# 黑龙江北大荒农业股份有限公司
# 信息系统管理制度

## 第一章 总 则

**第一条** 为了推动和指导黑龙江北大荒农业股份有限公司（以下简称“公司”）建立健全内部控制，提高信息系统的可靠性、稳定性、安全性及数据的完整性和准确性，提高计算机信息系统管理水平，形成良好的信息传递渠道，根据五部委联合发布的《企业内部控制基本规范》、《企业内部控制应用指引第18号－信息系统》及国家有关法律法规规定，结合公司实际，制定本制度。

**第二条** 本制度所称信息系统，是指公司利用大数据、云计算、物联网、人工智能、通信等信息化技术手段，对内部控制进行集成、转化和提升所形成的信息化管理平台。

**第三条** 公司利用信息系统实施内部控制至少应当关注下列风险:

（一）信息系统缺乏或规划不合理，可能造成信息孤岛或重复建设，导致经营管理效率低下。

（二）系统开发不符合内部控制要求，授权管理不当，可能导致无法利用信息技术实施有效控制。

（三）系统运行维护和安全措施不到位，可能导致信息泄漏或毁损，系统无法正常运行。

（四）涉及个人信息处理的，应当同时遵守《中华人民共和国个

人信息保护法》及公司相关隐私政策；涉及重要数据和核心数据的，应当执行数据分类分级保护及备份要求。

**第四条** 本制度适用于公司及公司所属企业（以下简称“企业”），企业是指公司下设的分公司和全资或控股子公司。

## 第二章 信息系统规划与管理

**第五条** 信息化战略和规划必须符合公司发展战略。

（一）公司信息化目标:

1.通过业务整合和流程优化，实现底层数据和管理流程的规范;

2.使主要信息系统的版本标准化，降低集成难度、加强公司管理控制能力;

3.通过完善产品研发体系、业务管控服务体系、资产资金运作体系、决策支持体系，实现公司集约化经营模式的深化;

4.建立和发挥集团式管控平台应用的优势，全面完成应用体系的建设;

（二）公司信息化战略:

1.总体规划，分步实施，需求牵引，效益驱动，合理推进，重点突破;

2.企业内部业务流程的优化重组与企业间的应用协同相互融合;

3.内外合作，充分发挥自身优势，整合外部资源。

（三）公司信息化管理:

1.公司信息化系统建设按照统筹规划、分步实施的原则进行规划、设计、建设并实施应用;

2.各企业信息化建设要符合公司的总体战略规划;

3.信息系统的设计与架构，要有整体性和前瞻性，能满足公司信息的内部集成、上下集成、横向关联;

4.公司科技信息产业部对各企业信息化工作进行必要指导、协调和技术支持，避免制度执行不力、信息孤岛、投资浪费等现象的发生;

5.公司科技信息产业部要保证公司信息系统的安全性，确保信息系统的连续运行，以支撑公司的正常经营。

## 第三章　部门职责

**第六条**　公司信息技术工作实行统一归口管理，明确相关岗位的职责权限、考核指标，建立有效的工作机制。公司可以委托专业机构从事信息系统的开发建设以及运行维护工作。

（一）公司管理层对信息系统的规划、建设负有决策权，主要职责如下:

1.根据公司整体发展目标和战略，审议公司信息技术发展总体战略规划，确定年度信息工作计划及预算;

2.审议确定公司信息系统重大项目的设立、投入和优先级;

3.审议、批准公司信息技术管理制度和重要流程，推动公司现代化管理，以适应市场经济、信息时代的发展要求;

4.监督、考核公司科技信息产业部信息系统相关工作的落实完成情况，各部门信息系统应用的落实完成情况;

5.组织评估公司重大信息技术事项，并提出处置意见;

（二）公司科技信息产业部是公司信息系统规划、建设、管理、

实施的职能部门，主要职责如下:

1.根据公司发展战略和业务需求，制定公司信息系统战略规划和年度工作计划，并据此对信息系统进行规划建设和项目实施;

2.制定并不断完善公司与信息系统相关的规章制度、管理办法、规范标准以及操作规程，指导各企业根据自身的业务特点制定实施细则，并对有关制度、办法、规程的执行进行指导、监督;

