确保只允许授权的人员进入；

4.仅限单位员工、维护和物业人员访问单位办公场所、布线室、机房和计算基础设施；

5.每位员工都有责任对没有陪同的不明身份者进行询问；

6.仅在拥有特定的、经批准的目的时才允许访客访问。

7.单位的访客应由专人陪同；

8.所有非单位员工在单位访问期间应一直有人陪同；

9.对所有进入单位的访客都应有访客登记，至少包含以下信息：

（1）姓名；

（2）所在的机构；

（3）接待的单位员工；

（4）进入和离开的日期和时间；

（5）接待人员签名；

10.在进入单位信息设施之前要逐项列出所携带的信息存储媒体和处理设备，并在离开时确认。

（四）建筑和环境的安全管理

1.为了确保计算机处理设施能正确的、连续的运行，应考虑以下威胁：偷窃、火灾、温度、湿度、水、电力供应中断、爆炸物、吸烟、灰尘、振动、化学影响；

2.建立环境状况监控机制，以监控厂商建议范围外的可能影响信息处理设施的环境状况；

3.应在运营范围内安装自动灭火系统；

4.定期测试、检查并维护环境监控警告机制，并至少每年操作一次灭火设备。

（五）数据单位访问记录管理

1.数据管理员每日检查物理访问记录本；

2.物理访问记录应至少保留12个月，以便协助事件调查。

（六）设备和电缆安全

1.建立并维护对设备的访问使用控制程序；

2.专门人员维护并定期核实资产报表中与每个系统有关的所有设备清单；

3.应明确标记所有设备；

4.单位建立设备运出单位的控制程序，控制单位设备的运出及归还；

5.对于敏感的或重要的信息媒介，须进行以下控制：

（1）安装有外壳的电缆管道，并锁住检查点和终止点的房间或盒子；

（2）定期清除连在电缆上的非授权设备。

（七）设备装载、处置或重新使用

1.未经授权的人员不得从建筑外部访问卸载设备的区域；

2.从卸载设备地区移动到使用点的过程中，应对其进行潜在风险的检查；

3.单位应建立程序来规范来料从入口处移动至其位置的过程。

五、计算机和网络的运行管理

为了保护系统些信息的安全性，需要使用安全和受控的方式管理和操作这些计算机，使它们拥有充分的资源。

用于处理和存储信息的计算机系统都是通过网络联接到外部网络的。由于使用这样的计算机系统，网络必须用可控和安全的方式来管理且拥有充足的资源。网络软件、数据和服务的完整性和可用性必须受到保护。信息通过网络传输，应该确保机密性。

（一）操作规程和职责

制定管理和操作所有计算机和网络所必须的职责和规程，来指导正确和安全的操作。这些内容包括：

1.数据文件处理，包括验证网络传输的数据；

2.对计划系统开发、维护和测试工作的变更管理规程；

3.为意外事件准备的错误处理和意外事件处理过程；

4.问题管理，包括记录所有网络问题和解决办法（包括怎样处理和谁处理）；

5.事故管理；

6.为新的或变更的硬件或软件，制定包括性能、可用性、可靠性、可控性、可恢复性和错误处理能力等方面的测试/评估；

7.日常管理活动，例如启动和关闭规程，数据备份，设备维护，计算机和网络管理，安全方法等；

8.当出现意外操作或技术难题时的技术支持合同；

9.为降低计算机或网络有意或无意的系统误用的风险；

10.职责分离；

11.开发、测试系统与运行系统隔离；

12.使用第三方来管理信息的建议应该判别是否有任何安全隐患，并且应该有详细的适当安全控制措施的说明；

13.计算机和网络操作者应对所有做过的工作进行日志记录维护；

14.频繁的、定期的或特殊的网络故障应被报告和调查；

15.开发、应用统一的安全管理平台；

16.应该维护所有软件及所使用的机器的许可证，并及时更新。

（二）操作变更控制

1.控制对信息处理设备和系统的变动；

2.应落实正式的管理责任和措施，确保对设备、软件或程序的所有变更得到满意的控制；

3.操作程序应严格控制变动。更改程序时，应保留包含所有相关信息的审计日志。改变操作环境可能会对应用程序造成影响。在适当的时候，应结合操作步骤和应用更改控制步骤。

（三）系统计划编制和批准

与系统计划编制和批准相关的所有项目应该采取安全措施。应该监控和估计当前和将来的需求，以便取得先机并且避免由于计算机或网络资源不足产生的问题。应该建立新建系统的批准准则，并在批准前进行适用性测试。应该对计算机系统和网络设备的变更进行有效控制。

