高新兴科技集团股份有限公司

受　　控

信息安全管理制度

文件编号：GSB／T 306.02

文件版本：A2

批　　准：刘伟辉

实施日期：2015-10-31

受控状态：受控

版本记录

版本	日期	修订页次	制/修订记录	制/修订者
A0	2013-12-12	/	新版制定	罗建明
A1	2014-10-19	13	“第十五章　应急安全管理”有部分内容修改	罗建明
A2	2015-10-31	11	“第十四章 项目建设安全管理”部分内容有修订	李旻

目　　录

信息安全管理制度

第一章 总则

第一条 为了加强高新兴科技集团股份有限公司信息安全管理,保障各种信息资产的机密性、完整性和可用性，特制定本管理办法。

第二条 本规程适用于公司信息资产各要素（包括：人员、数据、网络、终端等）的安全管理，全体员工在涉及到信息安全时应遵照执行。

第三条 本规程的最终解释权归高新兴科技集团股份有限公司信息安全管理委员会。

第四条 本规程使用以下术语定义：

(1) 信息安全：指信息的机密性、完整性和可用性的保持。

机密性：确保只有那些被授予特定权限的人才能够访问到信息。

完整性：要保证信息和处理方法的正确性和完整性。

可用性：确保那些已被授权的用户在他们需要的时候，确实可以访问得到所需信息。

(2) 信息安全管理：规定机制，使信息安全得以执行。

(3) 设备：包括服务器、存储设备、终端、网络设备、安全设备等。

(4) 风险评估：对信息、信息处理设施、信息处理过程和信息系统管理所受威胁、系统弱点保护不当等风险因素的发生可能性和后果影响的资产价值评估。

(5) 资产：指被组织赋予了价值，组织需要保护的有用资源。

(6) 内部计算机网络：指 U9 财务系统网、OA 办公网等在内的全部内部网络。

(7) 安全事件：任何已经发生的或可能发生导致信息安全受到损害的行为，或是违反安全程序的行为。

第二章 安全组织和人员职责描述

第五条 公司信息化安全实施统一领导、专业分工负责的原则。

由信息安全管理委员会负责全公司的信息安全指导和运行管理。办公室负责具体工作的执行。

第六条 信息安全管理委员会职责

1、负责审定公司信息安全项目规划和工作计划，布置信息安全工作任务，研究决定相关重大事项。

2、负责传达与贯彻上级有关信息安全方针政策，审批公司信息安全管理各项规章制度。

3、负责本公司信息系统安全重大事项决策和协调工作。

4、具体负责公司系统信息安全工作。

5、负责组织监督信息安全保障体系相关工作

第七条　网络管理员职责

1、负责防病毒管理、防火墙系统管理、入侵检测管理、安全漏洞扫描管理等；

2、参与网络系统安全策略、计划和事件处理程序的制定；

3、承担网络安全事件的处理；

4、参与网络安全建设方案制定；

5、负责网络设备操作系统升级、补丁；

6、负责网络日常监控、优化和安全加固；

7、负责网络设备操作系统和配置数据备份。

第八条　数据库系统管理员职责

1、参与数据库系统安全策略、计划和事件处理程序的制定；

2、承担数据库系统安全事件的处理；

3、负责数据库系统升级、补丁和和安全加固；

4、负责数据库系统的日常安全监控、配置和数据备份；

5、负责数据库系统权限和口令管理。

第九条　操作系统管理员安全职责

1、参与操作系统系统安全策略、计划和事件处理程序的制定；

2、承担操作系统系统安全事件的处理；

3、负责操作系统系统的升级、补丁和安全加固；

4、负责操作系统的日常安全监控和操作系统和文件系统的备份；

5、负责操作系统权限和口令管理。

第十条　系统管理员的安全职责

1、参与应用系统安全策略、计划和事件处理程序的制定；

2、承担应用系统安全事件的处理；

3、负责应用系统的安全加固；

4、负责应用系统的日常安全监控和数据备份；

5、负责应用系统帐号权限和口令管理；

