粤海投资有限公司网络安全应急预案

（2023年11月修订）

第一章　总则

第一条 编制目的。为加强粤海投资有限公司（下称本公司）网络与信息安全应急管理工作，提高应对网络与信息安全事件能力，特制定本预案。

第二条 适用范围。本预案适用于本公司、各附属公司（不含上市公司）、酒店板块公司，指导网络与信息安全应急管理工作，具体如下：

（一）附件1所列附属公司应自行制定、执行符合自身行业特点及经营状况的网络安全应急预案。

（二）附件2所列附属公司（下称三级附属公司）按本预案执行，并按合法合规原则、依据自身实际情况建立健全网络安全应急预案体系，报本公司备案。

（三）附件3所列附属公司（下称直管公司）按本预案执行

（四）附件4所列的酒店板块公司按本预案执行，并可在本公司酒店经营管理部统筹指导下按合法合规原则，依据自身实际情况建立健全网络安全应急预案体系，报本公司备案。

第三条 事件分类。根据网络与信息安全事件的发生原因、

性质和机理,网络与信息安全事件主要分为以下三类:

(一) 攻击类事件:指网络与信息系统因计算机病毒感染、非法入侵等导致业务中断、信息篡改、系统宕机、网络瘫痪等情况。

(二) 故障类事件:指网络与信息系统因计算机软硬件故障、人为错误操作等导致业务中断、系统宕机、网络瘫痪等情况。

(三) 灾害类事件:指因爆炸、火灾、雷击、地震、台风等外力因素导致网络与信息系统损毁,造成业务中断、系统宕机、网络瘫痪等情况。

第二章　应急响应组织机构

第四条 本公司按照“精简、统一、高效”原则，设立处置网络与信息安全事件应急领导小组(下称应急领导小组)，由本公司董事会副主席担任组长，总经理担任副组长，成员包括分管法务、信息化业务领导，财务总监及总法律顾问。

应急领导小组是信息安全应急响应工作的领导机构。统一领导信息安全应急管理及处置工作。

应急领导小组下设网络及信息安全事件应急工作小组(下称应急工作小组)，由战略发展部负责人担任组长，网络安全管理员、安全管理员组成。应急工作小组的主要职责如下:

1. 协助灾难恢复系统实施。

2. 备份中心日常管理。

3. 备份系统的运行和维护。

4. 灾难恢复的专业技术支持。

5.开始应急演练相关工作。

6. 信息安全突发事件发生时的损失控制和损害评估。

7. 信息安全事件发生后信息系统和业务功能的恢复。

8. 信息安全事件发生后的外部协作。

第三章　应急响应流程

第五条 应急启动。在信息安全突发事件发生后,应该立即通知应急工作小组。应急工作小组分析事件的严重性后，及时向应急响应领导小组提出处理建议，由应急响应领导小组进行决策，并启动本预案。

第六条 信息上报。信息安全突发事件发生后,应按相关规定及时向上级单位报送应急信息。

第七条 信息发布。信息安全事件及应对处置工作的信息发布，坚持统一、及时、准确、适度原则。涉及本公司层面的应急事件，未经本公司应急领导小组批准，严禁任何人擅自接受记者采访、发表谈话或其他方式对外透露事件进展情况等，以免造成信息混乱或不利舆论影响。

需以本公司名义上报的材料，按本公司公文运转规定处理。

信息安全事件信息发布相关工作，严格按照有关新闻危机应对制度有关规定执行。

第八条 应急终止及事后处置。

（一）应急终止。信息安全事件得到有效处置后，经评估确认事件在短期内不会再扩大或再次发生，可视情况终止应急工作。

(二)后期处置。在应急处置工作结束后,要迅速采取措施,抓紧组织抢修受损的基础设施,减少损失,尽快恢复正常工作。通过统计各种数据,查明原因,对事件造成的损失和影响以及恢复重建能力进行分析评估,认真制定恢复重建计划,迅速组织实施信息系统重建。

