中国海油管理制度

体系名称	信息化管理	编　码	IT-01-04-03	版 本 号	2022-1

中海石油气电集团有限责任公司江苏分公司
网络安全应急响应细则

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）
发布范围	普发
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

1 目的

规范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）网络安全应急响应机制与流程。

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 职责分工

3.1 公司网络安全和信息化领导小组负责督促、检查、指导公司网络安全应急响应工作。

3.2 综合管理部负责组织实施公司网络安全应急响应的具体工作。

3.3 公司各部门负责履行网络安全应急响应的义务和责任，参照本细则，根据本部门具体实际建立网络安全应急响应机制，明确本部门建设和维护的重要信息系统的应急预案，明确负责网络安全应急响应的机构和负责人、联络人等信息。

4 网络安全事件类别

网络安全事件分为：有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件等。

4.1 有害程序事件包括计算机病毒事件、蠕虫事件、木马事件、僵尸网络事件、

混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等；

4.2 网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其它网络攻击事件等；

4.3 信息破坏事件包括信息篡改事件、信息假冒事件、信息窃取事件、信息丢失事件和其它信息破坏事件等；

4.4 信息内容安全事件是指通过公司网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公共利益的事件；

4.5 设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障等；

4.6 灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等突发事件导致的网络安全事件。

5 网络安全事件级别

网络安全事件依照其造成后果的严重程度和持续时间等因素分为四个等级：一般（I 级）、较大（II 级）、重大（III 级）、特别重大（IV 级）。当网络安全事件同时满足多个级别的定级条件时，按最高级别确定网络安全事件等级。

5.1 一般网络安全事件（I 级）

a）网络与信息系统遭受破坏后，对公司内部日常工作造成损害的网络安全事件；

b）除上述情形外，对公司业务、运营、办公构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

5.2 较大网络安全事件（II 级）

a）网络与信息系统遭受破坏后，对公司内部日常工作造成严重损害网络安全事件；

b）由于网络攻击导致网络与信息系统服务异常，在业务服务时段内运营与日常办公无法正常开展达 4-8 个小时，或核心业务无法正常开展在 1-4 个小时的网络安全事件。

5.3 重大网络安全事件（III）

a）网络与信息系统遭受破坏后，导致重要信息泄露，对气电集团声誉、利益和安全造成严重损害的网络安全事件；

b）由于网络攻击导致网络与信息系统服务异常，在业务服务时段内运营与日常办公无法正常开展达 8 个小时（含）以上，或核心业务无法正常开展达 4 至 8 个小时的网络安全事件。

5.4 特别重大网络安全事件（IV 级）

a）网络与信息系统遭受破坏后，导致重要信息泄露，使国家安全和公众利益受到损害的网络安全事件

b）由于网络攻击导致网络与信息系统服务异常，核心业务无法正常开展达 8 个小时（含）以上的网络安全事件。

5.5 网络安全事件发生后，应依据事件影响范围和影响时间的变化，按照上述定义评估事件级别。

6 网络安全应急响应

6.1 监测预警

6.1.1 公司对网络安全事件进行主动监测，接收国家网络安全主管机构及上级单位的预警，收集来自用户的报告，对网络安全事件进行预警。

6.1.2 公司根据监测信息或相关预警信息分析研判，对可能发生的网络安全事件进行预警。预警级别分为四级，对可能导致 I 级网络安全事件的预警定义为蓝色预警；可能导致 II 级网络安全事件的预警定义为黄色预警；可能导致 III 级网络安全事件的预警定义为橙色预警；可能导致 IV 级网络安全事件的预警定义为红色预警。

6.1.3 预警信息发布后，各部门应依据发布的预警级别，启动相应的应急预案。

6.2 应急响应

公司网络安全应急响应实行联动机制。网络安全事件发生后，相关部门应立即向综合管理部报告情况，请求启动相关应急预案，实施处置并及时报送信息；综合管理部根据事件等级和事态发展，及时向网络安全和信息化领导小组报告有关情况；公司适时向气电集团通报处置进展，必要时向气电集团协调支援。

6.2.1 相关部门应积极控制事态发展，防控蔓延，组织相关力量先期处置，采取各种技术措施，及时控制事态发展，最大限度地防止事件蔓延。

6.2.2 相关部门应快速判断事件性质和危害程度，分析事件发生原因，根据网络与信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范

围，密切关注事态发展。

6.2.3 在处置的同时，相关部门应及时向综合管理部报告事件信息，并做好事件发生、发展、处置的记录和证据留存。

6.3 应急结束与后期处置

6.3.1 应急响应结束工作由综合管理部根据相关部门报送的情况，组织进行综合研判后，提出结束应急响应的建议，上报公司网络安全和信息化领导小组批准后结束应急响应状态，转入后期处置阶段，综合管理部将有关情况通报相关部门。

6.3.2 恢复重建工作按照“谁主管谁负责，谁运行谁负责”的原则，由相关部门负责组织制定恢复、整改或重建方案，由综合管理部报气电集团主管部门审核实施。

7 应急资源保障

7.1 人力资源保障

应建立长效的应急人员保障机制，确保人员能够胜任应急处置工作。

7.2 物资保障

应建立有效的应急物资保障机制，确保在应急响应过程中不会因物资缺乏而导致应急处置中断或延长应急处置时间。

7.3 技术保障

应建立有效的技术保障机制，确保在应急响应过程中不会因技术能力缺乏而导致应急处置中断或延长应急处置时间。

7.3.1 应建立完善的信息资产台账，确保及时、准确处理应急事件，并及时通知有关人员启动应急响应。

7.3.2 明确相关厂商的技术支持服务水平，确保应急处置过程中相关厂商能够提供及时有效的技术支持。

7.3.3 应与重要基础设施服务商，主机、网络、存储等重要设备服务商，系统集成服务商以及其他外包服务商签订服务水平协议，并对服务商的技术与产品政策、服务水平、服务能力发生变化可能产生的影响及时进行风险评估和预警。

