1、信息安全管理方针(fāngzhēng)和策略

范围(fànwéi)

公司依据 ISO/IEC27001:2013信息安全管理体系标准的要求(yāoqiú)编制《信息安全管理手册》，并包括了风险评估及处置的要求。规定了公司的信息安全方针及管理目标，引用了信息安全管理体系的内容。

1.1规范性引用(yǐnyòng)文件

下列参考文件的部分或整体在本文档中属于标准化引用，对于本文件的应用必不可少(bìbùkěshǎo)。凡是注日期的引用文件，只有引用的版本适用于本标准；凡是不注日期的引用文件，其最新版本（包括任何修改）适用于本标准。

ISO/IEC 27000，信息技术——安全技术——信息安全管理体系——概述和词汇。

1.2术语和定义

ISO/IEC 27000中的术语和定义适用于本文件。

1.3公司环境

1.3.1理解公司及其环境

公司确定与公司业务目标相关并影响实现信息安全管理体系预期结果的能力的外部和内部问题，需考虑：

明确外部状况：

社会、文化、政治、法律法规、金融、技术、经济、自然和竞争环境，无论国际、国内、区域，还是本地的；

影响组织目标的主要动力和趋势；

与外部利益相关方的关系，外部利益相关方的观点和价值观。

明确内部状况：

治理、组织结构、作用和责任；

方针、目标，为实现方针和目标制定的战略；

基于资源和知识理解的能力（如：资金、时间、人员、过程、系统和技术）；

与内部利益相关方的关系(guān xì)，内部利益相关方的观点和价值观；

组织(zǔzhī)的文化；

信息系统、信息流和决策过程(guòchéng)（正式与非正式）；

组织所采用的标准、指南(zhǐnán)和模式；

合同(hé tong)关系的形式与范围。

明确风险管理过程状况：

确定风险管理活动的目标；

确定风险管理过程的职责；

确定所要开展的风险管理活动的范围以及深度、广度，包括具体的内涵和外延；

以时间和地点，界定活动、过程、职能、项目、产品、服务或资产；

界定组织特定项目、过程或活动与其他项目、过程或活动之间的关系；

确定风险评价的方法；

确定评价风险管理的绩效和有效性的方法；

识别和规定所必须要做出的决策；

确定所需的范围或框架性研究，它们的程度和目标，以及此种研究所需资源。

确定风险准则：

可以出现的致因和后果的性质和类别，以及如何予以测量；

可能性如何确定；

可能性和（或）后果的时间范围；

风险程度如何确定；

利益相关方的观点；

风险可接受或可容许的程度；

多种风险的组合是否予以考虑，如果是，如何考虑及哪种风险组合宜予以考虑。

1.3.2理解相关方的需求和期望

信息安全管理小组应确定信息安全管理体系的相关方及其信息安全要求，相关的信息安全要求。对于利益相关方，可作为信息资产识别，并根据风险评估的结果，制定相应的控制措施，实施必要的管理。相关方的要求可包括法律法规要求和合同义务。

1.3.3确定(quèdìng)信息安全管理体系范围

本公司(gōng sī)ISMS 的范围包括

a) 物理(wùlǐ)范围：

b) 业务范围：计算机软件开发(kāifā)，计算机系统集成相关(xiāngguān)信息安全管理活动。

c) 内部管理结构：办公室、财务部、研发部、商务部、工程部、运维部。

d) 外部接口：向公司提供各种服务的第三方

1.3.4信息安全管理体系

本公司按照 ISO/IEC27001:2013标准的要求建立一个文件化的信息安全管理体系。同时考虑该体系的实施、维持、持续改善，确保其有效性。ISMS 体系所涉及的过程基于 PDCA 模式。

1.4领导力

总经理应通过以下方式证明信息安全管理体系的领导力和承诺：

a) 确保信息安全方针和信息安全目标已建立，并与公司战略方向一致；

b) 确保将信息安全管理体系要求融合到日常管理过程中；

c) 确保信息安全管理体系所需资源可用；

d) 向公司内部传达有效的信息安全管理及符合信息安全管理体系要求的重要性；

e) 确保信息安全管理体系达到预期结果；

f) 指导并支持相关人员为信息安全管理体系有效性做出贡献；

g) 促进持续改进；

h) 支持信息安全管理小组及各部门的负责人，在其职责范围内展现领导力。

1.5规划

1.5.1应对风险和机会的措施

1.5.1.总则

公司针对公司内部和公司外部的实际情况，和相关方的要求，确定公司所需应对的信息安全方面的风险。在已确定的 ISMS 范围内，针对业务全过程所涉及的所有信息资产进行列表识别。信息资产包括软件/系统、数据/文档、硬件/设施、人力资源及外包服务。对每一项信息资产，根据信息资产判断依据确定信息资产的重要性等级并对其重要度赋值。

