**市民服务中心智能化运维服务**

**应急预案**



青岛慧海联创信息技术有限公司

2025 年 1 月3日

文档信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文档名称编号 | 应急预案（HHLC-ITSS-ZNHFYJYA） | | | |
| 编制单位 | 青岛慧海联创信息技术有限公司 | | | |
| 文档密级 | 秘密 | | | |
| 文档版本 | 版本日期 | 版本说明 | 作者 | 审核 |
| V1.0 | 2025-1-3 | 发布版本 | 李琳 | 张仲全 |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[市民服务中心智能化运维服务 1](#_Toc14753)

[应急预案 1](#_Toc9009)

[文档信息 2](#_Toc24056)

[一、编写目的 8](#_Toc20076)

[（一）预防为主 9](#_Toc17703)

[（二）加强监控 9](#_Toc18781)

[（三）资源整合 9](#_Toc376)

[（四）适时演练 10](#_Toc20771)

[（五）快速反应 10](#_Toc26525)

[（六）高效配合 10](#_Toc2929)

[二、适用范围 10](#_Toc17182)

[三、应急组织 10](#_Toc26565)

[四、编制依据 11](#_Toc14137)

[五、适用范围 11](#_Toc28500)

[六、信息系统运维安全风险识别 11](#_Toc30603)

[（一）应急事件的发现 11](#_Toc8578)

[（二）确认应急事件及等级 11](#_Toc7998)

[（三）应急事件分类 12](#_Toc10453)

[（四）应急事件分级 12](#_Toc25246)

[（五）事件列表 13](#_Toc21702)

[七、事前预测预警 13](#_Toc30261)

[（一）信息监测与报告 14](#_Toc26338)

[（二）预警处理与发布 15](#_Toc8159)

[（三）预警支持系统 16](#_Toc30222)

[（四）预防机制 16](#_Toc18810)

[八、应急响应 16](#_Toc250)

[（一）四级响应 16](#_Toc27166)

[（二）三级响应 17](#_Toc20731)

[（三）二级响应 17](#_Toc507)

[（四）一级响应 17](#_Toc6372)

[九、专项应急预案 18](#_Toc1623)

[（一）服务器故障应急预案 18](#_Toc22436)

[（二）安全系统应急预案 18](#_Toc17981)

[（三）软件故障应急预案 19](#_Toc1186)

[（四）灾害性事件应急预案 19](#_Toc21977)

[十、应急预案基本流程 20](#_Toc31793)

[（一）判断事件类型 21](#_Toc15776)

[（二）启动专项预案 21](#_Toc5281)

[十一、后期处置 21](#_Toc21415)

[（一）调查评估 21](#_Toc18598)

[（二）恢复重建 21](#_Toc6371)

[（三）信息发布 22](#_Toc2610)

[十二、宣传和演练 22](#_Toc287)

[（一）预案宣传 22](#_Toc10492)

[（二）预案演练 22](#_Toc1002)

[十三、预案修订和培训 22](#_Toc21054)

[十四、政务企云 23](#_Toc1497)

[（一） 网络攻击事件应急预案 23](#_Toc7030)

[（二）信息破坏事件应急预案 24](#_Toc25791)

[（三） 网络故障事件应急预案 25](#_Toc22580)

[（四）服务器故障应急预案 26](#_Toc1746)

[（五）软件故障事件应急预案 27](#_Toc15154)

一、编写目的

为进一步提高运维组应对网络、信息安全、应用系统、硬件设备突发事件的应急处置能力，加强组织领导，全面保障系统的稳定运行及其数据安全等，特编制本应急预案，应急体系图如下：

