关于安全管理制度的管理标准

1 引言

本标准阐述了广州国为信息科技有限公司（以下简称“公司”）在信息安全管理制度方面的基本任务和管理原则，确定了公司在信息安全管理制度方面的职责和义务，明确了公司信息安全管理制度在编写、制定和发布、评审和修订等过程中应遵守的原则与工作方式及流程。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡注明日期的引用文件，其随后所有的修改单或修订版均不适用于本标准（不包括勘误、通知单），然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡未注日期的引用文件，其最新版本适用于本标准

《信息安全技术 信息系统安全保障评估框架》（GB/T 20274.1-2006）

《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006 ）

《信息安全技术 信息系统安全等级保护基本要求》（GBT 22239-2008）

本标准未涉及的管理内容，参照国家、电力行业、南方电网公司的有关标准和规定执行。

3 目标

总体目标：为贯彻执行国家、地方和本行业有关信息化建设的方针政策，有效保障公司信息系统正常运行。公司信息系统管理的规范化、程序化、制度化，进一步提高管理制度的体系化和制定发布流程的标准化，特制定本制度。为更好的适应公司的企业文化，本标准参照南方电网信息安全管理制度的相关要求，并借鉴了国内外流行标准。

具体建设目标：

1）建立完整的信息安全管理体系和组织机构，提高信息安全管理的能力，完善各项业务和管理过程中的信息安全措施，确保信息安全管理正规有序。

2）建立完整的信息安全运行体系，实现网络系统安全系统的集中管理和透明化监控，提高对突发事件的应急响应处理能力，保证关键业务应用运行的可用性、可依赖性以及故障恢复能力。

4 术语和定义

本标准采用以下术语和定义。

制度：

对流程具体实施办法的解释，规定必须的关键因素，指明各类表单的填写要求等。

流程：

一个输入到输出的过程，一般以流程图表示，标识关键环节和关键步骤，明确职责分工；

表单：

对每个关键环节进行控制的过程文档，表单文件闭环后作为档案文件进行管理。

一 总体方针

第一章 组织与体制

构筑确保信息安全所必需的组织与体制，明确其责任与权限。

第二章 遵守法令法规

遵守与信息安全有关的法令法规，制定并遵守按基本方针所制定的信息安全相关的规定。

第三章 信息资产的分类与管理

按照重要级别信息资产进行分类，并妥善管理。

第四章 培训与教育

为使相关人员全面了解信息安全的重要性，适当开展针对性培训与教育教育活动。使他们充分认识信息安全的重要性以及掌握正确的管理方法。

第五章 物理性保护

为避免非法入侵、干扰及破坏信息资产等事故的发生，对其保管场所与保管办法加以明确。

第六章 技术性保护

为切实保护信息资产不受来自外部的非法入侵，对信息系统的登录方法、使用限制、网络管理等采取适当的措施。

第七章 运用

为确保基本方针的实际成效，在对遵守情况进行监督的同时，对违反基本方针时的处置办法及针对来自外部的非法入侵等紧急事态采取的应对措施等加以规定。

第八章 评价及复审

随着社会环境的变化、技术的进步等，应定期对基本方针与运用方式进行评价与复审。

¬ 安全策略

第一章 安全管理机构

建立组织管理体系是为了建立自上而下的信息安全工作管理体系，确定安全管理组织机构的职责，统筹规划、专家决策，以推动信息安全工作的开展。

公司成立信息安全领导小组，是信息安全的最高决策机构，负责研究重大事件，落实方针政策，制定实施策略和原则，开展安全普及教育等。下设办公室挂靠在公司信息中心，负责信息安全领导小组的日常事务。

