第一条为加快公司信息系统建设步伐，规范信息系统工程项目建设安全管理，提升信息系统建设和管理水平，保障信息系统工程项目建设安全，特制定本规范。

第二条本规范主要对 XX 公司（以下简称 公司”）信息系统建设过程提出安全管理规范。保证安全运行必须依靠强有力的安全技术，同时更要有全面动态的安全策略和良好的内部管理机制，本规范包括五个部分：

1）项目建设安全管理的总体要求：明确项目建设安全管理的目标和原则；

2）项目规划安全管理：对信息化项目建设各个环节的规划提出安全管理要求，确定各个环节的安全需求、目标和建设方案；

3）方案论证和审批安全管理：由安全管理部门组织行内外专家对项目建设安全方案进行论证，确保安全方案的合理性、有效性和可行性。标明参加项目建设的安全管理和技术人员及责任，并按规定安全内容和审批程序进行审批；

施的阶段的安全管理目标和实施办法，并完成项目安全专用产品的确定、非安全产品安全性的确定等；

5）项目投产与验收安全管理：制定项目安全测评与验收方法、项目投产的安全管理规范，以及相关依据。

第三条规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包孕勘误的内容）或修订版均不适用于本规范，但鼓励研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。

GB/T 5271.8－2001 信息技术词汇第 8 部分安全

第四条术语和定义

本规范引用 GB/T5271.8－2001 中的术语和定义，还采用了以下术语和定义：

1）信息安全 infosec

信息的机密性、完整性和可用性的保护。

注释：机密性定义为确保信息仅仅被那些被授权了的人员访问。

完整性定义为保护信息和处理方法的准确性和完备性。

相关资产。

2) 计 算 机 系 统 安 全 工 程 ISSE （ Information Systems Security

Engineering）

计算机系统安全工程（ISSE）是发掘用户信息安全保护需求，然后以经济、精确和简明的方法来设计和建造计算机系统的一门技巧和科学，ISSE 识别出安全风险，并使这些风险减至最少或使之受到遏制。

3)风险分析 risk analysis

对信息和信息处理设施所面临的威胁及其影响以及计算机系统脆弱性及其发生的可能性的分析评估。

4)安全目标 security objective

本规范中特指公司项目建设信息安全管理中需要达成到的目标。

5)安全测试 security testing

用于确定体系的安全特征按设计要务实现的过程。这一过程通常包孕现场功能测试、渗透测试和验证。

各种信息化项目建设的具体情况，依据各种标准、规范以及安全管理规定而制定。

第六条项目建设安全管理目标

一个项目的生命周期包括：项目申报、项目审批和立项、项目实施、项目验收和投产；从项目建设的角度来看，这些生命周期的阶段则包括以下子阶段：需求分析、总体方案设计、概要设计、详细设计、系统实施、系统测试和试运行，如下表所示。

项目建设安全管理的目标就是保证整个项目管理和建设过程中系统的安全。为了达到这个目标，信息安全（INFOSEC）必须融合在项目管理和项目建设过程中，与公司的业务需求、环境要求、项目计划、成本效益以及国家和地方的政策、标准、指令相一致。这种融合应该产生一个计算机系统安全工程（ISSE）项目，它要确认、评估、并且消除或控制住系统对已知或假定的威胁的脆弱点，最终得到一个可以接受水平的安全风险。

）并不意味着存在一个单独独立的过程。它支持项目管理和建设过程，而且是后者不可分割的一部分。第三章到第六章将以项目管理过程为主轴，并结合项目建设过程，规定了在每个阶段中应达到哪些计算机系统安全工程要求。

第七条项目建设安全管理原则

信息系统项目建设安全管理应遵循如下原则：

1)等级

2)全生命周期安全管理：信息安全管理必须贯串信息化项目建设的整个生命周期；

3)成本-效益分析：进行信息安全建设和管理应考虑投入产出比；

4)明确职责：每个参与项目建设和项目管理的人员都应该明确安全职责，应进行安全意识和职责培训，并落实到位；

5)管理公开：应保证每个项目参与人员都知晓和理解安全管理的模式和方法；

6)科学制衡：进行适当的职责分离，保证没有人可以单独完成一项业务活动，以避免出现相应的安全问题；

7)最小特权：职员对项目资产的访问权限定到最低限度，即仅赋予其执行授权任务所必需的权限。

目的申报、审批、立项、实施、验收等关键环节中，必须依照规定的职能行使职权，并在规定的时限内完成各个环节的安全管理行为，否则应承担相应的行政责任。

第三章项目申报

第九条项目申报阶段应对信息体系项目及其建设的各个环节进行统一的安全管理规划，确定项目标安全需求、安全目标、安全建设方案，以及生命周期各阶段的安全需求、安全目标、安全管理措施。

第十条应由项目应用主管单位进行项目需求分析、确定总体目标和建设方案。项目应用主管单位进行项目申报时应填写《信息系统项目立项申请表》，并提交《业务需求书》和《信息系统项目可行性研究报告》。