6、负责应用系统在操作系统和数据库中帐号及该帐号下数据安全。

第十一条 资产管理员的安全职责

1、按照资产存放环境要求存放相关物资和资料；

2、根据信息资产的分类分级标识的要求进行资产、资料的标识；

3、根据资产的信息安全等级进行物资的入库、出库、销毁，资料的保管、借阅、销毁；

4、资产管理员应特别注意以下内容的安全管理：系统备份、数据备份载体及相应文档管理；业务数据、经营数据、运行数据的载体及相应文档的管理；软件资料管理（包括软件开发的源代码、软件设计说明书、使用说明书、许可证等)；硬件随机文档；系统设计方案、工程施工过程文档、系统运行维护文档、招投标过程文档；其它文档管理（包括各种规章制度、收发文、工作日志归档、设备清单、合同）等等。

第三章 资产安全管理

第十二条 为了保证信息资产得到适当的保护，应该对信息分类分级，指明其保护级别；将信息资产分为不同的安全防护等级，有助于“应级而异”地规划、设计、实施相关的信息资产安全管理和保护措施,从而更有效地保障信息资产的机密性、完整性和可用性。

第十三条 数据在信息资产中占有非常重要的地位，通常作为企业知识产权、竞争优势、商业秘密的载体。属于需要重点评估、保护的对象；数据分类标签的对象包括各种存储介质、磁带、软盘以及其他介质，所有印刷的、手写的敏感信息都需要考虑在恰当的位置放置标签。

第十四条 信息资产的存放

1、物理资产的存放地点应通风良好，温湿度适宜并有消防安全设施；

2、对于存放有特殊要求信息资产应存放在其所需的存放环境中，以防数据丢失；

3、定期进行资产存放环境的检查和清洁，对不符合存放要求的情况应作出整改。

第四章 用户帐号与口令安全管理

第十五条 口令中至少应包括以下三种：数字、大写字母、小写字母以及特殊字符（特殊符号举例如下：!@#$%^&*()_+|~-=\`{}[]:”;’<>?,./）；口令长度不应小于 8 位。

第十六条 新增用户：必须由申请小组提出正式申请，需填写相关信息：使用者的姓名、联系电话、职责（岗位）、MAC 地址、使用时间、申请使用的系统范围和权限等信息。由部门经理审批后移交给信息安全管理委员会办公室，审核后，下发至相应的管理员，管理员根据申请的内容进行赋权；操作完成后，系统管理员通过邮件或其他安全方式通知相关人员或部门。

第十七条 注销用户：由于人事变动，帐号的使用者发生岗位变动或者离职，人事部门发报人事变更讯息，通知至系统管理员所在小组。由系统管理员提出正式申请经系统所在部门经理审批后，立即进行相应的权限变动或帐号回收，严格防止由于岗位变动，帐号、权限没有进行变更的情况。

第十八条 系统管理员负责对应用系统、网络、服务器或其他信息设备的用户帐号、权限进行管理。对用户帐号和权限进行登记备案，至少每半年审核一次用户帐号的使用情况，对长期未使用的或过期的帐号进行清理。

第十九条 对系统、网络、数据库、信息的访问采用分级管理，根据人员职责设定权限； 仅有操作系统管理员及 DBA 拥有数据库的写权限；应用系统管理员只能拥有相关数据库的读权限；超级用户权限只允许操作系统及数据库管理员使用，其他用户需要使用超级权限时需提出申请，经审批后，由数据库管理员作一次性授权，并在数据库管理员监督下操作。

第二十条 员工只能拥有本岗位内的权限，且采取最低可用原则配置；如因工作需要另外增加岗位外权限的，需要领导审批；经使用员工所在小组主管和信息安全工作组同意后方可增加，增加后要保留操作日志和审批记录；禁止使用系统内置帐号进行应用系统数据的维护工作；严禁使用数据库内置帐号的口令进行数据库管理。

第二十一条 用户应记住自己的帐号、口令，不允许记载在不保密的媒介物或贴在终端上。同时，避免泄漏口令，不要将口令告诉其他人。如果发现口令泄漏，应立即通知系统管理员及时更改；用户通过公网连接到公司内部网站时，需注意帐号、口令的保密，避免在公共场所泄漏帐号、口令。