3.公司总部计算机硬件、网络通信设备的安装调试等工作;

4.积极配合公司业务部门，负责计算机软件系统的采购与开发，以满足企业的发展建设需求;

5.管理、执行公司与信息系统日常运行维护、系统变更以及安全管理相关的工作;

6.配合公司党委工作部（人力资源部），落实年度信息技术、应用软件和信息安全等方面的培训、考核工作;

7.进行持续性的信息系统风险评估工作，定期对信息系统进行安全评估，及时发现系统安全问题并加以整改;

8.对各企业信息化工作进行指导和协调，提供必要的技术支持，避免制度执行不力、信息孤岛、投资浪费等现象的发生;

（三）公司各部门职责:

1.积极落实基于信息技术或与信息系统相关的内部控制;

2.结合本部门业务特点和发展需求，积极与信息系统归口管理部门沟通，寻求传统管理模式的信息化解决方案;

3.参加公司组织的信息技术、应用软件和信息安全等方面的培

训，熟练掌握办公相关的应用软件的使用方法。

（四）各企业信息管理部门职责:

1.依据公司信息系统管理制度，结合自身业务、管理特点制定各企业信息系统管理办法;

2.负责各企业计算机硬件、网络设备的采购、安装调试、资产管理、报损、报废等工作;

3.结合自身业务需求，在公司总部未作统一安排的情况下，采购开发部分应用系统;

4.管理、执行各企业与信息系统日常运行维护、系统变更以及安全管理相关的工作;

5.积极配合完成总部科技信息产业部安排的各项工作。

## 第四章　信息系统的开发

**第七条**　可行性分析与立项管理。

（一）信息系统项目的立项由科技信息产业部和信息系统项目需求部门（以下简称“需求部门”）共同完成。

（二）需求部门根据公司的发展战略和自身发展需要，提出相关信息系统项目的建设需求，指定项目建设业务负责人（以下简称“业务负责人”），负责项目建设中有关业务方面的工作。

（三）科技信息产业部派熟悉相关业务和系统的技术人员为项目协调（以下简称“项目协调负责人”），负责组织协调项目技术资源（技术专家或供应商）。

（四）需求发起部门根据实际情况，编写《可行性分析报告》对

项目进行可行性论证。

（五）《可行性分析报告》应当包括以下内容：项目名称、项目内容、项目市场调研和费用预算、效益分析、技术可行性分析、财务可行性分析、风险分析、技术预案等。

（六)科技信息产业部和需求部门领导负责对《可行性分析报告》进行审核，审核通过后，按审批程序提交公司审批。

**第八条** 招标、选型管理。

（一）《可行性分析报告》审批通过后，科技信息产业部和需求部门共同负责信息系统的招标、选型工作。

（二）信息系统的招标、选型工作按公司相关规定执行。

**第九条** 项目实施管理。

（一）在与系统供应商签订《软件服务/开发合同》后，由企业和系统供应商共同成立项目小组进行项目开发，小组名单需要明确小组成员的工作职责和能够进行访问的环境。系统供应商在调研的基础上提交《需求分析确认书》《项目设计方案》，由需求部门和科技信息产业部共同确认。

（二）项目实施的过程中，企业需引入项目管理理念对项目的实施进行适当的管理与监控以确保开发建设能够在预计时间内得到有效的实施并且满足设计需求。为了保障企业重要信息的安全，在与供应商签订合同内容条款中,要加入保密条款。

（三）系统建设完成后，系统供应商对系统进行严格的测试。测试内容应当包括：功能正确性测试、运行维护测试、性能指标测试、

压力测试等。

（四）在需求部门与科技信息产业部确认后，系统方可上线试运行。

**第十条** 数据移植与测试。如果软件项目涉及数据移植，由系统供应商与需求部门共同研究确定新旧系统数据的映射关系，对原有数据进行规范和净化，确定数据移植的方式和计划，数据成功移植完毕，项目小组编制《数据移植报告》。

**第十一条** 软件上线后，系统供应商编写《用户使用手册》，负责对用户进行培训，培训记录交党委工作部（人力资源部）归档、保存。

**第十二条** 系统试运行管理。

（一）信息系统的运行管理采取科技信息产业部和业务需求部门共同合作的运行管理模式。科技信息产业部负责系统运行环境的维护，包括服务器，数据备份等；需求部门可以承担业务系统管理员的角色,负责业务账号创建、分发与权限配置。