信息安全管理小组制定信息安全风险评估管理程序，经信息安全管理小组组长批准后组织实施(shíshī)。风险评估管理程序包括可接受风险准则和可接受水平。该程序的详细内容见《信息安全风险评估管理程序》。

1.5.1.1.信息安全风险(fēngxiǎn)评估

1.5.1.1.1 风险评估的系统(xìtǒng)方法

信息安全管理小组制定(zhìdìng)信息安全风险评估管理程序，经管理者代表审核，总经理批准后组织实施。风险评估管理程序包括可接受风险准则和可接受水平。该程序的详细内容适用于《信息安全风险评估管理程序》。

1.5.1.1.1资产(zīchǎn)识别

在已确定的 ISMS 范围内，对所有的信息资产进行列表识别。信息资产包括软件/系统、数据/文档、硬件/设施及人力资源、服务等。对每一项信息资产，根据信息资产判断依据确定信息资产的重要性等级并对其重要度赋值。

1.5.1.1.1评估风险

a) 针对每一项信息资产、记录、信息资产所处的环境等因素，识别出所有信息资产所面临的威胁；

b) 针对每一项威胁，识别出被该威胁可能利用的薄弱点；

c) 针对每一项薄弱点，列出现有的控制措施，并对控制措施有效性赋值；同时考虑威胁利用脆弱性的容易程度，并对容易度赋值；

d) 判断一个威胁发生后可能对信息资产在保密性(C)、完整性(I)和可用性(A)方面的损害，进而对公司业务造成的影响，计算信息资产的安全事件的可能性和损失程度。

e) 考虑安全事件的可能性和损失程度两者的结合，计算信息资产的风险值。

f) 根据《信息安全风险评估管理程序》的要求确定资产的风险等级。

g) 对于信息安全风险，在考虑控制措施与费用平衡的原则下制定风险接受准则，按照该准则确定何种等级的风险为不可接受风险，该准则在《信息安全风险评估管理程序》有详细规定，并在《风险评估报告》中进行系统汇报并针对结果处理意见获得最高管理者批准。

