中海石油气电集团有限责任公司江苏分公司
信息资产及网络安全管理办法

公司名称：中海石油气电集团有限责任公司江苏分公司

批 准 人：总经理办公会

批准依据：《中海石油气电集团有限责任公司江苏分公司内控制度体系管理办法》（CG-02-01）

发布文号：江苏分公司风险办（2022）3 号

发布日期：2022年 7 月 29 日

生效日期：2022年 7 月 29 日

目　　录

中海石油气电集团有限责任公司江苏分公司
信息资产及网络安全管理办法

1 目的

为明确中海石油气电集团有限责任公司江苏分公司（以下简称“公司”）信息资产及网络安全工作的职责分工、管理内容和管理程序，实现信息资产全生命周期管理，规范网络安全建设管理。

2 适用范围

中海石油气电集团有限责任公司江苏分公司及下属单位。

3 主要应对风险

a）信息资产配置没有充分发挥整体效益；

b）知识产权保护对企业的影响；

c）信息资产全生命周期监控不足，影响决策；

d）安全制度建设不到位产生的风险；

e）网络安全培训与教育不到位产生的风险；

f）网络安全监督、检查管理不到位产生的风险；

g）网络安全技术措施不到位产生的风险；

h）网络安全审计缺失产生的风险。

4 职责分工

4.1 网络安全和信息化领导小组

a）领导公司信息资产及网络安全管理工作；

b）研究、决策公司网络安全重大事项；

c）指导、监督处理公司重大网络安全事故。

4.2 信息化管理部门

a）负责制定公司信息资产管理的策略和规章制度，指导公司信息资产的管理工作；

b）负责公司信息资产产权登记，组织信息资产的建账工作与管理；

c）负责组织公司信息资产的清查、统计、报告和日常监督检查工作；

d）负责公司通用系统软件的账户管理及业务数据管理工作；

e）对公司信息资产进行日常管理。

f）负责网络和信息系统、工控系统的网络安全管理和建设；

g）组织制订和完善公司网络安全规章制度、标准规范以及通信安全生产和应急保障的相关管理规定；

h）负责指导、组织开展网络安全管理工作；

i）负责监督和检查网络安全策略及规划的执行情况；

j）负责组织开展公司网络安全教育和检查；

k）负责组织和处理公司重大网络安全事故

4.3 财务资金部

a） 负责公司信息固定资产和软件资产的相关账务处理；

b） 参与公司信息固定资产和软件资产的财务相关管理工作。

4.4 各部门及所属单位

a） 负责本部门信息资产登记与管理；

b） 协助信息化管理部门进行信息资产管理工作；

c） 负责本部门自建专用信息系统的账户管理及业务数据管理工作；

d） 对本部门所拥有的信息系统及系统使用人员进行安全管理监督；

e） 落实公司网络安全相关要求，支持、配合信息化管理部门做好网络安全工作。

5 管理内容及要求

5.1 信息资产管理范围

5.1.1 公司信息资产管理的范围包括提供基础服务的硬件及设施、系统软件、各种与信息化建设和应用相关的文件、系统账户、业务数据等。

5.1.2 公司提供基础服务的硬件及设施，包括但不限于：

a）服务器，包括小型机、PC 服务器、虚拟机；

b）存储设备，包括磁盘阵列、SAN 交换机、磁带库、其他；

c） 网络设备，包括路由器、交换机、防火墙、VPN 网关、QoS 设备及其他网络设备

d） 机房环境设备，包括空调设施、电源设施、监控设施、消防设施等。

5.1.3 各类通用及专用系统软件账户，包括但不限于 NOTES 账户、SAP 账户、VPN 账户、邮箱账户、AD 域账户、互联网账户，及其他专用信息系统账户。