第六章 网络安全管理

第二十二条 网络配置管理

1、所有的网络配置工作都要有文档记录，网络设备的配置文件需要定期备份；

2、按照最小服务原则为每台基础网络设备进行安全配置；

3、网络需保持持续不断的运行，维护工作要在用户使用量小的时候进行。

第二十三条 网络监控管理

1、网络管理小组负责网管系统和网络安全的建设和维护，以实现对网元以及网络安全情况的实时监控和管理，确保整个网络安全、稳定运行。

2、各级网络管理部门可使用入侵检测、漏洞扫描等设备和技术定期对网络安全情况进行监控和分析，对于监控到的异常行为要有及时、有效的处理机制。

3、网络管理员负责网络设备的日常检查，监测网络设备性能参数和网络运行状况；对关键设备要做到每日检查，发现问题应迅速解决，全部管理工作应保留记录。

4、定期或不定期对备件及备用线路进行检测和维护。

5、网络安全监控设备的运行不能影响网络的正常使用。

6、各级网络管理部门要对所有在线网络设备运行情况记录登记，并定期向上级上报网络运行状况报告。

第七章 数据安全管理

第二十四条 数据的访问范围和权限设置必须由系统或业务系统管理员集中控制,并可以控制授权范围内的信息流向和行为方式。

第二十五条 数据访问采用分级管理,数据的操作必须经过严格的身份鉴别与权限控制，确保数据访问遵循最小授权原则。关键业务数据和用户帐号信息必须实行专人管理。

第二十六条 数据的更改应严格遵循相关管理办法及操作规范执行。应采取有效措施防止系统数据的非法生成、变更、泄漏、丢失与破坏；重要数据的更改必须两人负责，一人操作，一人审核，防止使用过程中产生误操作或被非法篡改。

第二十七条 应用软件对重要数据应进行传输加密和完整性校验处理;对外提供系统业务数据的统计必须参照数据提取流程进行审批，并签订保密协议，保障数据信息的使用范围可控制。

第二十八条　数据备份应保证及时、完整、真实、准确地转储到不可更改的介质上，并规定保存期限；备份介质应采用性能可靠、不易损坏的介质，如磁带、光盘等，并采取防盗、防毁、防电磁干扰等措施，保障数据安全。

第二十九条　备份数据（包括系统、网络配置文件、应用软件和应用数据信息）应专人统一管理。要建立备份介质保管登记制度，由专人负责。严防业务数据泄密或丢失。

第三十条　定期对备份数据的可用性进行检查。要保证备份数据是可读的，经常对备份介质进行测试；备份数据应做到定期全备份和增量备份。备份内容包括系统备份和数据备份两部分。系统常规备份至少每月一次，关键业务数据备份至少每天一次。

第三十一条　当发现数据丢失后，应保护好现场，停止任何操作，立即通知系统管理员，由系统管理员采取相应恢复措施；如系统管理员不能恢复数据，视数据的重要程度，通知相关领导和信息安全工作组，并联系第三方工程师解决。

第三十二条　备份数据的恢复需经主管人员签字认可后，方可进行；对存储有涉密数据的设备故障，需交外单位人员修理时，本单位必须派专人在场监督；过期的备份数据应经主管人员认可后，方可销毁。

第八章　保密安全管理

第三十三条 数据密级分类原则

数据密级根据其内容重要性的不同，划分为：机密、秘密、内部、公共四个级别。其中，机密、秘密、内部数据属于涉密信息。

(1)　机密数据

机密数据是指那些具有最高安全级别，对企业正常经营、管理和安全运行起到至关重要作用，一旦被非法访问或篡改，会导致灾难性的影响，并且这种影响在短时期内是不可恢复的；或者会严重影响公司业务发展，使公司在市场竞争中非常被动的关键数据。

(2)　秘密数据

秘密数据是指那些必须在企业内使用，并且有严格访问控制的信息。任何对秘密数据的非法访问、修改或删除会严重影响企业内计算机系统的安全，但这种影响是可以在短时期内恢复的；或者会对公司业务拓展产生不利影响但通过努力可以逐渐扭转的数据。