h）获得最高管理者对建议的残余风险的批准，残余风险应该在《残余风险评价报告》上留下记录，并记录残余风险处置批示报告。

i）获得管理者对实施和运行 ISMS 的授权。ISMS 管理者代表(dàibiǎo)的任命和授权、ISMS 文档的签署可以作为实施和运作 ISMS 的授权证据。

1.5.1.1.信息安全风险(fēngxiǎn)处置

1.5.1.1.2风险处理方法(fāngfǎ)的识别与评价

信息安全管理小组应组织有关部门(bùmén)根据风险评估的结果，形成《风险处理计划》，该计划应明确风险处理责任部门、方法及时间。

对于信息安全风险，应考虑控制措施与费用的平衡原则，选用以下适当(shìdàng)的措施：

a）采用适当的内部控制措施；

b）接受某些风险（不可能将所有风险降低为零）；

c）回避某些风险（如物理隔离）；

d）转移某些风险（如将风险转移给保险者、供方、分包商）。

1.5.1.1.2选择控制目标与控制措施

信息安全管理小组根据信息安全方针、业务发展要求及风险评估的结果，组织有关部门制定信息安全目标。信息安全目标应获得总裁的批准。

控制目标及控制措施的选择原则来源于附录 A 。本公司根据信息安全管理的需要，可以选择标准之外的其他控制措施。

1.5.1.1.2适用性声明 SoA

信息安全管理小组编制《信息安全适用性声明》（SoA ）。该声明包括以下方面的内容：

a）所选择控制目标与控制措施的概要描述；

b）对 ISO/IEC 27001:2013附录 A 中未选用的控制目标及控制措施理由的说明。

1.5.1.1.2残余风险

对风险处理后的残余风险应形成《残余风险评估报告》并得到信息安全最高责任人的批准。信息安全管理小组应保留信息安全风险处置过程的文件化信息。

1.5.2信息安全目标和实现规划

根据公司的信息安全方针，经过最高管理者确认，公司的信息安全管理目标为：

顾客保密性抱怨/投诉的次数不超过 1 起/年。

受控信息泄露的事态发生不超过 3 起/年

秘密信息泄露的事态不得发生。

信息(xìnxī)安全管理小组根据《适用性声明》、《信息资产风险评估表》中风险处理(chǔlǐ)计划所选择的控制措施，明确控制措施改进时间表。对于(duìyú)各部门信息安全目标的完成(wán chéng)情况，按照《信息安全目标及有效性测量(cèliáng)程序》的要求，周期性在主责部门对各控制措施的目标进行测量，并记录测量的结果。通过定期的内审、控制措施目标测量及管理评审活动评价公司信息安全目标的完成情况。

1.6支持

1.6.1资源

总经理负责确定并提供建立、实施、保持和持续改进信息安全管理体系所需的资源。

1.6.2能力

办公室应：

a）确定公司全体员工影响公司信息安全绩效的必要能力；

b）确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c）适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d）保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，对新入职员工进行的信息安全意识教育；定期对公司员工进行的业务实施过程中的信息安全管理相关的培训等。

1.6.3意识

公司全体员工应了解：

a）公司的信息安全方针；

b）个人其对公司信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；

c）不符合信息安全管理体系要求带来的影响。

1.6.4沟通

信息安全管理小组负责确定与信息安全管理体系相关的内部和外部的沟通需求，包括：

a）沟通内容；

b）沟通时间；

c）沟通对象；

d）谁应负责沟通；

e）影响沟通的过程。

1.6.5文件(wénjiàn)化信息

1.6.5.1总则(zǒngzé)

公司(gōng sī)的信息安全管理体系应包括：

a）本标准要求(yāoqiú)的文件化信息；

b）信息安全管理小组确保信息安全管理体系的有效运行，需编制《文件控制程序》用以管理公司(gōng sī)信息安全管理体系的相关文件。

1.6.5.2创建和更新

创建和更新文件化信息时，信息安全管理小组应确保适当的：

a）标识和描述（例如标题、日期、作者或编号）；

b）格式（例如语言、软件版本、图表）和介质（例如纸质、电子介质）；

c）对适宜性和充分性的评审和批准。

1.6.5.3文件化信息的控制

信息安全管理体系及本标准所要求的文件化信息应予以控制，以确保：

a）在需要的地点和时间，是可用和适宜的；

b）得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。

c）为控制文件化信息，适用时，科技规划部应开展以下活动：

d）分发，访问，检索和使用；

e）存储和保护，包括保持可读性；

f）控制变更（例如版本控制）；

g）保留和处置。

信息安全管理小组需在《文件控制程序》中规划和运行信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

1.7运行

1.7.1运行规划和控制

为确保 ISMS 有效实施，对已识别的风险进行有效处理，本公司开展以下活动：

a）形成《信息安全风险处理计划》，以确定适当的管理措施、职责及安全保密控制措施的优先级，应特别注意公司外包过程的确定和控制；对于系统集成和 IT 外

包运维服务项目，项目经理应在项目策划阶段识别所面临的信息安全风险，并在项目全过程中对信息安全风险进行监控和更新。

b）为实现(shíxiàn)已确定的安全保密(bǎo mì)目标、实施风险处理计划，明确各岗位(gǎng wèi)的信息安全职责；

c）实施(shíshī)所选择的控制措施，以实现控制目标的要求；

d）进行(jìnxíng)信息安全培训，提高全员信息安全意识和能力；

e）对信息安全体系的运作进行管理，控制计划了的变更，评审非预期变更的后果，必要时采取措施减缓负面影响；

f）对信息安全所需资源进行管理；

g）实施控制程序，对信息安全事故（或事件）进行迅速反应。

总经理为本公司信息安全最高责任者。

办公室制定全公司的组织机构和各部门的职责（包括信息安全职责），并形成文件。

信息安全管理小组成员负责完成信息安全管理体系运行时必须的任务；对信息安全管理体系的运行情况和必要的改善措施向信息安全最高责任者报告。

各部门负责人作为本部门信息安全的主要责任人，信息安全内审员负责指导和监督本部门信息安全管理体系的运行与实施，并形成文件；全体员工都应按保密承诺的要求自觉履行信息安全义务。