（四）软件和信息保护

应采取措施预防和检测对软件和信息非授权的更改。应当采取病毒检测和预防措施以及适当的用户意识培养规程。使用正式的变更控制规程来规范对产品软件和数据的更改。

（五）介质的处理和安全性

应该对计算机介质进行控制，如果必要的话需要进行物理保护：

1.可移动的计算机介质应该受控；

2.制定并遵守处理包含机密或关键数据的介质的规程；

3.与计算相关的介质应该在不再需要时被妥善废弃；

4.系统文档应该进行适当分级并实施保护以防非授权访问或删除。

（六）维护完整性和可用性

应该采取措施维护服务的完整性和可用性：

1.应该建立控制备份计算机和网络的规程；

2.应该定期检查办公网络的网络管理单位和节点的通讯软件和数据的完整性；

3.所有网络设备应受到保护以避免物理攻击；

4.线缆应采取物理保护措施以防止中断、侦听和非授权访问；

5.应该考虑将大型网络分割为分离的、受保护的逻辑域。

（七）鉴别和网络安全

鉴别和网络安全包括以下方面：

1.网络访问控制应包括对个人的识别和鉴定；

2.用户连接到网络的能力应受控，以支持业务应用的访问策略需求；

3.专门的测试和监控设备应被安全保存，使用时要进行严格控制；

4.通过网络监控设备访问网络应受到限制并进行适当授权；

5.应配备专门设备自动检查所有网络数据传输是否完整和正确；

6.应评估和说明使用外部网络服务所带来的安全风险；

7.通过公共网络或其他远程网络进行连接的远程用户应被授权和加密；

8.应考虑共享网络的路由控制；

9.根据不同的用户和不同的网络服务进行网络访问控制；

10.对 IP 地址进行合理的分配；

11.关闭或屏蔽所有不需要的网络服务；

12.隐藏真实的网络拓扑结构；

13.采用有效的口令保护机制，包括：规定口令的长度、有效期、口令、规则或采用动态口令等方式，保障用户登录和口令的安全；

14.应该严格控制可以对重要服务器、网络设备进行访问的登录终端或登录节点，并且进行完整的访问审计；

15.严格设置对重要服务器、网络设备的访问权限；

16.严格控制对重要服务器、网络设备进行访问的人员；

17.保证重要设备的物理安全性，严格控制可以物理接触重要设备的人员，并且进行登记；

18.对重要的服务器必须设置自动锁屏或在操作完成后，必须手工锁屏；

19.严格限制进行远程访问的方式、用户和可以使用的网络资源；

20.接受远程访问的服务器应该划分在一个独立的网络安全域；

21.根据单位系统的运行特点、业务特点和信息资产的归类情况，在单位的网络运行环境中划分不同的网络安全域；

22.安全隔离措施必须满足国家、行业的相关政策法规；

23.个人终端用户（PC 个人计算机）的鉴别，以及连接到所有办公网络和服务的控制职责，由信息安全管理部门决定。

（八）数据交换

无论单位内部还是与外部的数据和软件交换都应受控：

1.应签订协议，描述数据和软件交换中所有要使用的安全控制措施；

2.保护介质，以防在传输过程中丢失或误用；

3.应考虑减少与电子邮件相关的业务和安全风险的控制措施；

4.应制定并执行用来控制与电子办公系统相关的业务和安全风险的明确的策略和指南。

（九）操作人员日志

操作人员应保留日志记录。根据需要，日志记录应包括：

1.系统和应用启动和结束时间；

2.系统和应用错误和采取的纠正措施；

3.所处理的数据文件和计算机输出；

4.操作日志建立和维护的人员姓名。

（十）错误日志记录

对错误及时报告并采取措施予以纠正。应记录用户报告的关于信息处理错误或通信系统故障。应有一个明确的处理错误报告的规则，包括：

1.审查错误日志，确保错误已经得到满意的解决；

2.审查纠正措施，确保没有违反控制措施，并且采取的行动都得到充分的授权。

（十一）网络安全管理

网络安全管理的目标是保证网络信息安全，确保网络基

础设施的可用性。特别是加强跨越单位系统边界的网络安全管理；网络管理员应确保系统的数据安全，保障连接的服务的有效性，避免非法访问。应该注意以下内容：

1.应将网络的操作职责和计算机的操作职责分离；

2.制定远程设备（包括用户区域的设备）的管理职责和程序；

3.应采取特殊的技术手段保护通过公共网络传送的数据的机密性和完整性，并保护连接的系统，采取控制措施维护网络服务和所连接的计算机的可用性；

4.信息安全管理活动应与技术控制措施协调一致，优化业务服务能力；

5.使用远程维护协议时，要充分考虑安全性。

（十二）信息和软件交换

为防止单位系统与其它系统交换信息时信息受到破坏、修改或滥用。应控制信息和软件的交换，并制定相关规定。

为了便于系统内部和外部之间以电子方式或手工方式交换信息和软件，应该签署协议，必要时还包括软件第三方协议。这些协议的内容应反映有关系统中信息的保密程度。协议应考虑的安全条款有：