第十二条系统定级

1）依据国家信息系统安全等级保护定级指南（GBT－2008）对项目中的系统进行定级，明确信息系统的边界和安全保护等级；

的方法和理由，形成信息系统定级报告；

3）组织相关部门和有关安全技术专家对信息体系定级结果的合理性和正确性进行论证和审定，上报上级主管单位和安全监控单位进行审定；

4）信息系统的定级结果向本地公安机关进行备案。

第十三条挖掘安全需求

在《业务需求书》中除了描述体系业务需求之外，还应进行体系的安全性需求分析，应最少包孕以下信息安全方面的内容：

1)安全威胁分析报告：应分析待建计算机系统在生命周期的各个阶段中可能遭受的自然威胁或者人为威胁（故意或无意），具体包括威胁列表、威胁可能性分析、威胁严重性分析等；

2)系统脆弱性分析报告：包括对系统造成问题的脆弱性的定性或定量的描述，这些问题是被攻击的可能性、被攻击成功的可能性；

3)影响分析报告：描述威胁利用系统脆弱性可能导致不良影响。影响可能是有形的，例如资金的损失或收益的减少，或可能是无形的，例如声誉和信誉的损失；

定环境中涉及到对某一系统有依赖关系的安全风险。它取决于上面的威胁分析、脆弱性分析和影响分析，应提供风险清单以及风险优先级列表；

5)系统安全需求报告：针对安全风险，应提出安全需求，对于每个不可接受的安全风险，都至少有一个安全需求与其对应。

第十四条安全可行性

在可行性报告的以下条目中应增加相应的信息安全方面的内容：

1）项目目标、主要内容与关键技术：增加信息化项目的总体安全目标，并在主要内容后面增加针对前面分析出的安全需求所提出的相应安全对策，每个安全需求都至少对应一个安全对策，安全对策的强度应根据相应资产的重要性来选择；

2）项目采用的技术路线或者技术方案：增加描述如何从技术、运作、组织以及制度四个方面来实现所有的安全对策，并形成安全方案；

3）项目标承担单位及职员情况介绍：增加项目各承担单位的信息安全方面的天分和经验介绍，并增加介绍项目主要参与职员的信息安全背景；

）项目安全管理：增加项目建设中的安全管理模式、安全组织结构、人员的安全职责、建设实施中的安全操作程序和相应安全管理要求；

5 -效益分析。

第十五条对投入使用的应用软件需求升级改造的，虽不需另行立项，但仍需参照上述方法进行一定的安全性分析，并针对可能发生的安全问题提出和实现相应安全对策。

第四章安全方案设计

第十六条本阶段主要是项目审批单位对项目申报内容进行安全方案的设计，对项目的安全性进行确定，必要时可以聘请外单位的专家参与论证工作。

第十七条安全标准的确定

1）根据体系的安全保护等级选择基本安全措施，设计安全标准必须达到等级保护相关等级的基本要求，并依据风险分析的结果进行补充和调整需要的安全措施；

2）指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件

4）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

5）根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

第五章方案论证和审批

第十八条本阶段主要是项目审批单位对项目申报内容进行审批，对项目进行安全性论证，必要时可以聘请外单位的专家参与论证工作。

第十九条安全性论证和审批

安全性论证应着重对项目的安全需求分析、安全对策以及总体安全方案进行成本-效益、合理性、可行性和有效性分析，并在《信息化项目立项审批表》上给出明确的结论：

1）适当

3）需作复议

对论证结论为 需作复议”的项目，通知申报单位对有关内容进行需要的补充大概修改后，再次提交复审。

第二十条项目安全立项

审批后，项目审批单位将对项目进行立项，在《信息体系项目任务书》的以下条目中应增加相应的计算机安全方面的内容：

1)项目标管理模式、组织结构和责任：增加项目建设中的安全管理模式、安全组织结构以及职员的安全职责；

项目实施的基本程序和相应的管理要求：增加项目建设实施中的安全操作程序和相应安全管理要求；

3)项目设计目标、主要内容和关键技术：增加总体安全目标、安全对策以及用于实现安全对策的总体安全方案；

4)项目实现功能和性能指标：增加描述系统拥有的具体安全功能以及安全功能的强度；

5)项目验收查核指标：增加安全性测试和查核指标。

第二十一条立项的项目，如采用引进、协作开发大概外包开发等形式，则需与第三方签订安全保密协议。

第二十二条信息化项目实施阶段包孕3个子阶段：提要设计、详细设计和项目实施，本阶段的主要工作由项目开发承担单位来完成，项目审批单位负责监监工作。

第二十三条提要设计子阶段的安全要求

在提要设计阶段，体系层次上的设计要求和功能指标都被分配到了子体系层次上，这个子阶段的安全目标是包管各子体系设计实现了总体安全方案中的安全功能。因此，《提要设计仿单》中最少应达到以下安全要求：

1)应当按子体系来描述体系的安部分系结构；

2)应当描述每一个子系统所提供的安全功能；

3)应当标识所要求的任何基础性的硬件、固件或软件，和在这些硬件、固件或软件中实现的撑持性保护机制提供的功能透露表现；

4)应当标识子系统的所有接口，并说明哪些接口是外部可见的；

5)描述子体系所有接口的用途与使用方法，并适当提供影响、例外情况和毛病音讯的细节；

6)确证子体系（不论是开发的，还是买来的）的安全功能指标满足体系安全需求。