（二）试运行完毕后，科技信息产业部协助业务需求部门对项目进行总结验收。

**第十三条** 系统验收管理

系统经过试运行确认后，应当及时进行系统验收。系统验收由科技信息产业部负责协助业务需求部门组织召开。验收内容应当包括系统涉及到的硬件设备、系统软件功能、系统设置、系统测试情况、系统相关的文档等。经验收形成《项目验收报告》、《项目验收单》，

并经业务需求部门与科技信息产业部相关参与同事及负责人确认签字，完成验收工作。

**第十四条** 文档管理：应用系统实施完成后，需求部门须配合科技信息产业部对项目开发建设及实施过程中的相关文档进行归档备案，以便日后查阅使用。

## 第五章 信息系统变更管理

**第十五条** 生产用软件系统的系统变更。

（一）生产用软件系统的变更工作可分为下面二种类型：功能完善维护、系统缺陷修改。

1.功能完善维护指根据业务部门的需求，对系统进行的功能完善性或适应性维护;

2.系统缺陷修改指对一些系统功能或使用上的问题所进行的修复，这些问题是由于系统设计和实现上的缺陷而引发的。

（二）系统变更工作以任务形式需求部门、科技信息产业部与合作厂商协作完成。系统变更过程类似软件开发，大致可分为四个阶段：任务提交和接受、任务实现、任务验收和程序下发上线。

1.系统变更需求由需求部门提出，信息系统运行维护部门受理。需求部门将变更需求整理成《信息系统变更申请审批表》，该审批表在提交前应由需求部门负责人审批。

2.科技信息产业部在变更需求的分析过程中应评估并核实变更对现有运行带来的影响并写入《信息系统变更申请审批表》中。

3.信息系统运行维护部门负责系统变更需求的实现，同时确保所

有的变更请求都已经记录。

4.实现过程应按照软件开发过程规定进行。系统变更过程应遵循软件开发过程相同的正式、统一的编码标准，并经过测试通过后才能下发和上线。

5.系统变更过程中，科技信息产业部应协调供应商采取各种措施保证维护环境程序代码访问权限受到良好控制，防止源代码在完成测试到正式上线之间的非授权修改。

6.系统变更项目的文档应进行归档管理，变更过程中涉及的所有文档应至少保存三年以上。

**第十六条** 生产用基础平台系统的升级管理。

（一）系统升级指依据公司科技信息产业部的发版通知进行的系统软件等一系列变更。变更类型主要包括以下两类:

1.系统补丁程序，用于修正完整版程序的程序包。主要针对系统功能完善进行维护、针对系统缺陷进行修改;

2.维护或设置变更。

（二）向下级相关人员发出升级发布通知，通知中应包括程序包的名称、版本下发时间期限、是否需要进行功能测试以及其他必要要求。

（三）公司科技信息产业部负责统筹协调下发新的版本，进行功能发布。

（四）基础系统升级文档要求保存三年以上。

**第十七条** 紧急变更。

在紧急变更的情况下，为了确保系统正常运行科技信息产业部变更操作人员可以根据业务部门需求采取先变更再进行事后审批的管理办法。

**第十八条** 参数管理。

（一）静态表数据管理是指应用系统的数据库产品定义表、字典表的表结构及其数据的管理。

（二）各个应用系统的静态表表结构由公司统一制定并控制，原则上不能调整静态表的数据。

（三）使用部门根据需要对静态表数据进行修改，需与科技信息产业部业务负责人对接，统筹协调。

## 第六章 信息系统安全管理

**第十九条** 信息系统安全管理的范围包括:

（一）应用安全

各业务部门在使用业务系统过程中的安全管理，主要涉及到系统的权限管理、数据管理、人员管理等方面。根据业务与技术相分离的原则，有关应用安全管理制度的制定及执行以相关业务部门为主，科技信息产业部提供协助及指导。