5.1.4 各系统业务数据，包括但不限于物资、供应商、客户、设备、财务、销售、薪酬、员工、生产、销售等业务数据。

5.2 信息资产的购置管理

5.2.1 进行信息固定资产和软件资产的采购时，应遵守公司采办相关管理办法和规定。

5.2.2 需要使用气电集团统一采购软件的部门，应向信息化管理部门提交使用申请，信息化管理部门报送气电集团信息部批准后，将软件资源发放到使用部门。

5.2.3 信息化建设项目竣工后，项目组或承建方应向信息化项目立项部门进行交接，并办理交接手续。

5.2.4 信息化项目立项部门和信息化管理部门在信息化建设项目完工时，应对信息资产进行验收，信息化项目立项部门办理资产接收手续；并向资产管理归口部门备案登记。

5.2.5 机房环境设备的采购由对应专业负责，相关设备设施需登记在信息固定资产登记表台账上。

5.3 信息资产维护使用

5.3.1 硬件/软件投入使用后，信息资产管理人应填写《信息固定资产登记表》（见附件 3）或《信息软件资产登记表》（见附件 4），并报送信息化管理部门。

5.3.2 气电集团或公司统一部署系统的账号申请应严格审查，按需求发放，杜绝浪费。

5.3.3 软件发放后，介质和许可证由使用人保管，如因保管人原因导致许可信息泄露或介质丢失，造成的信息资产损失，责任应由使用人负责。

5.3.4 各部门应严格按申请数量安装使用软件，否则因此产生的后果由申请部门负责。

5.4 信息资产维护使用

5.4.1 信息固定资产应统一编号，贴有统一标识的标签，标签内容应包含使用部门，硬件使用负责人，用途及其他相关信息（如 IP、配置、所安装的软件版本等）。

5.4.2 信息固定资产的使用说明书、保修卡、光盘介质等随机物品应由使用人统一保管。

5.4.3 业务数据的管理应遵循“谁生产的数据，谁负责维护，并保证数据的质量，

即数据的准确性、实时性等”的总体原则。

5.4.4 业务系统数据的授权管理遵循分级授权、分级管理的总体原则。

5.4.5 机房环境设备的维护由对应专业负责，相关设备设施需登记在信息固定资产登记表台账上。

5.5 信息资产报废

5.5.1 信息资产报废管理工作，遵照《中海石油气电集团有限责任公司江苏分公司信息资产报废管理细则》执行。

5.5.2 人员离职或离岗，所涉及到的信息资产应及时处理，避免信息资产闲置或浪费。

5.5.3 信息资产在报废过程中应加强信息安全处置。

5.5.4 机房环境设备的报废由对应专业人员负责，相关设备设施需登记在信息固定资产登记表台账上。

5.6 网络安全管理机构要求

5.6.1 机构设置和人员配备

5.6.1.1 应明确网络安全工作分管领导、责任部门、工作专员，并定义相关职责。

5.6.1.2 应配备系统管理员、网络管理员、安全管理员等，并定义各个工作岗位的职责、分工和技能要求。

5.6.2 授权与审批

5.6.2.1 应根据部门和岗位职责，明确授权审批事项、审批部门和批准人等。

序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。

5.6.2.3 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

5.6.2.4 应记录审批过程并保存审批文档。

5.6.3 沟通和合作

5.6.3.1 应加强各类管理人员之间、组织内部机构之间以及网络安全责任部门 内部的合作与沟通，定期或不定期召开协调会议，共同协作处理网络安全问题。7.6.3.