信息安全领导小组下设两个工作组：信息安全工作组、应急处理工作组。

第二章 人员安全管理

通过建立安全岗位责任制，最大限度降低人为失误所造成的风险。人是决定性因素，人员安全管理的原则是：职责分离、有限授权、相互制约、任期审计。

人员安全管理的要素包括：安全管理人员配备、信息系统关键岗位、人员录用、人员离岗、人员考核与审查、第三方人员管理等。

信息安全人员的配备和变更情况，应向上一级单位报告、备案。

信息安全人员调离岗位，必须严格办理调离手续，承诺其调离后的保密义务。涉及 XX 业务核心技术的信息安全人员调离单位，必须进行离岗审计，并在规定的脱密期后，方可调离。

第三章 标准化管理

应通过公司信息系统内部业务处理、操作流程、信息系统管理和技术等一系列标准化和规范化的过程，应根据系统的安全等级，依照国家相关法律法规及政

策标准，建立信息安全的各项管理规范和技术标准，规范基础设施建设、系统和网络平台建设、应用系统开发、运行管理等重要环节，奠定信息安全的基础。

第四章 系统建设管理

信息系统的安全管理贯穿系统的整个生命周期，系统建设管理主要关注的是生命周期中的前三个阶段（初始、采购、实施）中各项安全管理活动。

系统建设管理分别从工程实施建设前、建设过程以及建设完毕交付等三方面考虑，具体包括系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评和安全服务商选择十一个控制点。

第五章 系统运维管理

目的是保障信息系统日常运行的安全稳定，对运行环境、技术支持、操作使用、病毒防范、备份措施、文档建立等全方位管理。包括用户管理、运行操作管理、运行维护管理、外包服务管理、有关安全机制保障、安全管理控制平台等方面的管理要素。

对运行过程的任何变化，数据、软件、物理设置等，都应实施技术监控和管理手段以确保其完整性，防止信息非法复制、篡改，任何查询和变更操作需经过授权和合法性验证。

应急管理也是运维的重要内容，目的是分析信息系统可能出现的紧急事件或灾难，建立一整套应急措施，以保障核心业务的快速恢复和持续稳定运行。应急计划包括应急处理和灾难恢复策略、应急计划、应急计划的实施保障等管理要素。

在公司统一的应急规划下，针对信息系统面临的各种应急场景编制相应的应急预案，并经过测试演练修订，同时宣传普及。

第六章 物理安全

目的是保护计算机设备、设施（含网络）以及信息系统免遭自然灾害和其他形式的破坏，保证信息系统的实体安全。

有关物理环境的选址和设计应遵照相关标准，配备防火、防水、防雷击、防静电、防鼠害等机房措施，维持系统不间断运行能力，确保信息系统运行的安全可靠。

对重要安全设备的选择，需符合国家相关标准规范，相关证书齐全。

严格确定设备的合法使用人，建立详细运行日志和维护记录。

第七章 网络安全

目的是有效防范网络体系的安全风险，为业务应用系统提供安全、可靠、稳定的网络管理和技术平台。

对于依赖网络架构安全的业务应用系统，需根据其安全级别，实施相应的访问控制、身份认证、审计等安全服务机制；在网络边界处，需根据资源的保护等级，实施相应安全级别的防火墙、认证、审计、动态检测等技术，防范信息资源的非法访问、篡改和破坏。

第八章 主机安全

主机安全包括服务器、终端/工作站等在内的计算机设备在操作系统及数据库系统层面的安全。终端/工作站是带外设的台式机与笔记本计算机，服务器则包括应用程序、网络、web、文件与通信等服务器。主机承载着各种应用，是保护信息安全的中坚力量。

主机安全需着重关注和加强身份鉴别、访问控制、恶意代码防范、安全审计、入侵防范几个方面，同时定期或不定期的进行安全评估（含渗透性测试）和加固，实时确保主机的健壮性。

第九章 应用安全

应用安全成是信息系统整体防御的最后一道防线，目的是保障业务应用系统开发过程及最终产品的安全性。

在应用层面运行着信息系统的基于网络的应用以及特定业务应用。基于网络的应用是形成其他应用的基础，是基本的应用；业务应用采纳基本应用的功能以满足特定业务的要求；故最终是保护系统的各种业务应用程序的安全运行。