8 应急演练

公司应定期组织开展网络安全应急演练。

9 附则

本办法由综合管理部负责解释。

【正文结束】

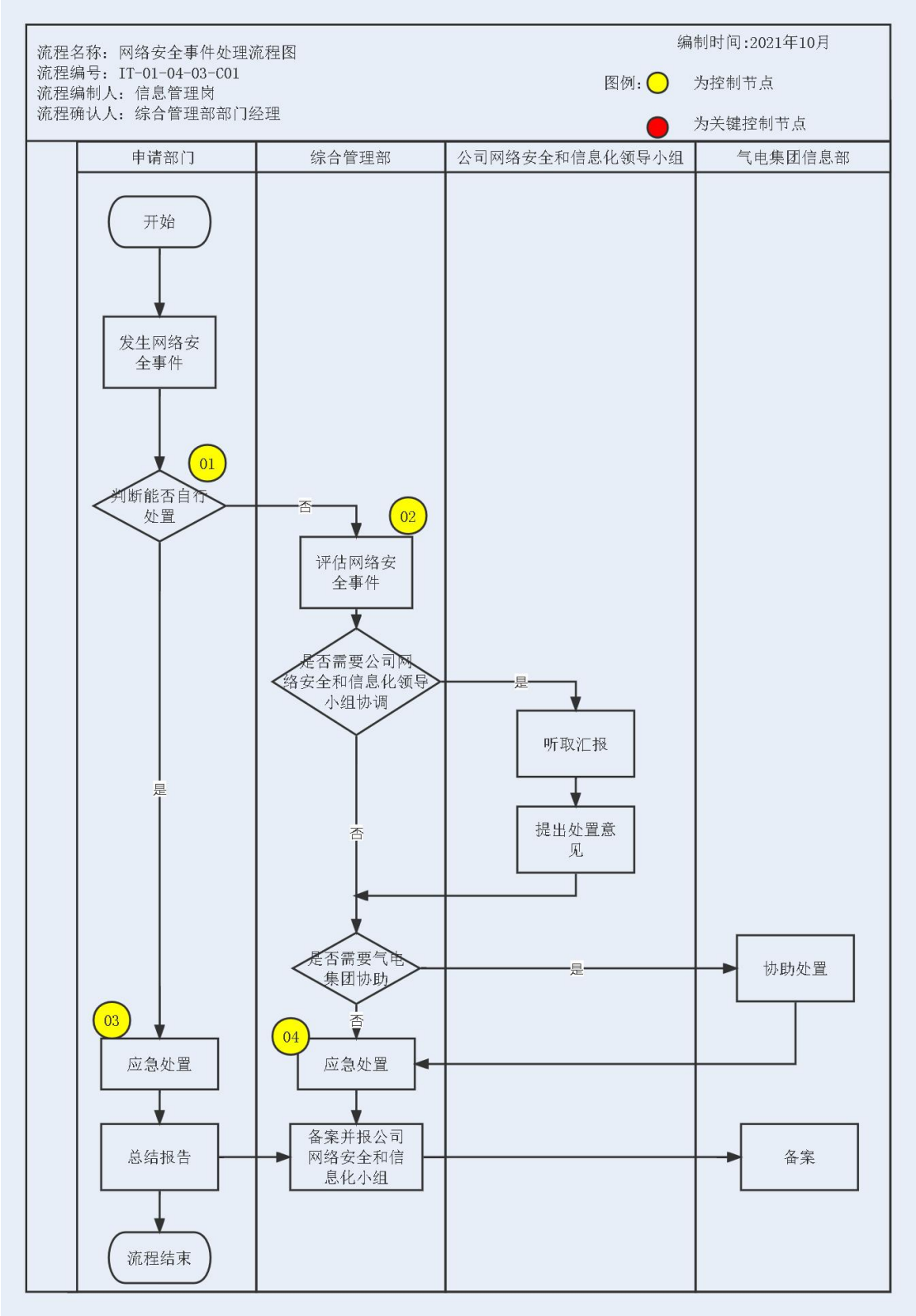
附件 1：网络安全事件处理流程

附件 2：网络安全事件处理内控活动列表

附件 3：编制依据

附件 1：

网络安全事件处理流程



附件 2：

网络安全事件处理内控活动列表

业务流程编号	业务流程名称	控制点编号	控制点描述	相关制度或程序（文号及名称）	是否为关键控制点	相关制度是否覆盖该控制点	责任岗位
IT-01-05-01-C01	网络安全事件处理流程	IT-01-04-03-C01-01	发生网络安全事件的单位判断是否可自行处置	《江苏分公司网络安全应急响应细则》（IT-01-04-03）	否	是	公司各部门
		IT-01-04-03-C01-02	综合管理部评估网络安全事件危害程度		否	是	综合管理部
		IT-01-04-03-C01-03	网络安全事件责任部门处置网络安全事件		否	是	公司各部门
		IT-01-04-03-C01-04	综合管理部协调资源处置网络安全事件		否	是	综合管理部

附件 3：

编制依据

3.1 《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。

3.2《中海石油气电集团有限责任公司网络安全应急响应细则》，IT-01-03-02，2019，气电集团。

3.3 《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》，IT-01-04，2022，公司。