5.6.3.2 应加强与内部单位、公安机关、电信公司的合作与沟通。

5.6.3.3 应加强与供应商、业界专家、专业安全公司、安全组织的合作与沟通。

5.6.3.4 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和

联系方式等信息。

5.6.4 审核和检查

5.6.4.3 应定期安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

5.6.4.4 应由内部人员或上级单位定期全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

5.6.4.5 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

5.6.4.6 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

5.7 人员网络安全管理要求

5.7.1 人员安全培训及教育

5.7.1.1 应制定网络安全培训计划，开展网络安全教育和培训，网络安全教育与培训结果应有书面记录。

5.7.1.2 网络安全教育与培训的内容主要包括：

a) 网络安全相关法律法规、要求、标准、制度等；

b) 信息系统的使用与网络安全管理知识；

c) 网络安全要求、标准、制度、法律法规等发生重大调整和变更的内容；

d) 信息系统的新建和升级对用户使用产生的影响与风险，包括系统变更所带来的网络安全权限和责任变化等。

5.7.2 员工信息系统使用安全

员工信息系统使用安全管理原则：不单独、限制使用期限、责任分散、最小权限。

5.8 网络安全控制管理要求

5.8.1 物理安全管理要求

5.8.1.1 物理位置的选择

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

5.8.1.2 物理访问控制

a) 机房出入口应安排专人值守，控制、鉴别和记录进入人员；

b）需进入机房的来访人员，应经过申请和审批流程，并限制和监控其活动范围；

c）应对机房划分区域进行管理，区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

d）重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

5.8.1.3 防盗窃和防破坏

a）应将主要设备放置在机房内；

b）应固定设备或主要部件，并设置明显不易除去的标记；

c）应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

d）应对介质分类标识，存储在介质库或档案室中；

e）应利用光、电等技术设置机房防盗报警系统；

f）对机房设置监控报警系统。

5.8.1.4 防雷击

a）机房建筑应设置避雷装置；

b）应设置防雷保安器，防止感应雷；

c）机房应设置交流电源地线。

5.8.1.5 防火

a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b）机房及相关工作房间和辅助房应采用具有耐火等级的建筑材料；

c）机房应采取区域隔离防火措施，将重要设备与其他设备隔离。

5.8.1.6 防水和防潮

a）水管安装不得穿过机房屋顶和活动地板下；

b）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

c）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

d）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

5.8.1.7 防静电

a）主要设备应采取必要的接地防静电措施；

b）机房应采用防静电地板。

5.8.1.8 温湿度控制

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所要求的范围内。

5.8.1.9 电力供应

a) 应在机房供电线路上配置稳压器和过电压防护设备；

b) 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行；

c) 应设置冗余或并行的电力电缆线路为计算机系统供电；

d) 应建立备用供电系统。

5.8.1.10 电磁防护

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离铺设，避免互相干扰；

c) 应对关键设备和磁介质实施电磁屏蔽。

5.8.2 主机安全管理要求

5.8.2.1 身份鉴别

a) 应对登录操作系统的用户进行身份标识和鉴别；

b) 操作系统管理用户身份标识应不易被冒用，口令应有复杂度要求并定期更换；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 当远程管理服务器时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

e) 应为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；

f) 应采取两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

5.8.2.2 访问控制

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；

b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c) 应限制默认账户的访问权限，重命名系统默认账户，修改账户默认口令；

d) 应及时删除多余、过期账户，避免存在共享账户；

e) 应对重要信息资源设置敏感标记；

f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.8.2.3 安全审计

a) 审计范围应覆盖服务器上的每个操作系统用户；

b) 审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内容重要的安全相关事件；

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d) 应根据记录数据进行分析，并生成审计报表；

e) 应保护审计进程，避免未预期的中断；

f) 应保护审计记录，避免未预期的删除、修改或覆盖等。

5.8.2.4 剩余信息保护

a) 存放在硬盘或内存中的操作系统和数据库系统用户的鉴别信息应当在其存储空间被释放或再分配给其他用户前完全清除；

b) 系统内的文件、目录和数据库记录等资源应当在被释放或重新分配给其他用户前完全清除。

5.8.2.5 入侵防范

a) 应能够检测到对重要服务器的入侵行为，能够记录入侵的源 IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时报警；

b) 应能够检测重要程序的完整性，并在检测到完整性受到破坏后具有恢复的措施；

c) 操作系统应遵循最小安装原则，仅安装需要的组件和应用程序，并及时更新系统补丁。

5.8.2.6 恶意代码防范

a) 应安装防恶意代码软件，并及时更新防恶意代码软件的版本和恶意代码库；

b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

d) 应支持防恶意代码软件的统一管理

5.8.2.7 资源控制

a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b）应监视重要服务器，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；

c）应根据安全策略设置登录终端的操作超时锁定或断开

d）应限制单个用户对系统资源的最大或最小使用限度；

e）应能够检测系统的服务水平，降低到预先规定的最小值时系统自动报警。

5.8.3 数据库安全管理要求

5.8.3.1 身份鉴别

a）应对数据库系统的用户进行身份标识和鉴别；

b）数据库系统管理用户身份标识应不易被冒用，口令应有复杂度要求并定期更换；

c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d）当远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