（二）运行安全

主要包括计算机硬件系统、操作系统、数据库系统、网络系统、机房环境、网络安全、运行情况等。有关运行安全制度的制定及执行，以科技信息产业部为主。

**第二十条** 信息系统安全评估。

（一）在新建IT应用项目进行选型招标时，所有参与选型招标的项目都必须提供该项目的安全设计内容。

（二）安全设计方案至少应包含以下内容：该项目对于公司的网络系统有什么运行环境的需求；可能会给公司在信息安全方面带来什么影响；该项目将采取什么措施来防范以致消除负面影响。

（三）项目验收要包括安全部分内容。所有项目在其生命周期中，科技信息产业部要妥善保存该项目的分析报告、设计文档、测试文档、安装手册、使用手册以及其它有关资料。

（四）信息系统管理部门负责定期协调供应商对各自信息系统进行安全测试评估，提出评估报告及整改意见报企业领导。

**第二十一条** 应用系统安全管理。

（一）应用系统管理员负责该应用系统下的用户开户及权限管理工作，行业部门应用系统由行业部门设系统管理员，负责系统下的用户开户及权限管理工作。

（二）业务系统原则上不允许两个或两个以上的自然人共同使用同一个用户账号与口令,行业负责部门可根据实际情况自行调整。

（三）除个别应用系统使用的公共操作用户账号不便加设口令外，开设任何用户都应加设口令。

（四）员工离职或调换工作岗位时，应在当日删除该用户或修改其操作权限。

（五）系统管理员应每季度末对本系统下的所有操作用户进行全面清理,对无用的用户进行删除。

（六）用户应自觉定期修改自己的口令，以防因口令泄露，提供给别人可利用的机会。口令字长度应在6位以上。

**第二十二条** 系统运行安全管理。

（一）资产安全管理

1.系统设备的选型与采购依据《采购管理制度》的规定合理选择采购方式，履行相关程序；新购硬件设备及网络安全产品应经过安全检测和实际测试；定期对关键设备进行保养，建立详尽维护操作记录，建立严格的设备保管、使用登记、报废管理制度；企业实施信息技术资产报废时，应使用技术手段消除存储介质中所有数据并确保其无法恢复；

2.企业应购买正版应用软件，同时保证技术文档资料齐全，由科技信息产业部负责协调软件安全、维护、升级及安装补丁；

3.所有系统文档资料必须妥善保管，关键设备的系统配置参数、网络地址分配、网络结构等资料属于机密文档资料，未经授权不得外传，授权管理由科技信息产业部负责。

（二）技术安全管理

1.设立专职岗位进行网络设备的运行维护，对于关键网络系统的任何调整修改，必须经过相关技术论证并获得科技信息产业部授权批准后方可实施；

2.设立专职岗位进行系统的运行维护，建立严格的系统权限管理机制，强化系统口令并定期更改口令，关闭业务应用无关的服务，对系统进行定期升级、打补丁或安全加固，对操作系统和业务系统进行

必要的安全配置，定期进行系统渗透扫描，进行整改记录。

（三）操作安全管理

业务系统及重要硬件设备的规范操作流程是系统安全运行的重要指引，必须严格按照流程操作，明确个人操作职责，禁止越权非法操作。

（四）信息安全及网络设备日常维护

公司信息安全及网络设备日常维护可委托供应商负责管理,内容包括:

1.定期通过网管软件或其它方式查看路由器、主交换机、防火墙等网络及信息安全设备工作状态，确保网络设备运转正常，及时发现问题以避免网络服务异常中断;

2.根据防火墙类型及配置不同，分别检查以下内容: 检查防火墙配置信息、检查CPU负载、检查内存使用率、检查防火墙日志;

3.根据路由器、主交换机型号及配置不同，分别检查以下内容: 检查对路由器、交换机的操作、检查路由器路由配置策略的变化、检查相关日志等;

4.管理VPN设备的使用、客户端的安装以及访问权限的申请。权限申请管理参照本制度第二十五条信息系统权限管理执行。

5.发现异常情况后立即分析原因并进行处理，处理过程记录在当日的《机房运维日志》中。

**第二十三条** 机房管理。

科技信息产业部是计算机房的归口管理部门，对机房进行日常管

理，对机房的环境、设备的安全负责、访问权限负责。

（一）机房出入管理

1.机房是生产重地，任何人员未经许可，不得出入;