(3)　内部数据

内部数据通常是指那些只供公司内部使用的信息资料，任何对内部数据的非法访问、

修改或删除可能会对企业安全造成一定的影响，但不可能是严重的或不可恢复的。

(4) 公共数据

公共数据是指可以公共访问和对外发布的信息,并且公共数据可以自由散布而不会产生任何安全问题。

第三十四条 涉密数据的获取

1、必须首先经过申请批准，才能查询和阅读文档、数据；

2、严禁复制机密数据。申请复制秘密数据必须部门主管签字批准；

3、信息使用、加工处理部门及网络管理部门，不得通过不正当的手段，超越权限查看、使用、复制保密信息，也不能擅自降低保密级别，把涉密信息作为非涉密信息传播。

第三十五条 涉密数据的传递

1、涉密数据的传递必须经过审批并采用适当的方式进行传递；

2、文档的密级必须清楚地标识在各种电子信息文档的每一页上，或每个电子文件的开始；如果不能标识，原创人必须告知所有接受者数据的密级；

3、涉密数据的披露或分发应当有所记录，涉密数据的分发必须发至收件人本人，并由收件人签收；

4、在对外合作中，如确实需向合作方提供涉密数据的，必须按密级由相应领导书面批准，并在提供前与之签订保密协议；

5、内部公共数据可以按部门分发，也可以在内部计算机网络上发布；

6、机密、秘密数据严禁在计算机网络上发布、公开和传送，内部数据如需在网络上传送，应得到相应领导的批准。

第三十六条 涉密数据保管、存档

1、要加强对计算机介质（软盘、磁带、光盘、磁卡等）的管理，对储存有秘密文件、资料的计算机等设备要有专人或兼职人员操作，采取必要的防范措施，严格对涉密存储介质的管理，建立规范的管理制度，存储有涉密内容的介质一律不得进入互联网络使用；

2、机密、秘密数据由数据的签收人和签发人亲自保管。内部数据由收件人本人或本部门专人保管，内部公共数据一般由各部门专人保管；

3、涉密数据的查阅和复制应当在文件保管人处进行登记，以备核查；4、如涉密数据的保管人不慎将文件丢失，应立即向相应的领导汇报情况，尽快挽回损失，减小影响。

第三十七条 必须签订保密协议，保密协议应包括：保密的内容和范围、保密的期限、

双方的义务、违约责任。

第三十八条 基本保密义务：

1、应当遵守公司的保密制度，妥善保管其所保存的秘密资料，不得刺探与本职工作、本身业务无关的公司秘密，不得泄露公司的技术秘密；

2、非经公司书面同意，不得利用公司的商业秘密进行生产、经营和兼职活动，不得利用公司的商业秘密组建新的企业；

3、如果发现公司秘密被泄露，应当采取有效措施防止泄密扩大，并及时告知公司；

4、无论是在职还是离职，不得披露、使用或者允许他人使用公司的商业秘密，不得利用公司的商业秘密从事兼职活动，不得利用公司的商业秘密到其他单位任职；

5、员工离职时，应当将所持有的秘密资料如数归还公司，不得保留拷贝；

6、员工离职后在约定期限内不得泄露原公司机密。

第九章 防病毒安全管理

第三十九条 管理员要及时了解防杀计算机病毒厂商公布的计算机病毒情报，关注新产生的、传播面广的计算机病毒，并知道它们的发作特征和存在形态，及时发现计算机系统出现的异常是否与新的计算机病毒有关；同时要及时了解操作系统厂商所发布的漏洞情况，对于很可能被病毒利用的远程控制的漏洞要及时提醒用户安装相关补丁；对有严重破坏力的计算机病毒的爆发日期或爆发条件，及时通知所有相关人员进行相应防范。

第四十条 对新购进的计算机及设备，在安装完操作系统后，要在第一时间内安装防病毒软件；没有安装防病毒软件的 Windows 系统不得接入到生产网络中；防病毒软件的类型遵循统一规划，不得私自安装其他类型的软件。病毒特征库至少要做到每天自动升级检查，自动部署；公司要求所有服务器及个人电脑均安装防病毒软件，并至少实现由防病毒软件的服务器端强制所有终端联网后可以自动实时更新病毒库。