e）应为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；

f）应采取两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

5.8.3.2 访问控制

a）应启用访问控制功能，依据安全策略控制用户对资源的访问；

b）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c）应实现操作系统和数据库系统特权用户的权限分离；

d）应限制默认账户的访问权限，重命名系统默认账户，修改账户默认口令；

e） 应及时删除多余、过期账户，避免存在共享账户；

f） 应对重要信息资源设置敏感标记；

g） 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.8.3.3 安全审计

a）审计范围应覆盖服务器上的每个数据库用户；

b）审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内容重要的安全相关事件；

c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d）应根据记录数据进行分析，并生成审计报表；

e）应保护审计进程，避免未预期的中断；

f）应保护审计记录，避免未预期的删除、修改或覆盖等。

5.8.3.4 入侵防范

数据库系统应遵循最小安装原则，仅安装需要的组件和应用程序，并及时更新系统补丁。

5.8.3.5 资源控制

a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b）应根据安全策略设置登录终端的操作超时锁定或断开；

c）应限制单个用户对系统资源的最大或最小使用限度。

5.8.4 网络和安全设备管理要求

5.8.4.1 结构安全

a）应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；

b）应保证网络各个部分的带宽满足业务高峰期需要；

c）应在业务终端与业务服务器之间进行路由控制，建立安全的访问路径；

d）应绘制与当前运行情况相符的网络拓扑结构图；

e）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为子网、网段分配地址；

f）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

g）应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

5.8.4.2 边界完整性检查

a）应能够检测非授权设备私自连接内部网络的行为，准确定位，并对其

进行有效阻断；

b）应能够检测内部网络用户私自连接外部网络的行为，准确定位，并对其进行有效阻断。

5.8.4.3 入侵防范

a）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

b）当检测到攻击行为是，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

5.8.4.4 恶意代码防范

a）应在网络边界处对恶意代码检测和清除；

b）应维护恶意代码库的升级和检测系统的更新。

5.8.4.5 访问控制

a）应在网络边界部署访问控制设备，启用访问控制功能；

b）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

c）应过滤进出网络的信息内容，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

d）应在会话处于非活跃一定时间或会话结束后终止网络连接；

e）应限制网络最大流量数及网络连接数量；

f）重要网段应采取技术手段防止地址欺骗；

g）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

h）应限制具有拨号访问权限的用户数量。

5.8.4.6 安全审计

a）应通过日志记录网络系统中的网络设备运行状况、网络流量、用户行为等；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c）应根据记录分析，并生成审计报表；

d) 应保护审计记录，避免未预期的删除、修改或覆盖等。

5.8.4.7 网络设备防护

a) 应鉴别登录网络设备的用户身份；

b) 应限制网络设备的管理员登录地址；

c) 网络设备用户的标识应唯一；

d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

e) 身份鉴别信息应不易被冒用，口令应有复杂度要求并定期更换；

f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

g) 当远程管理网络设备时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

h) 应实现设备特权用户的权限分离。

5.8.5 应用和备份恢复管理要求

5.8.5.1 身份鉴别

a) 应提供专用的登录控制模块标识，鉴别登录用户身份；

b) 应对同一用户采取两种或两种以上组合的鉴别技术实现用户身份鉴别；

c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

5.8.5.2 访问控制

a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

c) 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限；

d）应授予不同账户为完成各自承担任务所需的最小权限，并形成相互制约的关系；

e）应对重要信息资源设置敏感标记；

f）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.8.5.3 安全审计

a） 应提供覆盖到每个用户的安全审计功能，审计应用系统重要安全事件；

b） 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

c） 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

d） 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.8.5.4 剩余信息保护

a）存放在硬盘或内存中的用户的鉴别信息应当在其存储空间被释放或再分配给其他用户前完全清除；

b）应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前完全清除。

5.8.5.5 通信完整性

密码技术保证通信过程中数据的完整性。

5.8.5.6 通信保密性

a）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；

b）应对通信过程中的整个报文或会话过程加密。

5.8.5.7 抗抵赖

a）应在请求的情况下，为数据原发者或接受者提供数据原发证据的功能；

b）应在请求的情况下，为数据原发者或接受者提供数据接收证据的功能。

5.8.5.8 软件容错

a）应提供数据有效性验证功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

b）应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

5.8.6 数据安全管理要求

5.8.6.1 数据完整性

a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

5.8.6.2 数据保密性

a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；

b) 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

5.8.6.3 备份和恢复

a) 应提供本地数据备份与恢复功能；

b) 应提供异地数据备份功能，利用通信网络将关键数据定时批量传输至备用场地；

c) 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

d) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

5.9 信息系统建设安全管理

5.9.1 信息系统建设立项阶段

a) 应根据业务需求，明确提出信息系统的安全需求，可包括但不限于： 业务连续性、可用性、机密性、完整性、合规性、业务操作记录、身份抗抵赖、数据安全、应用安全、主机安全、网络安全、物理环境、日志记录等安全需求；

