

信息安全总体方针及安全策略

一、 总则

1. 目的

本文件为了深入贯彻落实国家信息安全政策文件要求和信息安全等级保护政策要求，加强大象集团的信息安全管理工作，增强公司全员信息安全意识，切实提高公司信息系统安全保障能力，特制定本文件。

2. 适用范围

适用于公司所有信息安全活动。

3. 职责

由信息安全领导委员会负责本方针文件的审核和修订，由信息安全局为主体的信息安全日常工作小组负责本方针文件的贯彻和执行。

4. 符合性

本方针文件主要遵循《信息安全技术信息系统安全等级保护基本要求（GBT 22239-2008）》标准的要求，同时在部分环节也符合以下两个国际标准。

ISO/IEC 27001 信息安全管理体系要求

ISO/IEC 27002 信息技术—安全技术—信息安全管理实践规范

二、 信息安全总体方针

公司总体安全方针为：提高人员信息安全风险意识、技术为主、管理为辅，确保公司信息系统安全；强化信息安全管理，坚持以人为本。

三、方针主要内容

1. 主要安全策略

(1) 信息安全是公司及相关管理部门正常经营的重要保障，公司将遵照“统一规划、分级管理、积极防范、人人有责”的原则，通过风险评估和风险管理，采取一切可能的措施，加强公司信息安全的建设和管理。

(2) 公司设立信息安全领导委员会，信息安全领导委员会是公司信息安全管理最高机构；下设两个职能小组：信息安全日常工作组和信息安全应急工作组。分别负责信息安全日常工作和紧急事务。

(3) 公司全体职工均有参与信息安全管理、保护公司及相关管理部门信息安全的义务和责任。公司全体职工应积极参加各种形式的信息安全教育培训，遵守相关国家法律、法规、部门规章和行业规范，遵守公司信息安全管理制

(4) 承载信息系统的所有软硬件设施及物理环境均应受到适当的保护。

(5) 采取必要的措施保护公司信息的机密性，以防止未经授权的不当存取；同时应确保信息不会在传递的过程中，或因无意间的行为透漏给未经授权的第三者。

(6) 采取必要的措施确保公司信息的完整性，以防止未经授权的篡改。

(7) 采取必要的措施确保公司信息的可用性，以确保使用者需求可以得到满足。

(8) 采取必要的措施确保公司信息的连续性，以确保业务持续可用。

(9) 公司相关的信息安全措施或规范应符合现行法令、法规的要求。

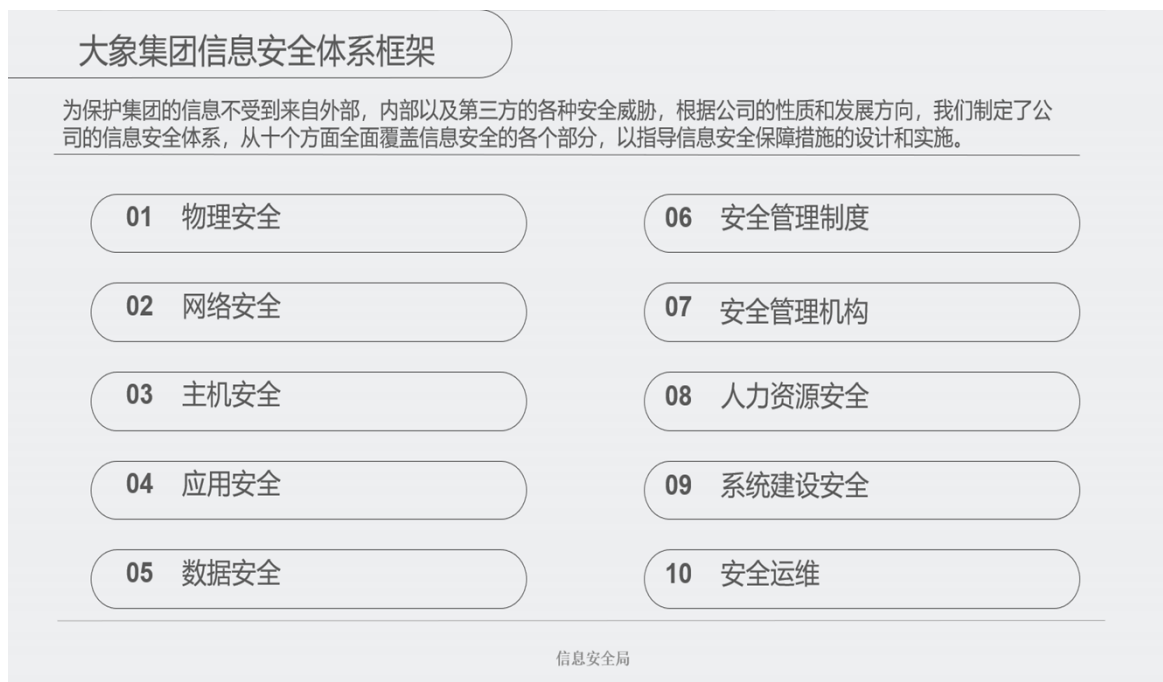
(10) 公司全体员工都有责任通过适当的上报机制，报告所发现的信息安全意外事故或信息安全弱点。

(11) 任何危及信息安全的行为，都应诉诸适当的惩罚程序或法律行动。

2. 信息安全目标

最大限度保证信息系统的完整性、保密性和可用性免遭破坏。确保每年信息安全重大事故的发生频率为可控范围内的最低。

3. 信息安全体系框架



公司信息安全体系框架通过各环节的不断完善，实现信息安全管理体制自身的持续改进，从而提高信息安全管理体制的全面性、有效性和适用性。

4. 信息安全管理原则

（1）基于安全需求原则：公司核心业务信息系统和互联网应用根据等级保护要求，定级为三级，安全需求主要参照三级等级保护要求，同时考虑可能受到的威胁及面临的风险分析安全需求，遵从三级等级保护的规范要求，从全局上恰当地平衡安全投入与效果。

（2）主要领导负责原则：信息安全领导小组的主要领导确立公司信息安全保障的宗旨和政策，负责提高全员的安全意识，组织有效的安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效。

(3) 全员参与原则：跟核心业务信息系统和互联网应用相关的所有运行维护人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全；

(4) 持续改进原则：安全管理是一种动态反馈过程，贯穿整个安全管理生命周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性；

(5) 依法管理原则：信息安全管理主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响；

(6) 选用成熟技术原则：成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的失误；

(7) 管理与技术并重原则：坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

四、 附则

1. 本文件由信息安全局负责解释和修订。
2. 本文档自发布之日起开始执行。