各部门应按照《信息安全适用性声明》中规定的安全保密目标、控制措施（包括安全保密运行的各种控制程序）的要求实施信息安全控制措施。

信息安全管理小组应对满足信息安全要求及实施 6.1中确定的措施所需的过程予以规划、实施和控制，同时应实施计划以实现 6.2中确定的信息安全目标。

信息安全管理小组应保持文件化信息达到必要的程度，以确信过程按计划得到执行。

信息安全管理小组应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻负面影响。

各部门确定本部门业务过程中的外包活动，并对外包过程进行必要的控制。

1.7.2信息安全风险评估

公司按照组织《信息安全风险评估管理程序》的要求，每年定期或当重大变更提出或发生时，执行信息安全风险评估。每次风险评估的过程均需形成记录，并由信息安全管理小组保留每次风险评估的记录，如：风险评估报告、风险处理计划等。

1.7.3信息安全风险处置

为确保 ISMS 有效实施，对已识别的风险进行有效处理，本公司开展以下活动：

a) 形成《风险处理计划》，以确定适当的管理措施(cuòshī)、职责及安全保密控制措施的优先级；

b) 为实现已确定的安全保密目标、实施风险处理(chǔlǐ)计划，明确各岗位的信息安全职责；

c) 实施(shíshī)所选择的控制措施，以实现控制目标的要求；

d) 进行信息安全培训(péixùn)，提高全员信息安全意识和能力；

e) 对信息安全体系的运作进行(jìnxíng)管理；

f) 对信息安全所需资源进行管理；

信息安全管理小组负责组织相关人员，定期检查风险处理计划的执行情况，并保留信息安全风险处置结果的文件化信息。

1.8绩效评价

1.8.1监视、测量、分析和评价

本公司通过实施定期的控制措施实施有效性检查、事故报告调查处理、电子监控、技术检查等检查方式检查信息安全管理体系运行的情况，并报告结果以实现：

a) 及时发现信息安全体系的事故和隐患；

b) 及时了解信息处理系统遭受的各类攻击；

c) 使管理者掌握信息安全活动是否有效，并根据优先级别确定所要采取的措施；

d) 积累信息安全方面的经验。

按照计划的时间间隔（不超过一年）进行 ISMS 内部审核，内部审核的具体要求。

根据控制措施有效性检查和内审检查的结果以及来自相关方的建议和反馈，由最高责任者主持，每年对 ISMS 的有效性进行评审，其中包括信息安全范围、方针、目标及控制措施有效性的评审。

管理者代表应组织有关部门按照《信息安全风险评估管理程序》的要求对风险处理后的残余风险进行定期评审，以验证残余风险是否达到可接受的水平，对以下方面变更情况应及时进行风险评估：