b) 应根据等级保护要求，进行系统等级保护的自定级工作。

5.9.2 信息系统设计阶段

a) 应根据信息系统业务和技术方面的安全需求，制定可以满足信息系统安全需求、符合等级保护标准的设计方案《信息系统安全设计子方案》；

b) 应组织相关部门和有关安全技术专家论证、审定总体安全策略、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，并且经过批准后，方可实施。

5.9.3 信息系统实施阶段

a）应指定或授权专门的部门或人员负责管理工程实施过程；

b）应按照《信息系统安全设计子方案》开展信息系统的实施工作；

c）信息系统建设涉及程序开发的，应当执行源代码安全测试。

5.9.4 信息系统上线和验收阶段

a）信息系统实施完成后，应完成信息系统的安全测试，包括配置检查、漏洞扫描和必要的渗透测试等；

b）信息系统实施完成后，应向综合管理部提报上线前安全检查申请，通过综合管理部向气电集团信息部提交上线前安全检查申请。由信息部协调集团公司统一开展上线前安全检查，信息系统实施单位应按照检查结果完成相应的安全整改，并提报复核申请，复核通过后，方可申请上线和验收。

5.10 信息系统安全等级保护

5.10.1 信息系统应根据业务重要程度及系统重要程度划分等级，采用相应技术手段保障其正常运行。

5.10.2 信息系统安全等级保护管理遵照《信息安全等级保护管理办法》（公通字〔2007〕43 号）及气电集团相关规定。

5.11 工控系统网络安全管理要求

5.11.1 连接安全

要求包括但不限于：

a）工控系统信息网络应隔离运行；

b）外部设备或设施不应接入工控系统。

5.11.2 组网安全

要求包括但不限于：

a）工控系统组网时要同步规划、同步建设、同步运行安全防护措施；采取虚拟专用网络（VPN）、线路冗余备份、数据加密等措施，加强对工控系统远程通信的保护；

b）对无线组网采取身份认证、安全监测等防护措施，防止经无线网络进行恶意入侵，尤其要防止通过侵入远程终端单元（RTU）进而控制部分或整个工控系统。

5.11.3 配置安全

5.11.4

应符合 Q/HS 5036 相关规定的基础上，还应包括但不限于：

a) 建立控制服务器等工控系统关键设备的安全配置和审计制度；

b) 根据工作需要分类设置账户权限；

c) 工控系统正式投产前，及时修改工控系统及相关设备的出厂密码或静默密码；

d) 账户密码符合：

Ⅰ）长度为至少 12 位；

Ⅱ）组成不应包含用户的账户名以及账户名中超过两个连续字符的部分；

Ⅲ）至少应包含以下四类字符中的三类字符：英文大写字母（A-Z）、英文小写字母（a-z）、10 个基本数字（0-9）、非字母字符（例如!、$、#、%）；

Ⅳ）及时清理不必要的用户和管理员账户，停止无用的后台程序和进程，关闭无关的端口和服务。

5.11.5 设备选型安全

工控系统设备时应确保安全可控，并在供货合同中明确供应商应承担的网络安全责任和义务。

5.11.6 升级及病毒防护

病毒防护管理应符合 Q/HS 5036-2011 相关规定的基础上，还应包括但不限于：

a) 在安全得不到保证的情况下禁止采取远程在线服务；

b) 工控系统软件升级、补丁安装前要请专业技术机构进行安全评估和验证；

c) 主机应采取防病毒措施。

5.11.7 数据安全

管理要求包括但不限于：

a) 工控系统的基础数据以及重要敏感数据的采集、传输、存储、利用等，应采取访问权限控制、数据加密、安全审计、灾难备份等措施加以保护；

b) 各级管理人员不应随意干涉工控系统管理人员或操作人员的正常工

作，工控系统管理人员或操作人员有权拒绝不准确、不合法、不符合要求的数据进入工控系统；

c) 工控系统的各种数据及报表应严格控制阅读范围，任何人不应泄露生产数据。

5.11.8 设备安全

要求包括但不限于：

a) 不应将工控系统计算机设备和相关零件挪作他用；