1.传播、发送和接收的管理责任；

2.发送、传输、和接收的步骤程序；

3.打包和传输的最低技术标准；

4.投递者标识标准；

5.丢失数据的责任和偿还；

6.对敏感或关键信息使用认可的标记方法，确保标记方式易于理解并且信息得到妥善保护；

7.信息和软件的所有权以及数据保护的责任、软件版权规定等；

8.保护敏感数据需要的特殊控制措施，例如加密密钥。

（十三）电子邮件安全

单位应制定关于使用电子邮件的策略，包括：

1.对电子邮件的攻击，例如病毒、拦截；

2.不违反国家、单位相关规定的责任，例如发送诽谤电子邮件、进行骚扰或非法采购；

3.必要时，使用相关技术保护电子邮件的机密性、完整性和不可抵赖。

（十四）病毒防范策略

1.病毒防范主要包括预防和检查电脑病毒（包括实时扫描/过滤和定期检查）。主要内容包括：

（1）控制病毒入侵途径；

（2）安装可靠的防病毒软件；

（3）对系统进行实时监测和过滤；

（4）定期杀毒；

（5）及时更新病毒库；

（6）及时上报；

（7）详细记录。

2.制定可行的“防病毒管理制度”，该制度适用于单位系统的所有使用者；防病毒软件的安装和使用由单位专门的防病毒管理员执行。

3.采用全网防病毒体系，并安装相应的防病毒套件。

4.严格控制盗版软件及其它第三方软件的使用，必要时，在运行前先对其进行查毒。

5.单位员工因为上不安全的网站下载东西或其他方式导致中毒，造成的后果由其本人负责。

（十五）互联网安全策略

互联网安全策略范围包括单位互联网安全域内的服务器及其相关应用。

1.所有接入互联网安全域的服务器、网络设备（包括：交换机、路由器等）必须经过严格的审批。

2.对互联网安全域的服务器、网络设备（包括：交换机、路由器等）配置的改变必须经过严格的审批。

3.只提供必须的网络服务。

4.及时安装软件、应用系统补丁包。

5.对网络攻击进行实时的监控和响应。

6.对操作系统、应用软件进行安全配置。

7.互联网安全域安全措施由专门的系统管理员和安全管理员负责执行，单位信息安全管理机构负责监督和审查执行情况。

8.做好 WEB 网页的备份与恢复工作，防止网页被篡改。

9.定期对互联网安全域的服务器、网络设备（包括：交换机、路由器等）的运行状况进行检查和审计。

10.采用适当安全隔离措施，单位互联网安全域应该采用自主可控的防火墙使之与互联网和内部的核心业务网络进行安全隔离。

（十六）备份与恢复

定义单位系统备份与恢复应该采用的基本措施。

1.建立有效的备份与恢复机制。

2.明确备份的操作人员职责、工作流程和工作审批制度。

3.建立完善的备份工作操作技术文档。

4.明确恢复的操作人员职责、工作流程和工作审批制度。

5.建立完善的恢复工作操作技术文档。

6.针对建立的备份与恢复机制进行演习。

7.对备份的类型和恢复的方式进行明确的定义。

8.妥善保管备份介质。

（十七）入侵检测

对网络攻击以及未经授权的访问进行及时的响应。

1.根据需要，针对系统的具体应用和操作系统配置入侵检测系统。

2.正常运行的入侵检测系统必须由专人负责，相关规则属于秘密信息，不得外传，否则，将承担法律责任。

3.由专人负责入侵检测系统软件归档入库以及登录、保管等工作。

4.由专人负责入侵检测系统软件拷贝和资料印刷等工作。

5.由专人负责入侵检测系统的安装、调试及卸载等工作。