a) 组织机构发生重大变更；

b) 信息处理技术发生重大变更；

c）公司业务目标及流程发生重大变更；

d）发现(fāxiàn)信息资产面临重大威胁；

e）外部环境，如法律法规或信息安全标准发生(fāshēng)重大变更。

保持上述活动和措施(cuòshī)的记录。

以上活动(huó dòng)的详细程序规定于以下文件中：

《控制措施有效性的测量(cèliáng)程序》

《信息安全职责权限划分对照表》

《信息安全风险评估管理程序》

《内部审核控制程序》

1.8.2内部审核

内部信息安全审核主要指内部信息安全管理体系审核，其目的是验证公司信息安全管理体系运行的符合性和有效性并不断改进和完善公司的信息安全管理体系。

1.8.2.1组织审核

a）公司统一组织、管理内部信息安全审核工作，信息安全管理小组负责制定《内部审核控制程序》并贯彻执行；

b）管理者代表负责领导和策划内部审核工作，批准年度内审计划和追加审核计划，批准审核组成员，批准审核实施计划，审批年度内审报告；

c）信息安全管理小组负责对审核组长及成员提名，编制年度审核计划和追加审核计划，报管理者代表批准后执行。

d）审核组长组织和管理内部审核工作，根据实际情况和重要性安排审核顺序实施审核。

e）审核员不应审核自己的工作。

1.8.2.2实施审核

a）审核组长编制的审核计划，经管理者代表批准后，负责在实施审核前5天向被审核方发出书面审核通知；

b）审核小组按《内部审核控制程序》实施审核；

c）审核员收集客观证据，通过分析整理做出公正判断，填写《内审不合格报告》提交审核组长，并请被审核部门经理在报告上签字认可。

1.8.2.3审核报告

审核组长应在完成全部审核后，按规定格式编写《内部管理体系审核报告》提交信息安全管理小组，经其审阅后报管理者代表，《内部管理体系审核报告》作为管理评审的输入(shūrù)证据。

1.8.2.4纠正(jūzhèng)措施和跟踪验证

a）被审核部门经理制定纠正措施，填写在《内审不合格(hégé)报告》中。

b）纠正措施完成后后，应将纠正措施完成情况填写(tiánxiě)到《内审不合格报告》相应栏内，然后将《内审不合格报告》交到审核组长。

c）审核(shěnhé)组长视具体情况通知审核组复查，跟踪验证纠正措施实施情况，并将验证结果填写在《内审不合格报告》中。

1.8.2.5审核记录

审核组长应收集所有内部信息安全审核中发生的计划通知、内部审核检查表、记录、审核报告、总结等原始资料，整理后由信息安全管理小组负责保管内审相关记录。

1.8.3ISMS管理评审

1.8.3.1总则

信息安全最高责任者为确认信息安全管理体系的适宜性、充分性和有效性，每年对信息安全管理体系进行一次全面评审。该管理评审应包括对信息安全管理体系是否需改进或变更的评价，以及对信息安全方针和信息安全管理目标的评价。管理评审的结果应形成书面记录，并至少保存 3 年，按照《文件控制程序》的要求进行受控访问。

1.8.3.2管理评审的输入

在管理评审时，信息安全管理小组应组织相关部门提供以下资料，供信息安全管理最高责任者和各部门负责人进行评审：

a）ISMS 体系内、外部审核的结果；

b）相关方的反馈（投诉、抱怨、建议）；

c）可以用来改进 ISMS 业绩和有效性的新技术、产品或程序；

d）信息安全目标达成情况，纠正和预防措施的实施情况；

e）信息安全事故或征兆，以往风险评估时未充分考虑到的薄弱点或威胁；

f）上次管理评审时决定事项的实施情况；

g）可能影响信息安全管理体系变更的事项（标准、法律法规、相关方要求）；

h）对信息安全管理体系改善的建议；

i）有效性测量结果。

1.8.3.管理(guǎnlǐ)评审的输出

信息安全管理最高责任者对以下(yǐxià)事项做出必要(bìyào)的指示：

a）信息安全管理体系有效性的改善(gǎishàn)事项；

b）信息安全方针(fāngzhēn)适宜性的评价；

c）必要时，对影响信息安全的控制流程进行变更，以应对包括以下变化的内外部事件对信息安全体系的影响：

业务发展要求；

信息安全要求；

业务流程；

法律法规要求；

风险水平/可接受风险水平。

d）对资源的需求。

以上内容的详细规定见《管理评审控制程序》。

1.9改进

1.9.1不符合和纠正措施

发生不符合事项的责任部门在查明原因的基础上制定并实施相应的纠正措施，以消除不符和的原因，防止不符合事项再次发生。

信息安全管理小组负责制定《纠正措施控制程序》并组织问题发生部门针对发现的不符合现象分析原因、制定纠正措施，以消除不符合，并防止不符合的再次发生。

对纠正措施的实施和验证规定以下步骤：

a）识别不符合；

b）确定不符合的原因；

c）评价确保不符合不再发生的措施要求；

d）确定和实施所需的纠正措施；

e）记录所采取措施的结果；

f）评审所采取的纠正措施，将重大纠正措施提交管理评审讨论。

1.9.2持续(chí xù)改进

公司的持续(chíxù)改进是信息安全管理体系得以持续保持其有效性的保证，公司在其信息管理体系安全方针、安全目标、安全审核、监视事态的分析、纠正措施以及管理评审方面都要持续改进信息安全管理体系的有效性。