应急响应总结是应急处置之后必须进行的工作,具体工作包括:

1. 事件发生原因分析:
2. 事件现象总结;
3. 系统的损害程度评估;
4. 事件损失估计:
5. 应急处置记录进行总结。

第四章 应急处理措施

第九条 日常安全预防措施。

(一)日常安全预防措施。为确保本公司信息系统业务的安全运行，在日常工作中注意加强各项安全措施，以应付各类突发事件发生时拥有足够的应急预备流程、辅助措施或有利条件，应严格执行以下日常安全措施：

1.信息系统业务管理员应定期对网络系统的运行状态、系统日志和安全日志等进行检查，对重要信息系统如网站、核心数据库等应每日进行运行检查，对重要数据要实时和定时进行备份，对核心网络设备定期检查和维护，确保及时发现网络安全事件，减少安全事件所造成的损失。

2. 预防数据丢失：在原有信息系统自己备份的基础上，针对重大节日或活动建立全公司统一本地备份，建议在重大节日或活动期间的备份周期能控制在每 12-24 小时一次。

3. 预防设备故障：对于易损件，准备必要的备品、备件。为相关服务器以及应用系统采用冷备或各服务器交叉备份的方式。

4.要求使用部门提高安全意识，避免由于人为失误造成企业信息网安全风险；

5. 为保证企业内部网和 INTERNET 的安全隔离，禁止应用系统采用双网卡方式一端接 INTERNET，一端接入企业内网；须对

本地企业内网上的应用系统进行核查，如存在上述情况应立即停止使用并进行整改。

6. 严禁员工办公电脑安装与工作无关的软件。禁止对外部人员开放相关信息系统网站系统 Ping、TELNET 功能，如果存在特殊情况，需得到审批。相关部门必须加强对社会维保公司、系统厂商开发人员的审核及管理，避免出现安全漏洞。

第十条 攻击类事件应急处置措施

病毒安全紧急处置措施

出现问题	任意文件上传挂马入侵；
风险影响	信息系统一旦感染病毒进而会导致计算机病毒的传播，引发系统崩溃、数据损坏和机密账号被盗等严重后果。
应急措施	1.发现系统服务器疑似感染病毒后系统管理员立即切断感染病毒计算机与网络的联接。
	2.由相关信息管理员对该计算机的重要数据进行数据备份。
	3.启用防病毒软件对该计算机进行杀毒处理，同时通过防病毒软件对其他计算机进行病毒扫描和清除工作。
	4.如果满足下列情况之一的，应立即向应急领导小组通报情况，由应急工作小组协助处理： （1）现行防病毒软件无法清除该病毒的； （2）业务系统服务器在 2 小时内无法处理完毕的； （3）办公系统在 4 小时内无法处理完毕的。
	5.在应急工作小组提取相关数据样本后，恢复系统和相关数据，检查数据的完整性。
	6.病毒爆发事件处理完毕，将计算机重新接入网络。

	7.总结事件处理情况，将有关情况向应急领导小组汇报有关情况，并提出防范病毒再度爆发的解决方案。
	8.配合应急工作小组实施必要的安全加固。

第十一条 故障类事件应急处理措施

（一） 信息系统安全紧急处理措施

出现问题	信息系统故障
风险影响	信息系统崩溃,应用无法正常运作导致相关业务系统无法工作。
应急措施	1. 系统管理员对重要的信息系统平时必须存有备份，在重大节日或活动期间对系统相对应的数据必须有多日备份,并将它们保存于安全处。
	2. 一旦信息系统发生故障，应由系统管理员进行应急处理。
	3. 做好必要记录，妥善保存有关记录及日志或审计记录。系统管理员负责系统和数据的恢复。
	4. 如果满足下列情况之一的，应立即向应急领导小组通报情况，由应急工作小组协助处理： （1）现行应急恢复措施无法恢复信息系统的； （2）业务系统在 2 小时内无法处理完毕的； （3）办公系统在 4 小时内无法处理完毕的。
	5. 在应急工作小组提取相关数据样本后，恢复系统和相关数据，检查数据的完整性。
	6. 相关系统故障事件处理完毕，将计算机重新接入网络。
	7. 总结事件处理情况，将有关情况向应急领导小组汇报有关情况，并提出防范故障再度爆发的解决方案。
	8. 配合应急工作小组实施必要的安全加固。