2.机房钥匙仅能由科技信息产业部或委托第三方单位管理人员持有或保管：机房钥匙由机房管理员保管，不得外借;

3.进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品;

4.为了保证机房的正常工作秩序和安全，未经领导同意任何人不得引领无关人员参观机房。任何其他人员因工作需要进入机房，均需填写《机房访问登记表》;

5.所有来访者离开机房时要做好登记工作;

6.进入机房人员应自觉遵守机房内各项管理规定，保持机房内安静、整洁。工作完毕后应及时离开。

（二）机房卫生管理规定

1.机房管理人员需要定期对机房进行打扫，保证机房内环境、设备的清洁;

2.任何人不得将食物或饮料带入机房，任何人不得在机房内吃东西、吸烟、吐痰;

3.进入机房人员在工作完毕后，自觉将所带纸张等废弃物品带走。

（三）机房设备管理规定

1.机房管理员应对机房内设备进行登记，包括在《信息技术资产

表》中记录现有设备的型号、配置、位置、状态等信息，在《机房设备出入登记表》中记录设备出入变化情况，任何设备未经许可，不得进出机房;

2.机房管理员对机房设备的操作必须严格按照操作程序进行;

3.非机房管理人员未经许可，不得擅自对机房设备进行操作;

4.综合办公室（董事会办公室）为机房内的供电系统、消防系统、机房监控系统、空调系统等设备应制定相关的维护保养计划，机房管理人员按计划进行维护保养;

5.机房管理员需要对机房内主机等设备的故障维修进行登记。

（四）值班管理规定

1.机房管理员进行每周机房巡检，并根据实际情况周内进行不定期机房巡查，检查机房内状况、各类系统设备的运行状况、空调、UPS、消防等设备的完好性，并将巡检结果填写在《机房运行日志》中，如果发现问题需要及时处理并将问题及处理结果记录在《机房运行日志》中，处理过程、结果报告科技信息产业部负责人;

2.对于进入机房人员不遵守机房管理规定或从事与正常工作内容不相符的操作，机房管理人员必须及时加以制止，必要时可终止其操作;

（五）机房消防、安全管理规定

1.机房应提供计算机设备正常运行所必须的温度、湿度等环境要求，安装温湿度报警设施，对运行环境可能出现的不利因素进行监测并预警;

2.机房内应定期除尘，在除尘时应确保计算机设备的安全;

3.机房应列为单位要害和重点防火部位，应严格按照相关国家标准安装配备足够数量的消防报警设备以及消防器材，机房工作人员要熟悉机房消防器材的存放位置及使用方法，定期检查更换;

4.严禁在防火通道内堆放杂物，确保设备及工作人员的安全;

5.机房应配备适当的不间断的电力供应，确保有足够的后备电力支持正常的系统应急操作; 每半年对现有的不间断的电力供应设备进行检查与维护，确保设备的正常运作; 根据机房设备的变更情况，更新不间断的电力供应设备以确保对新运行环境的保护;

6.每半年对机房供电线路及照明器具进行检查，防止因线路老化短路造成火灾;

7.机房管理人员要熟悉设备电源和照明用电以及其他电气设备总开关位置，掌握切断电源的方法与步骤，发现火情应及时报告，采取有效措施及时灭火;

8.对于安全系统检查出现异常，需记录并及时通报科技信息产业部负责人。

**第二十四条** 信息系统权限管理。

（一）用户管理

1.各信息系统用户分为三个级别：系统级用户、管理级用户、普通用户;

2.系统级用户包括:数据库超级用户和各信息系统超级管理员，是系统安装时自动创建的用户;

3.管理级用户是对普通用户授权管理并维护系统正常运行的用户，由应用系统使用部门设专人担任。管理级用户的主要职责有:

（1）按照各信息系统用户和权限审批流程建立普通用户;

（2）按照各信息系统权责对等和权限最小化原则分配普通用户权限;

（3）定期审核用户日志，发现异常立即向部门领导汇报;

（4）对普通用户临时授权要按照各信息系统临时授权权限管理的流程进行,并按规定期限及时回收权限;

4.普通用户是为申请使用相关信息系统人员建立的一般用户。普通用户的主要职责有:

（1）按照职责范围使用相关信息系统;

（2）发现系统异常，立即反映;