6.定期查看入侵检测系统日志记录，并做备份。

7.如发现异常报警或情况需及时通知相关负责人。

8.运行于本网络的入侵检测系统的各条规则设计，均需由单位安全管理部门领导批准并登记在案，方可进行。

9.及时升级入侵检测系统。

（十八）加密

1.对于应用系统安全需求分析中要求采用加密措施，或相关法规中要求采用加密措施的处理，一定要满足要求。

2.采用加密技术或选用加密产品，要求符合国家有关政策或行业规范的要求。

3.选用的加密机制与密码算法应符合国家密码政策，密钥强度符合国家规定。

4.对于敏感或重要信息，要求通过加密保障其私密性、通过信息校验码或数字签名保障其完整性、通过数字签名保障其不可否认性。

5.要求采用高强度的密钥管理系统，保证密钥全过程的安全。包括密钥的生成、使用、交换、传输、保护、归档、销毁等。

6.对敏感或重要密钥，要求分人制衡管理。

7.对敏感或重要密钥，要求采用一定的密钥备份措施以保障在密钥丢失、破坏时系统的可用性。

8.密钥失密或怀疑失密时，必须及时向安全主管部门报告，更新密钥。并采取有效措施，防止再次发生类似情况。

六、访问控制

为了保护系统中信息不被非授权的访问、操作或破坏，必须对系统和数据实行控制访问。

系统控制访问包括建立和使用正式的规程来分配权限，并培训员工安全地使用系统。对系统进行监控检查是否遵守所制定的规程。定义和分配用户访问权限是系统所有者的职责。

（一）应用程序访问控制

访问系统和数据应受控：

1.定义并文档化访问控制业务需求。

2.对授权访问用户标识其唯一性，并对其行为在应用层实现审计功能。

3.应根据所定义的业务需求，授权对数据和计算机系统的访问。

4.应定期检查用户访问权限。

5.访问系统功能应受限和受控。

6.访问源程序库应受限和受控。

7.应为关键系统和应用考虑使用隔离的计算环境。

（二）计算机访问控制

应根据相关的国家法律的要求和指导方针控制对系统和数据的访问：

1.计算机活动应可以被追踪到个人。

2.访问所有多用户计算机系统应有正式的用户登记和注销规程。

3.应使用有效的访问系统来鉴别用户。

4.应通过安全登录进程访问多用户计算机系统。

5.特殊权限的分配应被安全地控制。

6.用户选择和使用密码时应慎重参考良好的安全惯例。

7.用户应确保无人看管的设备受到了适当的安全保护。

8.应根据系统的重要性制定监控系统的使用规程。

9.必须维护监控系统安全事件的审计跟踪记录。

10.为准确记录安全事件，计算机时钟应被同步。

（三）帐号管理

应根据“必须知道”原则控制和限制对系统资源、敏感工具和数据资源的访问。

1.业务和职能单位应建立并归档帐号注册和注销过程。

2.每个业务和职能单位都应负责对其系统授予访问权限。

3.如果员工和第三方的状态发生了变化，则必须在变化的24小时内更改其访问权限。

4.业务和职能单位应建立并归档处理机制，每3个月检查一次批准的帐号及其访问权限。

5.如果需要紧急帐号，则应该：

（1）经由信息安全管理部门批准。

（2）经记录并批准后使用。

（3）仅使用一次。

（四）口令管理

1.管理员职责

对于 administrator 或 root/超级用户帐号的访问，管理员也仅仅是基于工作需要时才被允许而不是基于主观判断。以下是有关使用口令方面不可接受的行为：