应用系统的总体需求计划阶段，应全面评估系统的安全风险，确定系统的访问控制、身份认证、审计跟踪等安全需求；总体架构设计阶段，应实施安全需求设计，确立安全服务机制、开发人员技术要求和操作规程；应用系统的实现阶段，应全程实施质量控制，防止程序后门，减少代码漏洞；在上线运行之前，应充分进行局部功能、整体功能、压力测试，以及系统安全性能、操作流程、应急方案的测试。

第十章 数据安全及备份恢复

信息系统处理的各种数据（用户数据、系统数据、业务数据等）在维持系统正常运行上起着至关重要的作用。由于信息系统的各个层面（网络、主机、应用等）都对各类数据进行传输、存储和处理等，因此，对数据的保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。

数据备份也是防止数据被破坏后无法恢复的重要手段，而硬件备份等更是保证系统可用的重要内容。

第十一章 应急计划

目的是分析信息系统可能出现的紧急事件或灾难，建立一整套应急措施，以保障核心业务的快速恢复和持续稳定运行。应急计划包括应急处理和灾难恢复策略、应急计划、应急计划的实施保障等管理要素。

在公司统一的应急规划下，针对信息系统面临的各种应急场景编制相应的应急预案，并经过测试演练修订，同时宣传普及。

¬ 职责分工

a) 信息安全领导小组

领导小组是信息安全的最高决策机构，批准公司信息安全总体策略规划、管理规范和技术标准；确定公司信息安全各有关部门工作职责，指导、监督信息安全工作。

b) 信息安全工作组

贯彻执行公司信息安全领导小组的决议，协调和规范公司信息安全工作；组织有关人员进行信息安全制度类文件的编制（包括成立编制小组）、评审、修订、发布、控制，并监督执行。

c) 信息安全管理人员

信息安全管理人员负责信息安全管理的日常工作；开展信息安全知识的培训和宣传工作，开展信息安全检查工作，对要害岗位人员安全工作进行指导和监督；维护和审查有关安全审计记录，及时发现存在问题，提出安全风险防范对策；及时向信息安全工作领导小组和有关部门、单位报告信息安全事件；并负责信息安全制度类文件的归档、保管。

¬ 制度与发布

信息安全工作组应根据信息安全人员与各部门负责人，了解各部门的安全管理制度现状。结合公司管理需求，提出相应的管理制度起草需求或计划，确定后信息安全工作组组长批准。

批准后组织制度编制项目组，编制流程如下：设计编制目录、流程图设计、制度（实施细则）设计、表单设计。所有相关文档需遵循省公司规定的统一格式，编制完后提交信息安全工作组论证。

信息安全工作组负责对开发流程进行监控指导，以保证开发质量和进度。

文档编制完成后，由项目组组织内部评审，评审须有书面记录。评审要点包括：

文档可行性、可操作性；

文档内部逻辑性，与相关文件匹配性；

文档现行状态（版本、编号）；

文字校对。

根据评审结果，对文档进行修订；如初审时问题较大，修订后再次组织评审。

全局性基础性制度由信息安全工作起草，公司主管副总审核，公司总经理批准后发布。

实施细则由信息安全工作小组组织项目组起草，信息安全工作小组组长审核，公司信息分管副总批准后发布。发布后，信息安全人员负责其发布，确保各相关部门得到最新的有效版本，并有签收记录。

¬ 评审和修订

信息安全工作组应该定期组织相关部门和人员对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

在重大流程改变的情况时，信息安全工作组应该组织相关部门和人员对安全管理制度进行修改或重新编写。

在安全事件发生或执行过程中问题积累到一定程度，信息安全工作组应该组织相关部门和人员对安全管理制度进行升级。

¬ 附 则

1) 本标准由广州国为信息科技有限公司负责解释。

2) 本标准自颁布之日起实行。