（3）根据自己的业务需求，提出对系统的修改建议;

（4）定期修改密码，并确保密码的安全;

（5）严格遵守各信息系统权责对等原则，对拥有超出职责的权限立即向管理级用户或部门负责人报告。

5.管理级用户和普通用户必须是实名制用户，相关信息系统对管理级用户有限定不能开设的情况除外,但对非实名管理级用户的管理须落实到具体操作人;

6.不允许两个或两个以上自然人共同使用同一个管理级用户或普通用户的账号。

（二）权限管理

1.对普通用户可以进行分组管理，用户组按组别的最小权责分配权限;

2.对普通用户授权时，由业务部门界定用户的权限范围，由业务系统管理级用户授权;

3.因业务需要需对普通用户临时授权时，由管理级用户授权，期限结束后主动删除。

（三）密码管理

1.各信息系统的任何用户都必须加设密码，系统正常运行后，严禁采用系统初始密码、默认密码等;

2.系统级用户和管理级用户的密码字长度应在8位以上，且必须采用数字和字母混合的方式，普通用户的密码字长度不少于6位;

3.对于同时拥有业务操作与授权管理的双重角色的系统用户，密码管理按照本条第（一）款规定执行。管理级用户需定期修改自己的密码，修改后的密码需封存保管。对于系统中有条件设定管理级用户密码有效期限的，最大期限不应超过3个月，以便强制管理级用户定期修改自己的密码;

4.普通用户应妥善保管和定期修改自己的密码，以防密码因泄露而提供给别人可利用的机会;

5.信息系统的程序开发中应考虑设置密码尝试次数限制。超过规定次数后，系统应采取相应措施封锁用户，并有预警功能。

**第二十五条** 防病毒。

（一）专人管理

科技信息产业部网络系统安全管理人员，负责公司并指导下属企业的病毒防杀工作，工作职责包括:

1.制定防病毒系统的整体安全规划和安全策略;

2.负责公司网络与信息系统的监控和预警工作;

3.对防病毒系统进行日常维护和管理，包括防病毒系统的安装、调试、测试、监控、维护、版本升级和病毒代码库的升级。

（二）经公司统一协调安装的防病毒软件，员工不得隐瞒，自行关闭或卸载防病毒软件。

（三）防病毒管理员负责对所有的服务器的杀毒软件进行监督、管理，以保障公司网络内服务器和客户端的病毒库代码被及时更新，并针对病毒库代码未能及时更新的客户端进行手动更新和杀毒。

（四）如果发现病毒，相关人员应立即联系防病毒管理员，对受感染的计算机进行有效的隔离，病毒清除后，应检查其最近使用过的软盘、光盘和移动存储设备，避免漏杀。

（五）禁止在计算机上安装与工作无关的软件；禁止从互联网上随意下载程序、数据，如果确实需要，应当先进行病毒检测后再使用;员工不得随意打开陌生人发送来的邮件附件或可疑邮件，必要时将其直接删除。

（六）外来的软盘、光盘和移动存储设备应先进行病毒检查后方可使用；对购置、借入的计算机及其他网络存储设备，应当及时进行病毒检测。

**第二十六条** 信息技术、信息安全培训。

（一）培训内容

科技信息产业部同党委工作部（人力资源部）定期组织信息技术、信息安全方面的培训，提高员工办公软件、应用系统的使用技巧，加强员工信息安全意识。培训内容包括办公软件、办公系统的使用方法，公司信息系统发展概况、系统日常使用注意事项、信息安全知识、灾难应急预案及恢复计划等，其中信息安全培训应为年度培训。

（二）受训人员

1.科技信息产业部员工为信息系统的运行管理者以及信息系统内部控制的执行者，在接受公司安排的信息技术、信息安全培训的基础上，应该主动加强专业业务的学习，提高自身的业务能力。

2.公司员工积极参加公司组织的信息技术，信息安全培训，不断提高信息安全意识，规范自身的安全操作流程。

（三）培训管理

党委工作部（人力资源部）负责对培训所形成的关键文档进行归档、保管，包括培训通知、签到表、讲义等。

**第二十七条** 数据备份。

（一）备份策略

1.备份策略的选择需要统筹考虑信息系统中需备份的总数据量，线路带宽、数据吞吐量、备份窗口等因素，策略经信息系统使用部门和科技信息部;