本公司(gōng sī)开展以下活动，以确保 ISMS 的持续改进：

a) 实施每年管理(guǎnlǐ)评审、内部审核、安全检查等活动以确定需改进的项目；

b) 按照《内部审核(shěnhé)管理程序》、《纠正措施管理程序》的要求采取适当的纠正和预防措施；

c) 吸取其他组织及本公司安全事故的经验教训，不断改进安全措施的有效性；

d) 对信息安全目标及分解进行适当的管理，确保改进达到预期的效果；

为了确保信息安全管理体系的持续有效，各级管理者应通过适当的手段保持在公司内部对信息安全措施的执行情况与结果进行有效的沟通。包括获取外部信息安全专家的建议、信息安全政府行政主管部门、电信运营商等组织的联系及识别顾客对信息安全的要求等。如：管理评审会议、内部审核报告、公司内文件体系、内部网络和邮件系统、法律法规评估报告等。

1.10信息安全管理方针方针

公司的信息安全管理(guǎnlǐ)方针：

安全第一(dìyī)，预防为主；全员参与，综治风险；

遵纪守法，提高绩效(jì xiào)；成本可控，持续发展。

对于(duìyú)信息安全方针的解释：

a) 满足客户要求：满足顾客(gùkè)的要求是企业运营的必然选择。

b) 保障信息安全：信息安全是企业管理的重中之重。

c) 遵守法律法规：遵守法律法规是企业生存之前提，满足法律法规及相关行业标准/技术规范的要求也是本公司必须承担的社会责任。

d) 持续改进管理：控制风险是前提，风险自身是动态的过程。通过各种方式提升公司员工的信息安全意识，提高公司的信息安全管理过程。

本公司承诺提供一切可能的资源与先进的技术，保证信息的保密性、可用性和完整性，有针对性地采取一切必要的安全措施。使用有效的风险评估的工具和方法，严格控制风险事故在可接受风险范围之内。制订周密可靠的应急方案并定期进行演练，关键信息数据异地备份，制订业务连续性计划，以确保业务的持续进行。

为了满足适用法律法规及相关方要求，维持计算机系统集成及服务、计算机应用软件的设计开发及服务活动的正常进行，本公司依据 ISO/IEC27001:2013标准，建立信息安全管理体系，以保证与公司经营管理相关信息的保密性、完整性、可用性和可追溯性，实现业务可持续发展的目的。本公司将：

a) 在公司内各层次建立完整的信息安全管理组织机构，确定信息安全方针、安全保密目标和控制措施，明确信息安全的管理职责；

b) 识别并满足适用法律、法规和相关方信息安全要求；

c) 定期进行信息安全风险评估，ISMS 评审，采取纠正预防措施，保证体系的持续有效性；

d) 采用先进有效的设施和技术，处理、传递、储存和保护各类信息，实现信息共享；

e) 对全体员工进行持续的信息安全教育和培训，不断增强员工的信息安全意识和能力；

f) 制定并保持完善的业务连续性计划，实现可持续发展。

上述(shàngshù)方针的批准(pī zhǔn)发布(fābù)及修订(xiūdìng)由公司(gōng sī)信息安全最高责任者负责；通过培训、宣贯等方式使得本公司员工知晓并执行相关内容；通过有效途径告知服务相关方及客户，以提高安全保密意识及服务水平；并定期通过《管理评审控制程序》评审其适用性、充分性，必要时予以修订。

组织的角色，职责和权限

公司经营管理层决定全公司的组织机构和各部门的职责（包括信息安全职责），并形成文件。

各部门的信息安全管理职责决定本部门组织形式和业务分担，并形成文件。

总经理为本公司信息安全最高责任者。各部门/项目组负责人为本部门/项目组信息安全管理责任者，全体员工都应按保密承诺的要求自觉履行信息安全保密义务；

各部门应按照《信息安全适用性声明》中规定的安全目标、控制措施（包括安全运行的各种控制程序）的要求实施信息安全控制措施。

2、制度与规范、业务流程

2.1信息安全与保密管理制度

2.1.1 为了保证项目网络数据的安全保密，维持安全可靠的计算机应用环境，特制定本规定。

2.1.2 凡项目组从事项目管理工作的员工都必须执行本规定。

2.1.3 项目的合同、需求说明、设计变更、工作联系单、工程洽商单、经济签证单、公司内部资料等必须由各部门信息管理员妥善管理，严禁外借，严禁非相关人员传阅、查看。