b) 不应将工控系统计算机备件与他人、厂外、家庭交换使用；

c) 不应擅自打开机箱，拆卸、加装计算机零件和附加设备；

d) 不应擅自格式化硬盘和相关伊东存储介质，或更改计算机配置参数；

e) 不应擅自删除、更改文件和安装程序；

f) 不应带电插拔辅连设备。

5.11.8 机房安全

管理应符合 GB2887 和 GB9361 的规定。

5.11.9 应急管理

工控系统信息安全应急预案，明确应急处置流程和临机处置权限，落实应急技术支撑队伍，并进行演练。

5.11.10 安全培训

a) 每年至少开展一次工控系统相关的信息安全培训。

b) 未参加信息安全培训并通过考核的人员，不得操作工控系统。

5.12 网络安全应急响应与处理

5.12.1 公司网络安全和信息化领导小组是网络安全应急响应管理的最高组织。

5.12.2 建立网络安全应急响应组织，并定义组织中每个角色和人员应承担的职责；建立关键业务系统的应急响应目标和恢复策略。

5.12.3建立网络安全应急响应流程，并定义网络安全应急响应的主要阶段和每个阶段主要内容。

6 附则

本办法由公司综合管理部负责解释。

【正文结束】

附件 1：编制依据

附件 2：释义

附件 3：信息固定资产登记表

附件 4：信息软件资产登记表

附件1：

编制依据

1.1 《中国海洋石油总公司IT资产管理办法》，IT-01-08，2016，集团公司

1.2 《中海石油气电集团有限责任公司信息资产及网络安全管理办法》， IT-01-03，2019，气电集团。

附件2：

释 义

2.1 气电集团

指中海石油气电集团有限责任公司机关，包括气电集团管理层和气电集团机关各部门，简称“气电集团”。

2.2 信息资产

是指在信息化过程中所涉及的网络基础设施、系统硬件和软件、技术和管理文档、系统账户、系统业务数据等。

2.3 信息固定资产

是指在信息化过程中由公司信息管理部门负责管理和监控的所涉及使用期限超过 1 年，单位价值在 2000 元（含）以上，可单独使用的网络基础设施和系统硬件。

2.4 信息软件资产

由公司外购和自行开发的，拥有使用权的软件产品。

2.5 信息资产领用人

依照本办法相关规定领用信息资产的单位或个人。

2.6 网络安全

指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断，涵盖人工和自动信息处理安全及网络化与非网络化的信息系统安全。本件中是指以纸介质、磁介质、胶片、有线信道以及无线信道为媒体的信息，在获取（包括信息转换）、分类、排序、检索、传递和共享中的安全。

附件 3：

信息固定资产登记表

存放位置	设备类型	设备名称	品牌	设备型号	设备序列号	资产所属单位	联系人	备注

设备类型：

网络类：交换机、路由器、无线接入设备、其他 。

机房环境类: 空调、电源、监控、消防、门禁、其他。

服务器类：PC 服务器、小型机 、其他 。

存储类：SAN、NAS、磁带库、其他 。

安全类：防火墙、防病毒、入侵检测、漏洞扫描、日志审计、消磁机、其他。

办公类：PC机、笔记本电脑、打印机、复印机、打印复印一体机、其他。

通信类：程控交换机、微波站、卫星站、移动基站、其他 。

附件 4：

信息软件资产登记表

序号	软件编号	*软件名称	*版本	*软件类型	*软件厂商	*厂商国别	*许可数量	*购买时间	*软件原值（元）	*来源途径	*是否通过安全认证	知识产权状况	备注

填写说明：

1 标有*号的项栏目是必填项 。

2 软件类型：操作系统、系统服务、中间件、数据库管理系统、开发系统、办公系统，业务应用软件（如 SAP）、网管系统、安管系统、服务管理软件（如 Remedy）、其他。

3 来源途径：自购，下发，自开发，免费下载、其他。

4 许可数量：具体数量或无限、其他。

5 知识产权状况：指软件知识产权占比情况。