2.备份策略包括，但不仅限于数据备份范围、备份方式、执行时间、备份频率、任务执行顺序、保存时限、离线及异地备份频率、备

份介质编号规则、恢复测试频率等;

3.数据备份由专人完成，备份操作人员需要在《信息系统运维日志》中记录系统数据备份相关工作，对失败的备份操作处理需进行汇报、跟进及记录;

4.备份对象发生变更后，应同时评估、调整备份策略。备份策略的变更应得到申请部门以及科技信息产业部相关负责人审批;

5.科技信息产业部负责人定期对备份工作记录进行检查，确保备份工作的完整性以及出现的问题已得到适当处理。

（二）备份介质

1.所有备份介质一律不准外借，不准流出公司，任何人员不得擅自取用，若要取用需经科技信息产业部相关负责人批准，并撰写《备份数据使用申请》。所借用存储介质使用后，应立即归还，由备份管理员检查确定介质完好，并填写归还记录;

2.离线或异地备份介质存放地至少应具备防火、防水、基本的门禁装置等设施。备份介质存放应有详细记录，记录内容包括但不仅限于：备份介质编号、存放人、存入日期等;

3.数据正本与备份应分别存放于不同地点，防止因火灾、水灾、地震等事故产生不利影响;

4.备份操作员每年对备份介质进行检查，一旦发现介质损坏，应立即更换;

5.存放备份数据的介质需要废弃或销毁时，应填写《介质冲洗、销毁登记表》，并履行审批、登记和交接手续，双人以上在场，防止

生产数据的泄漏。

（三）备份恢复

1.如果需要对备份数据进行恢复，申请部门应填写《数据恢复申请单》，并经请部门以及科技信息产业部相关负责人批准;

2.备份操作员需按照数据的重要程度对恢复对象进行分类，以保证能够按照优先级进行数据恢复，并制定详细的备份恢复操作计划，计划应包含备份恢复的操作步骤、恢复前的准备工作、恢复失败的处理方法和跟进步骤、验收标准等;

（四）办公电脑中的数据备份

员工对个人电脑中的工作数据完整性，有效性负责，需要定期将重要信息备份至移动存储设备。对于以前年度的重要工作文档和底稿可以进行硬盘拷贝，以备长期保存、参考。

**第二十八条** 紧急情况与数据灾难恢复。

（一）科技信息产业部建立紧急情况联系人方式列表，以便在紧急情况发生的第一时间通知有关人员。

（二）紧急情况处理

1.火灾发生：切断电源，迅速报警，根据火情，选择正确的灭火方式灭火;

2.水灾发生：切断电源，迅速报告有关部门，尽可能地弄清水灾原因，采取关闭阀门、排水、堵漏、防洪等措施;

3.地震发生：切断电源，避免引发短路和火灾。

（三）灾难恢复

1.硬件故障恢复

（1）对信息系统的关键设备均需留有冗余备份，当硬件故障发生后，及时用备份设备替换故障设备。

（2）按照硬件采购合同，迅速与硬件制造商或中间集成商取得联系，对故障设备进行售后服务。

（3）对故障事件进行备案。

2.系统或软件故障恢复

（1）数据瘫痪：用最近的数据备份文件进行恢复。

（2）数据库瘫痪：对数据库管理系统进行修复或重新安装，之后用最近的数据备份文件进行恢复。

（3）操作系统瘫痪：重新安装操作系统，进行业务系统安装配置，进行数据库的恢复，信息安全策略配置等。

（4）系统或软件恢复时间按照公司 IT 系统运行连续性要求执行。

（5）填写《系统运维日志》，对故障事件进行备案。

## 第六章　第三方服务商管理

**第二十九条**　第三方服务商管理

（一）第三方服务商的资质标准

1.第三方服务商的基本资质

（1）第三方服务商应是按照中华人民共和国有关法律法规在我国境内设立的企业法人，并具备合格有效的工商营业执照，具备独立承担民事责任的能力;

（2）第三方服务商应具有良好的经营业绩和银行资信状况，遵

守国家法律法规，具有很好的商业信誉。

2.第三方服务商应具备的技术能力

（1）应具备对专业服务对象的故障诊断、排除和技术支持能力;