（1）泄漏口令，包括将其张贴出来。

（2）监控任何网络中的口令。

（3）非授权尝试访问存储的口令。

（4）收集其他人的口令。

（5）暴力猜测口令。

2.口令安全

应根据以下要求确保口令安全：

（1）在计算机等常驻的口令必须是加密格式的。

（2）在登陆输入口令过程中不能以任何方式显示口令。

（3）如果可能的话，通过网络的口令应加密。

（4）应将允许特权访问(比如“管理员”、“root”或“系统”功能)的帐号严格限制于完成管理功能所需的最少人数。

（5）如果终止雇佣管理用户，应更改这位用户可以访问的所有管理口令。

（6）应将对这些特权口令的访问记录归档，且这些访问应基于经证明的工作需要。

3.口令选择

口令必须满足所有以下标准：

（1）Windows 系统最少口令长度为 7 个字符，Unix 系统最少为 8 个字符。如果可能的话，Windows 系统特权帐号口令应为 14 个字符，Unix 系统应为 8 个或 8 个以上字符。

（2）至少 1 个字符必须为符号。

（3）至少 1 个字符必须为数字。

（4）口令应区分大小写(至少 1 个字符为大写，至少 1 个为小写)。

（5）口令中禁止包含人名或登陆标识符。

（6）不应使用常见的或字典词语。

（7）系统和应用程序管理员负责在创建帐号时为最终用户选择好的口令。最终用户负责在更改口令的时候选择好的口令。

（8）严禁共享一般用户帐号口令。

（9）必须仅基于“必须知道”才能允许使用系统帐号口令。

（10）如果必须给予外部单位(比如厂商支持工程师)系统帐号口令的话，则在外部单位完成工作时必须更改口令。

4.口令过期

（1）必须在 90 天后终止不使用的帐号。

（2）必须每 90 天更改一次口令。如果给定的口令已超过 90 天，则必须锁定帐号。

（3）必须每 30 天更改一次系统帐号口令(比如 root，管理员)。

（4）建议可以访问系统帐号的人员每 30 天更改一次他们的用户口令。

（5）在口令过期前 2 周提醒用户。

5.口令恢复

（1）严禁重新使用口令。所有系统都必须配置为禁止重新使用口令。

（2）不允许口令恢复。如果用户忘记了口令，授权的管理员必须根据文中的规定为最终用户重置口令。

6.口令发布

口令发布包括向期望的和授权的用户最初及此后的口令交付。

（1）严禁通过电子邮件发布口令。

（2）应只通过直接的或电话联络发布口令。仅在确认了用户身份后才能发布口令。

（3）在为新用户帐号初次创建口令时，必须强迫用户在第一次登陆对话时更改口令。

（五）权限管理

特权帐号(例如 root)的分配和使用必须是经过授权的、受限的、分隔的、且是可控的：

1.单位应对特权用户 ID 建立归档的授权过程。权限分配必须遵守“必须使用”和“逐个分析”的准则。

2.为用户分配的特权用户 ID 必须与普通业务使用的 ID 不同。

3. 单位应建立已归档的处理机制，最少每3个月检查一次特权帐号及其访问权限。

4.仅在以下条件下使用特权帐号：

（1）具有特定的时间范围。

（2）对单位系统本地网络范围内或远程访问用户，职能单位应至少每周进行一次对特权用户行为的审计记录的检查和维护。

七、系统开发和维护

安全特性应从系统的规划阶段开始考虑。在开发或采购系统之前应考虑安全需求。特别地，应该对系统文件、源代码和执行代码的访问进行控制。

（一）系统的安全需求

在开发和采购系统安全控制措施及产品之前应识别和批准系统安全需求。应在每个开发或采购项目的需求分析阶段描述信息安全问题。