（二） 网络中断紧急处理措施

出现问题	网络线路故障

风险影响	网络故障，造成办公环境无法正常运作。
应急措施	1.网络中断后，网络安全管理员应立即判断故障节点，查明故障原因，并向应急工作小组汇报。
	2.如属线路故障，应重新安装线路。
	3、如属路由器、交换机等网络设备故障，如有备用设备则临时替换使用，并立即与设备提供商联系更换设备，并调试畅通。
	4.如属路由器、交换机配置文件破坏，应迅速使用最近的备份进行恢复，再按照要求更新配置，并调试畅通。如遇无法解决的技术问题，立即向应急领导小组或有关厂商请求支援。
	5.总结事件处理情况，将有关情况向应急领导小组领导汇报有关情况，并提出防范故障再度爆发的解决方案。

第十二条　灾害类事件应急处理措施

出现问题	设备物理故障
风险影响	设备故障导致相关服务器无法启动，信息系统瘫痪。
应急措施	1、小型机、服务器等关键设备损坏后，有关人员应立即向战略发展部汇报。
	2、战略发展部应立即查明原因。
	3、如果能够自行恢复，应立即用备件替换受损部件。
	4、如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。
	5、如果设备一时不能修复，应向应急领导小组汇报，并告知各下属单位。
	6、总结事件处理情况，将有关情况向应急领导小组领导汇报有关情况，并提出防范故障再度爆发的解决方案。

第五章　应急演练

第十三条 建立网络安全应急预案定期演练制度，每年至少组织 1 次网络安全应急演练。通过演练，发现应急工作体系和工

作机制存在的问题，不断完善应急预案，提高应急处置能力。

第六章　附 则

第十四条　本预案由本公司战略发展部负责解释。

第十五条　修订后的本预案自 2023 年 11 月 30 日起施行。原《粤海投资有限公司网络安全应急预案》(2021 年 12 月修订)(粤投〔2021〕513 号)同时废止。

附件：1.二级附属公司名单

2.三级附属公司名单

3.直管公司名单

4.酒店板块公司名单

附件 1

二级附属公司名单

本办法第二条所列的二级附属公司名单：

1. 广东粤港供水有限公司

2. 粤海水务控股有限公司

3. 广东粤海天河城（集团）股份有限公司

备注：本公司将根据管控要求的调整，动态调整此公司名单。

附件 2

三级附属公司名单

本办法第二条所列的三级附属公司名单：

1. 中山粤海能源有限公司

2. 广西粤海高速公路有限公司

备注：本公司将根据管控要求的调整，动态调整此公司名单。

附件 3

直管公司名单

本办法第二条所列的直管公司名单：

1.广东粤海投资财务管理有限公司

2.广东电力(国际)有限公司

备注：本公司将根据管控要求的调整，动态调整此公司名单。

附件 4

酒店板块公司名单

本办法第二条（四）所指酒店板块公司包括:

一、酒店经营管理部统筹管理的实体运营附属公司：

1.粤海（国际）酒店管理集团有限公司

2.粤海国际酒店管理（中国）有限公司

3.深圳粤海酒店企业有限公司

4.珠海粤海酒店

5.粤海酒店管理（珠海）有限公司

6.粤海酒店有限公司

7.SEN INTERNATIONAL VENTURES CORPORATION (HONG KONG) LIMITED （华美酒店）

二、酒店经营管理部统筹管理的受委托管理公司：

1. 上海粤海大酒店有限公司

2. 河南省粤海酒店有限公司

备注：本公司将根据管控要求动态调整此名单。