第四十一条 尽量使用专杀工具对病毒进行查杀，杀毒完成后，重启计算机，再次用最新升级的防病毒软件检查系统中是否还存在该病毒，如是系统漏洞应及时打上相应补丁，并确定被感染破坏的数据是否确实完全恢复；如果重要数据文件被感染，无法修复，可以请数据恢复的专业人员进行处理。

第四十二条 如果发现本机有感染病毒的迹象，应立刻通知系统管理员，必要时拔掉网线；定期对所有重要敏感数据进行备份；定期对自己的电脑进行杀毒和漏洞扫描。

第十章 电子邮件安全管理

第四十三条 邮件帐号管理

1、帐号口令的设置原则遵循本规程第四章《用户帐号与口令安全管理》；

2、如果确认某个帐号的活动已经威胁到整个系统的安全，应立即禁用此帐号，并第一时间通知用户；

3、网络应能控制用户登录入邮件系统次数，应对所有用户的访问进行审计，如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息；

4、建立口令管理制度。做到口令专管专用、定期更改，失密后立即报告；

5、离职员工在离职日起必须对其持有的公司内部员工邮件帐号进行删除；

6、禁止匿名发送邮件，必须做身份认证。

第四十四条 电子邮件操作

1、用户必须以本人的真实身份使用用于办公用途的电子邮件，禁止以他人名义滥发邮件或盗用他人邮箱。未经授权任何人不得以他人帐户口令进行登录,阅读他人邮件内容；

2、邮箱用户的登录密码（用户口令），必须严格保密，不得泄露，用户使用完邮件系统后，必须立即退出登录，以防他人冒名使用。用户必须使用本人的邮件帐号口令访问系统。如将其借予他人使用，由此造成的一切安全后果由邮件帐号所有人承担；

3、用户若发现任何非法使用该用户帐号或其它系统安全漏洞情况，须立即通告系统管理员；

4、不要阅读和传播来历不明的邮件及附件，提高对于病毒邮件的防范意识，避免传递病毒邮件，具体措施遵循本规程第九章《防病毒安全管理》；

5、用户不得将公司提供的电子邮件地址用于非工作目的(特别是以娱乐、购物、交友等为目的身份注册)，如果受到大量垃圾邮件的困扰应该通知系统管理员；

6、邮件用户必须经常清理各自的邮箱，防止邮箱超限。用户要保留的邮件要及时拷贝到本地计算机上保留；

7、邮件系统管理员必须遵守有关法律规定和职业道德规范，维护企业、用户个人的隐私与安全。

第十一章 终端用户安全管理

第四十五条 终端管理

1、外来人员携带电脑需要接入公司计算机网络的，必须征得相关部门负责人允许方可接入，并且要在相关人员随工的情况下完成操作；2、新购终端入网前要进行病毒扫描并统一部署安全软件；未经授权严禁使用他人帐号口令进行系统操作；

3、不得随意将终端设备提供给他人使用，长时间离开时，应将终端置于锁定状态或关机；

4、不得利用终端安装或使用嗅探、扫描、攻击等各类黑客软件进行信息窃取或攻击他人或其他系统；

5、禁止利用终端从事危害国家安全、泄漏国家秘密等违法犯罪活动，禁止编制、运行、传播危害网络安全的软件，禁止制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息；

6、禁止用户随意改动自己的网络参数配置，包括 IP 地址、网关、子网掩码、DNS 等。

第十二章 系统安装及升级安全管理

第四十六条 所有新的应用系统软件或者软件增强部分功能必须在用户需求说明中详细定义，并提交给业务系统管理员审核；新软件和升级软件在实施前必须搭建测试环境进行功能、性能和兼容性测试。测试前应提供测试方案，测试后提供详细的测试报告。

第四十七条 公司应有明确规定各类服务器设备、终端安装的软件，禁止安装盗版软件和非认可软件；对于公司设备及所安装的软件及 LICENSE 应有清晰的记录；对于非规定范围内的软件安装前应由系统维护人员进行评估和记录，并交由信息安全经理审核批准后，方可认为为认可软件，进入系统使用。