（二）系统的安全

系统应当设计恰当的安全控制措施：

1.为保证信息完整性应进行定期检查。

2.危险的信息进入系统时应确认输入的正确性。

3.系统处理的信息应由系统的控制措施进行验证。

4.对可能会被恶意修改并用来进行信息传输的应用程序，应考虑使用加密及消息校验系统。

（三）系统文件的安全

访问系统文件、源代码和执行代码应进行控制：

1.只要可能，软件测试不应在正在使用的数据或系统上进行。

2.测试数据应受保护和控制。

3.禁止对系统文件的非授权访问。

（四）开发和支持环境的安全

1.开发和支持环境应严格受控。

2.应有正式的系统软件和数据的变更控制规程。

3.当操作系统发生变更，可能会对安全性和功能产生任何影响时应检查应用程序。

（五）软件开发和维护

1.严格管理软件开发的过程；软件开发与维护管理遵循相关技术规范如GB/T8566《计算机软件开发规范》与GB/T8567《计算机软件产品开发文件编制指南》。

2.软件开发与维护的过程文档遵循相关规范要求，并统一归档。

3.如果要求第三方协作开发或软件外包，选择具有相关资质的软件开发商。并就涉及到单位的秘密事宜签订保密协议。

4.提供系统设计阶段的风险分析报告和安全设计报告，在系统需求分析阶段引入安全需求，并将安全需求延续到系统设计与实施中。

5.系统开发过程中的安全设计要求考虑并验证用户的输入及输出，定义系统资源的安全属性与级别，对用户进行标识与鉴别，严格权限管理和访问控制机制。

6. 确保由合法用户提出的业务和安全需求以及修改请求。

7. 严格开发与运行维护隔离的措施。运行系统应只有执行代码。

8. 运行程序库的更新要有日志记录，记录所有软件更新的版本控制。软件的旧版本应保存，并保护及控制测试数据。

9. 测试环境必须与生产环境严格隔离，在应用系统软件安装前进行测试。软件测试过程中对访问控制功能进行严格的测试。测试数据不得进入生产环境。

10. 源程序库的维护及拷贝应有严格的更改管理制度，源代码不得保留在生产系统。严格控制技术人员访问源程序库，并记录所有对源程序库的访问。

11. 及时响应系统运行过程中出现的安全漏洞或隐患，并提出解决方案。

八、个人计算机和信息安全

个人计算机（PC）的使用，由于其轻便和容易取得，给系统带来严重的威胁。员工应被告知使用个人计算机带来的风险并进行相关的安全意识和技术培训：

1. 个人计算机应妥善保护以避免非授权使用。

2. 在个人计算机使用前应该对包括供应商提供的所有盘片进行病毒检测。

3. 员工应通过正确的渠道尽快报告任何个人计算机出现的异常行为。

4. 个人计算机上应该永久安装病毒检测软件。

5. 由于游戏文件经常被用来传播病毒、Trojan 木马程序，所以应禁止在系统的个人计算机上玩游戏。

6. 只有经批准的软件（无论私有软件、共享软件、公共域的软件还是自由软件）可以传入个人计算机。

7. 应该对个人计算机进行定期审计，保证遵守软件许可和授权需求。

8. 系统的个人计算机未经批准不能更换硬件。

9. 旅行时，员工应该特别小心保护手提电脑和任何关联设备。

九、风险管理

风险管理对于帮助单位相关员工识别和理解信息被攻击、更改和不可用所带来的（直接和间接的）潜在业务影响来说至关重要。所有信息资产和 IT 过程应通过风险评估活动来识别与它们相关的安全风险并执行适当的安全对策。系统的信息安全风险评估活动应当定期执行，特别是系统建设前或系统进行重大变更前，也必须进行风险评估工作。风险评估活动应该根据单位所制定的管理制度和指南进行。