2.1.4 对接入计算机及设备，必须符合一下规定：

2.1.4.1 在未经许可的情况下，不得擅自对处计算机及其相关设备的硬件部分进行修改、改装或拆卸配置，包括添加光驱、软驱，挂接硬盘等读写设备，以及增加串口或并口外围设备，如扫描仪、打印机等。

2.1.4.2 非我项目的计算机及任何外设，不得接入网络系统。

2.1.4.3 严禁私自开启计算机机箱封条或机箱锁。

2.1.5 凡使用项目配备计算机网络系统的员工，必须遵守以下规定；

2.1.5.1 未经批准，严禁非本项目工作人员使用除计算机及任何相关设备。

2.1.5.2 对新上网使用办公网络系统的员工，由办公室负责上岗前的计算机网络设备系统安全及信息(xìnxī)保密的技术培训工作。

2.1.5.3 未经批准，任何(rènhé)人严禁将其以任何形式（如数据形式：Internet、软盘、光盘(guāng pán)、硬磁盘等；硬拷贝形式：图纸打印、复印、照片等）复制、传输或对外提供。

2.1.5.4 任何员工均不得超越权限侵入网络中未开放(kāifàng)的信息，不得擅自修改入库数据资料和修改他人数据资料。

2.1.6 严格执行国家、有关保密、安全及办公自动化系统的有关法律、法规的规定和要求。各部门应自觉按照(ànzhào)有关规定和要求配合做好保密和信息安全工作。

2.1.7 任何经由我公司外网接入互联网的员工，必须严格遵守国家有关法律、法规。

2.1.8 凡使用公司网络系统的员工，必须配合网络管理员做好防病毒工作。

2.1.8.1 由办公室负责网络防病毒工作。信息维护员负责实施防病毒的日常管理工作。

2.1.8.2 凡装有可与外界进行数据传输的设备的计算机，必须安装防病毒程序，办公室定期对防病毒程序进行升级，增强对病毒的查杀能力。

2.1.8.3 凡需入网传输数据的盘片，由网络管理员负责检查、清查计算机病毒，确保没有病毒后方可传输数据。

2.1.8.4 员工在使用过程中如发现计算机病毒，应立即停止进行任何程序并报告网络管理员，如遇到现有防病毒程序无法清杀的病毒，网络管理员必须先将受感染的计算机从网络上隔开，协助员工做好数据备份工作，并为用户恢复系统。

2.1.9 分公司办公室定期对有关部门进行计算机网络系统安全和数据保密检查，并将检查结果向处保密工作小组汇报。

2.1.10 涉及项目信息安全与保密的管理人员均需要对本制度相关具体要求，进行保密工作承诺。

2.2文件(wénjiàn)加密管理制度

2.2.1目的(mùdì)

为规范(guīfàn)公司重要文件的安全管理级别，通过文件外发控制以及加密管理，防止公司机密文件外泄，保障公司信息安全。

2.2.2范围(fànwéi)

本管理制度适用于所有安装加密(jiā mì)软件用户。

2.2.3重要文件定义

需要保护的公司重要电子文档包含：公司财务数据，公司人员信息总表，各部门培训课件，采购部商品分析表，薪资表，工程图纸，市场部合同信息，公司 vip信息汇总表。

2.2.4职责与权限

所有安装加密软件用户必须按照本制度规定进行执行；网管负责人负责加密软件的日常维护，安装管理，以及加密软件权限分配；综合部负责监管。

2.2.5规定描述：

2.2.5.1文件加密类型　目前对所有安装加密软件的用户电脑的重要文件进行加密处理。

2.2.5.2文件传播方式控制

2.2.5.3禁止通过复制/剪贴方式进行外发信息；

2.2.5.4重要文件在创建或编辑时必须在指定机器上操作并进行加密。所有通过 U 盘、E-mail、QQ 、MSN 等工具传送的重要文件，都必须经过部门主管许可才允许。

2.2.5.5公司部提倡远程工作及登录服务器，如有必要(bìyào)需进行申请，开放端口，并通过加密的方式进行通讯。

2.2.5.6文件外发控制(kòngzhì)管理