第四十八条 各系统管理员应定期检查系统或相关安全软件的补丁或升级文件的更新情况；要根据厂商的补丁公告和安全公告的紧急程度以及对系统的影响上报给信息安全工作组；所有补丁或升级文件的下载应尽量从原厂商的技术支持网站下载或原厂商提供的光盘文件中获得，以保障补丁或升级文件的可靠性。

第四十九条 各系统管理员针对自己的情况，安排补丁或升级文件的测试，以防止补丁或升级文件与现有业务或应用系统的冲突，应综合考虑安装补丁对系统安全和运行效率的影响。

第十三章 应用开发安全管理

第五十条 软件的更新应由合适权限的管理员负责进行；系统的用户认证和授权要严格、完善，遵循最小授权原则，对用户访问要有日志记录；不允许未经加密而用普通文本形式通过网络传输口令。

第五十一条 软件变更必须严格进行版本控制，版本的差异要有明确的记录。

第五十二条 当软件开发的工作由外部人员或厂家承担时，除了遵循本章以上管理要求外还必须加强以下方面的的安全管理：

1、明确代码及知识产权的归属；

2、审计系统的安全机制是否满足要求；

3、双方应签订保密协议。

第十四章 项目建设安全管理

第五十三条 项目从可行性研究、立项、招投标、合同到设计、施工等各个环节，必须符合《中华人民共和国招标投标法》和《中华人民共和国合同法》等相关法律法规的规定。

第五十四条 项目设计安全管理

1、项目实施方案的制订必须从网络安全、数据安全、应用安全、系统安全等各个角度进行评审和认可；

2、项目设计方案要利于网络安全策略和应用安全策略等的实施；并且要有完整的安全扩展方案（包括本系统扩容、功能增强和与第三方系统对接三个方面），以及故障恢复应急处理措施；

3、为了进行方案设计而提供给投标方的技术资料和信息应该以够用为标准，避免泄露过多的信息，并且应该与投标单位签订保密协议。

第五十五条 项目施工安全管理

1、在施工之前应与中标方签署详细的保密协议；

2、施工之前按照设计制定详尽的施工方案。包括：具体的施工步骤、每个步骤的具体操作、失败时的回退方案、测试方案等；

3、工程施工过程中，不得降低原有系统的安全级别；

4、项目实施中要重视机房、设备的物理安全，为施工人员派发临时工作证作为施工凭据；

5、新系统上线前，需经过严格的功能、性能测试，提交相应的测试报告；进行漏洞扫描和安全评估，并提交评估报告，确保系统符合相关的安全规定。

第五十六条 项目试运行安全管理

1、加强对试运行系统的安全监控，并定期进行详细记录，避免对其他系统造成影响；

2、加强试运行期间的跟踪支持和系统优化；

3、不得降低试运行期间系统的安全级别。

第五十七条 项目验收安全管理

(1)项目验收后，对于项目中曾经使用过的临时帐号应该立刻删除或修改密码；

(2)要求实施方提供由安全信息工作组认可的系统安全机制说明文档。

第五十八条 运维项目现场/客户的安全信息管理

1. 公司每一位员工都有保守客户信息安全，防止泄密的责任，任何人不得向任何单位或个人泄密客户信息。
2. 各运维项目经理应主动向客户提出信息安全的管理服务，若客户不愿意做，项目经理应向客户阐明利弊，提出合理的信息安全管理服务建议。
3. 如果为客户提供的数据备份服务，应定期对服务范围内的重要信息进行备份，管理人员实施备份操作时，必须有两人在场，备份完成后，立即交由客户制定的备份管理人员进行保管。
4. 存放备份数据的介质包括电脑、U盘、移动硬盘、光盘和纸质等，涉密单位介质使用参照客户保密要求。
5. 数据恢复前，必须对原环境的数据进行备份，防止有用数据的丢失。数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。
6. 数据清理前必须对数据进行备份，在确认备份正确后可进行清理操作，历次清理前的备份数据要定期保存或者永久保存，并确保可以随时使用。数据清理的实施应避开业务高峰期避免对客户业务运行造成影响。
7. 同意送修的设备，送修前，需将设备存储介质内的应用软件和数据等涉及经营管理的信息备份后删除，并进行登记。对修复的设备，应进行病毒检测。