十、业务连续性管理，恢复

（一）业务连续性管理的特点

1. 业务连续性管理的目标是防止业务活动中断，保证重要业务流程不受重大故障和灾难的影响。

2. 应该实施业务连续性管理程序，将预防和恢复控制措施相结合，将灾难和安全故障（可能是由于自然灾害、事故、

设备故障和蓄意破坏等引起）造成的影响降低到可以接受的水平。

3.应该分析灾难、安全故障和服务损失的后果。制定和实施应急计划，确保能够在要求的时间内恢复业务的流程。应该维护和执行此类计划，使之成为其它所有管理程序的一部分。

（二）业务连续性管理程序

应该制定维护业务连续性的管理流程。包括以下主要内容：

1.考虑突发事件的可能性和影响，包括确定重要业务流程及其优先级别。

2.了解中断系统服务可能对业务造成的影响（必须找到适当的解决方案，正确处理较小事故以及可能威胁组织生存的大事故），并确定信息处理设施的业务目标。

3.适当考虑风险处理措施，可以将其作为业务连续性程序的一部分。

4.定期对业务连续性管理的计划和流程进行检查和更新。

5.确保在组织的程序和结构中纳入业务连续性管理。业务连续性管理流程的协调责任应该在系统管理部门进行适当分配。

（三）业务连续性和影响分析

1.要确保业务连续性，应该首先确定可能引起业务流程中断的事件，如设备故障、水灾和火灾等。然后，进行风险

评估，确定中断可能造成的影响（破坏程度和恢复时间）。这两项活动都应让具体业务的责任人完全参与。

2.应该根据风险评估结果制定相应的战略计划，确定业务连续性总体方案。计划制定后应该由管理层进行批准。

（四）编写和实施连续性计划

应该制定计划维护业务运作，或在重要业务流程中断或发生故障后在规定时间内恢复业务运作。业务连续性计划和程序应该考虑以下内容：

1.确定并认可各项责任和应急程序。

2.执行应急程序，以便在规定时间内进行恢复。要特别注意对有关外部业务和合同的评估。

3.商定程序的备案。

4.适当地对技术人员进行培训，让他们了解包括危机管理在内的应急程序；检查并更新计划。

5.计划和程序应着重强调系统的业务目标，如在可接受的时间内恢复必要的服务。为此，应该考虑所需的服务和资源，包括人员、非信息处理资源等。

（五）业务连续性计划框架

应该对业务连续性计划的框架进行维护，保证所有计划前后一致，确定测试和维护的优先级别。每个业务连续性计划都应该详细说明计划执行的条件以及执行计划的负责人员。确定新的要求时，应该对已制定的应急程序适当进行修改。

业务连续性计划框架应该考虑以下内容：

1. 计划执行条件。

2. 应急程序。

3. 恢复程序。

4. 说明计划检查方式和维护安排。

5. 宣传培训活动。

6. 个人责任。

7. 每个计划都应该有一个负责人。应急程序恢复计划也应该由相关的技术人员负责。

（六）业务连续性计划的检查、维护和重新分析

业务连续性计划常常由于错误估计、疏忽或者设备（人员）的变化可能无法通过检查。因此，应该对计划进行定期检查，保证其可实施性和有效性。进行此类检查时，还应该保证负责进行恢复的所有小组成员以及其他相关人员对计划有一定的了解。

业务连续性计划的检查计划应该说明各部分计划的检查方式和时间。

应该通过定期审议和更新对业务连续性计划进行维护，确保其始终有效。应该在组织的变更管理计划中采用适当程序，确保业务连续性问题得到适当处理。

应该分配各个业务连续性计划的定期评审责任；业务连续性计划更新后，应该检查还有哪些业务安排尚未在该计划中得以反映。该正式变更控制程序还应该确保把更新计划分发下去，在对完整计划完成定期审议后还需要更新计划。

十一、符合性

系统必须符合国家法律和法规的要求[8]-[17]。

系统执行所有必要的控制措施，避免违背所有法定的、关键的义务和安全需求。

（一）软件的使用

在系统中，不允许使用非法的软件，不经版权所有者的同意就拷贝任何版权资料。

（二）防止滥用 IT 工具

系统中的 IT 工具都是为特定业务目的而提供的。禁止任何部门和个人的 IT 工具用以非业务或未经授权的目的，一旦查出必须立即报告给各级负责人并进行处罚。

（三）符合安全策略和标准

1.系统中，所有的区域都应定期检查，以确保与安全策略和规程保持一致，系统的所有者和系统、应用的管理员必须尽力协助执行安全审查，同时鉴别并执行必要的纠正措施。

2.为了将风险带来的危害最小化，安全审计的要求和行为必须经过仔细计划并获得批准。

参考标准及法规

[1]国家标准 GB/T18336《信息技术安全技术信息安全评估通用准则》

[2]国家标准 GB9361-1988《计算机场地安全要求》

[3]国家标准 GB2887-2000《电子计算机场地通用规范》

[4]国家标准GB50174-1993《电子计算机机房设计规范》

[5]国家标准GB9254-1998《信息技术设备的无线电骚扰限值和测量方法》

[6]国家保密标准BMB2-1998《使用现场的信息设备电磁泄漏发射检查测试方法和安全判据》

[7]国家保密标准BMB3-1999《处理涉密信息的电磁屏蔽室的技术要求和测试方法》

[8]《互联网信息服务管理规定》

[9]《计算机软件保护条例》

[10]《计算机系统安全专用产品检测和销售许可证管理办法》

[11]《计算机系统保密管理暂行规定》

[12]《商用密码管理条例》

[13]《涉及国家秘密的通信、办公自动化和计算机系统审批暂行办法》

[14]《国家信息化领导小组关于加强信息安全保障工作的意见》

[15]《中华人民共和国计算机系统安全保护条例》

[16]《互联网信息服务管理办法》

[17]《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》