中国石化信息系统网络安全责任书

信息系统名称：

业务主管部门：

信息管理部门：

建 设 单 位 ：

运 维 单 位 ：

为贯彻落实《中华人民共和国网络安全法》有关规定，按照《中国石化信息安全管理办法》和《中国石化信息安全责任制暨总部机关各部门（单位）信息安全职责》有关要求，进一步落实网络安全责任，保障信息系统的安全、稳定运行,特签订此责任书。业务主管部门、信息管理部门、建设部门、运维部门郑重承诺如下：

一**、业务主管部门责任**

1.业务主管部门是信息系统网络安全工作第一责任单位。

2.负责落实年度各项网络安全保障工作，确保不发生对集团公司造成影响的重大网络安全事件。

3.负责明确信息系统网络安全保护对象，如关键业务流程和操作、关键业务用户、关键业务数据等，根据业务特点和重要程度提出网络安全需求，包括信息系统变更和废弃时相应的需求。

4.负责确定系统等级保护级别, 根据系统服务中断、信息被篡改或泄露等事件对公司和社会造成的影响程度，形成等级保护预定级报告。

5.负责用户、权限、数据、业务操作等应用安全管理，负责用户账号弱口令治理工作，监督并反馈信息系统安全问题和隐患的整改情况。

6.负责信息系统业务应急预案制定并组织演练，持续完善业务应急机制，做好应急队伍和资源的配备，安排应急值守工作。

7.遵照集团公司网络安全事件（事故）发现、报告、处置等工作机制开展工作。

**二、信息管理部门责任**

1.信息管理部门是信息系统信息安全工作归口管理部门。

2.负责组织协调业务主管部门，进行信息系统的定级、报备、测评、整改工作。

3.负责组织对信息系统的安全需求、技术框架、防护方案等进行论证和审定。

4.负责督导信息系统建设部门，切实落实信息系统的网络安全防护方案，负责会同有关业务主管部门进行网络安全专项验收工作。

5.负责对网络安全方案设计的实现进行验证检查；负责信息系统上线安全检查。

6.负责监督信息系统应急预案的编制和演练工作。

7.负责建立网络安全通报机制，完善重大突发网络安全事件事故报告和应急处置流程。

8.负责向业务主管部门通报信息系统安全漏洞，发布网络安全风险预警、协调处置网络安全事件。

**三、建设单位责任**

1. 按照业务主管部门要求，落实年度各项网络安全保障工作，配合网络安全事件的调查，确保不发生对集团公司造成影响的重大网络安全事件。

2.负责根据信息系统业务主管部门确定的网络安全需求和网络安全等级保护级别，进行安全方案总体设计。

3.负责根据公司信息化项目管理的相关要求，进行网络安全方案的实施工作，对架构设计、开发环境、代码实现和系统测试等环节进行规范约束，确保实施过程安全可控。

4.配合开展系统上线/验收前的网络安全检查和测评工作，负责问题整改，确保安全防护措施与信息系统同步投用。

5.负责信息系统上线运行后、正式移交前的安全运维职责，涉及到系统变更时，严格按照变更流程执行，对重大变更进行安全风险评估。

6. 配合信息系统应急预案制定及演练工作，根据演练结果，配合更新相关信息系统应急方案。

**四、运维单位责任**

1.按照业务主管部门要求，落实年度各项网络安全保障工作，负责信息系统日常运行监控和安全运维工作。配合网络安全事件的调查，确保不发生对集团公司造成影响的重大网络安全事件

2.负责定期对信息系统进行安全自查，开展漏洞扫描、恶意代码检测、安全策略审核、安全配置核查等工作，及时发现安全隐患并整改。

3.负责信息系统运维变更工作，严格按照变更流程执行变更操作，对重大变更进行安全风险评估。

4.配合信息系统相关网络安全制度、流程、标准和规范的制定工作。

5.配合开展信息系统应急演练、安全测评和风险评估等工作。

**填写说明：**

本责任书为项目验收安全检查前签署，由信息系统项目组填写并协调有关部门签署，责任书一式四份，签字、盖章后由签署各方分别留存。

根据“谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”原则，分别落实各方责任。

（签字页）

业务主管部门负责人： 职务：

联系人及电话： （部门签章）

信息管理部门负责人： 职务：

联系人及电话： （部门签章）

建设单位负责人： 职务：

联系人及电话： （单位签章）

建设单位负责人： 职务：

联系人及电话： （单位签章）

运维单位负责人： 职务：

联系人及电话： （单位签章）

签订日期： 年 月 日