8. 管理部门应对报废设备中存有的程序、数据资料进行备份后清除，并妥善处理废弃无用的资料和介质，防止泄密。
9. 严禁利用客户的信息化设备资源为第三方提供服务。
10. 非客户授权人员对服务范围内的设备、系统等进行维修、维护时，必须由相关技术人员现场全程监督。计算机设备送外维修，必须经过客户相关负责人批准。
11. 禁止在计算机应用环境中放置易燃易爆、强腐蚀、强磁性等有害计算机设备安全的物品。
12. 客户的密码管理需由客户指定专人进行管理，项目经理应建议客户定期修改并妥善保管。
13. 涉及系统管理员的服务项目，系统管理员权限由客户授权。

第十五章 应急安全管理

第五十八条 信息安全应急工作主要是指由于自然、社会及技术问题而引起重大的信息灾害后，为尽可能减少系统损失而采取的应急工作，其中信息灾害包括不可预期的黑客攻击、DOS 入侵、系统崩溃等重大信息安全问题。信息安全应急工作的目的是以最快速度恢复系统的机密性、完整性和可用性，阻止和减小安全事件带来的影响。同时收集与突发安全事件有关的信息，提供有价值的报告和建议。

第五十九条 根据系统的重要程度和可能遭遇的问题严重程度，应分别制定不同的应急响应计划。核心系统是我公司正常生产和运营的基本保证，是系统出现问题后进行恢复工作的基础。有严重灾难发生时，应首先对核心系统进行抢救。重要系统是我公司正常生产和运营的保证，在出现问题后，应在保证数据的情况下尽快加以恢复。

第六十条 信息安全突发事件级别分为四级：一般(IV 级)、较大(III 级)、重大(II 级)和特别重大(I 级)，对应颜色依次为蓝色、黄色、橙色和红色。

IV 级：发生未达到三级的一般安全事件，本级安全事件对计算机系统、网络系统和所承载的业务以及公司利益可能造成一定的影响或破坏；

III级：本级信息安全事件对计算机系统、网络系统和所承载的业务、公司利益以及社会公共利益有较为严重的影响或破坏。

II 级：本级信息安全事件对计算机系统、网络系统和所承载的业务、公司利益以及社会公共利益有极其严重的影响或破坏，对公司正常运行、社会稳定、国家安全造成危害；

I 级：本级信息安全事件对计算机系统或网络系统所承载的业务、基础网络、重要信息系统、重点网站瘫痪，导致业务中断以及灾难性的影响或破坏，造成或可能造成严重社会影响或巨大经济损失以及严重危害国家安全的信息安全事件。

第六十一条 应建立信息安全应急信息库，包括各种发生过的或很可能发生的具体安全事件，以及每种安全事件的最佳应急措施和备用方案，以便为后面的应急响应工作做好知识储备；应急信息库中应当包括发生过的安全事件的应急响应详细记录。

第六十二条 应急人员要定期对应急响应计划中各种安全事件的应急方案进行演练和测试，确保应急方案的可行性和可靠性，锻炼应急人员的应急响应速度和熟练程度；每次应急演练和测试均应当作详细的记录。

第六十三条 定期对应急人员在应急响应中所承担的任务和职责进行相应的培训和定期再培训。培训应急计划中的各种应急方案和技术措施，使他们既要掌握实施过程，又要做到熟练操作。培训一般包括以下内容：

1、信息安全的基本知识；

2、信息系统中可能发生的安全事件及其应急处理措施；

3、实际发生的信息安全典型事故及应急处理的经验教训。

第十六章 安全培训管理

第六十四条 为保证公司信息安全，提高部门员工的信息安全意识和知识水平，促使部门员工在日常工作时遵守相关的安全管理规定，部门员工需接受相应的信息安全教育与培训。

第六十五条 在进行安全培训前，需根据培训的具体内容和培训要求，制定安全培训计划，培训计划应包括培训项目、主要内容、主要负责人、培训日程安排、培训方式、培训对象等内容。

第六十六条 培训方式可采用集中授课、网络自助、短期培训和脱产培训等方式；培训后应进行考核。考核内容可以包括理论考核、实际操作技能考核；考核形式可以有问答、问卷、试验。