（2）应具备将国际先进的 IT 技术和经验引入到我公司系统的能力;

（3）具备制订应用解决方案和实施的能力;

（4）具有同主流信息技术厂商良好的合作关系，并且能够帮助我公司协调同相关厂商的关系。

3.第三方服务商资质验证

（1）在签订服务协议前须验明第三方服务商资质。第三方服务商需经过我公司资质验证方可有资格参加服务协议的签订。资质验证的工作应由不参与合同签订的部门根据公司规定进行;

（2）第三方服务商若发生企业重组或法定代表人变更等重要事项时，项目执行机构（组织）应及时提醒第三方服务商将有关事项以书面形式告知我公司。对服务协议的执行会产生影响的，双方应尽快签订有关变更协议，以保证相关服务的有效延续。

（二）第三方服务商提供服务范围

1.技术咨询

（1）根据公司总部信息技术建设总体部署，协助公司制定切实可行的技术实施方案;

（2）对公司现有的信息技术基础架构、设备运行状态和应用情况进行诊断和评估，提出合理化建议;

（3）提供其他需要的技术咨询;

（4）系统集成;

（5）服务器、网络、操作系统、数据库、应用系统及其他软件等的技术集成;

（6）系统的整合及性能优化。

2.运行维护

（1）硬件设备的维修和保养;

（2）软件系统的升级及故障处理;

（3）系统定期巡检和整体性能评估;

（4）信息安全的定期检测和评估，并提出建议以及根据实际情况对公司信息安全进行优化。

3.技术和管理培训

（1）根据公司的实际情况提供技术和管理培训;

（2）跟踪适合公司应用发展的国际先进技术和管理经验并及时推介;

（3）协调公司与设备（软件）制造方、提供方等相关方面的关系;

（4）需要完成的其他技术工作。

（三）第三方服务商协议的签订与费用支付

1.所有由第三方服务商提供的服务均需签订第三方服务协议或合同。

2.与第三方服务商签订的服务协议或合同中应明确规定:

（1）对第三方服务商服务持续性的要求，并作为合同中的主要

条款之一;

（2）应与第三方服务商签订服务规范及保密协议，明确规定第三方服务商在服务提供过程中应该遵守公司制度,严禁任何对公司可能造成不良影响的行为，严禁泄露公司信息，并明确违约责任;

（3）未经公司授权允许，严禁第三方服务商进行转包和分包，第三方服务商进行转包何分包，须向公司科技信息产业部、发展战略部函询批复。

3.项目执行机构负责人员或相关工作人员应将服务合同提交法律、财务等相关部门会签、管理层批准后才可进行合同的签订工作。第三方服务商的各项服务费(含报酬)应纳入公司当年的相关预算中。

4.公司总部、各企业单独与第三方服务商签订的服务合同，其服务费用应根据合同规定分别由公司总部、各企业自行支付。第三方服务商的各项服务均应在服务合同中明确，并事先列出清单，计算出所需要的人工天数，形成服务合同的附件，作为合同到期后确定最终获得服务的人工天数的结算依据。

（四）对第三方服务商的监控和考核

1.当第三方服务商对科技信息产业部提出的服务请求进行响应时，科技信息产业部应对第三方服务商服务进行监控。

2.公司科技信息产业部根据实际情况组织对第三方服务商的评估。评估内容应包括第三方服务商服务响应速度、服务质量，评估主要涉及第三方服务商是否按照合同涉及的服务条款实施服务,第三方服务商提供的服务是否能够满足企业的需求。

（五）第三方服务商持续性要求

在第三方服务商合同到期前一个月，科技信息产业部根据评估结果确定该第三方服务商是否能够充分满足公司业务需求，并确定是否与该第三方服务商续签合同。如果确定可以续签合同，应按合同规定执行。根据监管部门对第三方服务商的评估，对于合同内容发生的变更应按公司合同管理相关规定执行。

## 第七章　附　则

**第三十条**　本制度由公司科技信息产业部负责草拟、解释和督办，由公司董事会负责审议和修订。

**第三十一条**　本制度自发布之日起执行，原《信息系统管理制度》（黑北农发[2014]54 号）同时废止。