总则

制目原则 编制依据

适用范围

工作目标

组织体系

响应领导小组

响应执行小组

响应专家组

响应技术支持小组

预测预警

预警系统

预警处理

监测报告

运行机制

应急响应

应急支持

信息报告

后期处置 风险识别

调查评估

确认风险

恢复健康

启动预案响应

应急管理

信息发布

宣传和演练

文档管理

预案修订和培训

图 1

建立统一的应急响应组织及应急响应制度，将运行维护

服务中应急响应方案内容划分为以下主要阶段：安全风险识别、事前预测预警、应急响应、专项应急预案及其基本流程、后期处置、宣传和演练以及预案修订和培训。

各应急响应阶段均有其重点应用特点，在后续应急预案方案的章节中将进行详细阐述。

编制原则：运维总体应急保障工作采用预防为主、加强监控、资源整合、适时演练、快速反应、高效配合的原则。

（一）预防为主

宣传普及信息安全知识，牢固树立“预防为主、常抓不懈 ”的意识，长久性地做好应对信息系统突发事件的准备工作，提高安全规范意识以及网络和重要信息系统的安全保障水平。

（二）加强监控

加强对信息安全隐患的日常监测，一旦发现安全事件及时采取有效措施，迅速控制其影响范围，将损失降到最低限度。

尤其对各个应用系统、音频设备、网络及网络设备、机房基础设施等进行监控，在每日的巡检时，认真检查每一项的具体情况，并记录在巡检记录中。

（三）资源整合

由甲方统领、各运维单位协同配合，整合人力、设备资源。

（四）适时演练

根据运维工作的需求，按照应急预案内容安排定期或者不定期的应急演练。模拟在网络、信息安全等事件发生时，组织相关人员完成事件的发现、上报、处理等完整流程。通过应急演练对应急预案的可行性、有效性进行验证，同时也进一步完善应急预案。

（五）快速反应

建立信息检测、信息报告、人员值班和应急人员待命制度。遇有网络、信息安全等应急事件发生时，按照应急响应等级，迅速启动相关预案，确保各有关人员快速到位。

（六）高效配合

在应急演练进行中，各应急厂商需要在总指挥的领导下，严格听从指挥，相互配合。确保事件顺利处理。

二、适用范围

本预案是市民服务中心智能化运维项目的保障工作，运行的各个模块如果出现技术性的问题，保障组能够迅速作出响应。

三、应急组织

根据平台各功能服务运维方成立相应的应急响应小组，应急响应小组由副总担任组长,总体规划应急相关事宜,组员有质量中心、研发中心、运维服务部组长等人。

四、编制依据

1. ITSS.1—2015 《信息技术服务 运行维护服务能力成熟度模型》

2. GB/T28827.1-2022《信息技术服务 运行维护 第一部分：通用要求》

3. GB/T 29264-2012 《信息技术服务 分类与代码》

4. GB/T 28827.2-2012 《信息技术服务 运行维护 第 2 部分:交付规范》

5. GB/T 28827.3-2012 《信息技术服务 运行维护 第 3 部分:应急响应规范》

6. 国家有关法律、法规及行业标准

五、适用范围

本预案主要针对项目基础环境、硬件维护、各类应用系统可能发生的突发事件。

组建运维应急保障机构，建立起快速反应、协调有力、配合密切的应急响应工作机制。提高应对突发事件的组织指挥和应急处理能力，针对系统运行过程中可能发生的不同类型和不同严重程度的安全事件，采取相应的响应级别和应急策略，保证系统能够在最短的时间内恢复正常运行。

六、信息系统运维安全风险识别

（一）应急事件的发现

应急事件的发现通过以下方式：

1. 监控设备报警

2. 监控过程日志分析

3. 安全部门通知

（二）确认应急事件及等级

确认事件及等级主要是为了准确无误的启动相关专项预案，并同时根据事件类型及事件等级逐级地向相关应急领导小组管理人员进行汇报。

（三）应急事件分类

根据网络、信息安全等事件的发生原因、性质和机理，网络、信息安全等事件主要分为以下两类：

1. 可控信息系统运维安全事件

指相关信息系统内部可以解决或有能力解决的信息运维安全事件，如网络与信息系统因计算机病毒感染、计算机软硬件故障、人为误操作、非法入侵等导致。业务中断、系统宕机、 网络因人为原因造成瘫痪、 内部电力中断等情况。

2. 不可控信息系统运维安全事件

指相关信息系统内部无法解决的信息运维安全事件，如由于网络供应商原因导致的网络瘫痪， 以及因爆炸、火灾、雷击、地震、台风、洪灾等外力因素导致网络与信息系统损毁、外部电力中断，造成业务中断、系统宕机、网络瘫痪等情况。

（四）应急事件分级

针对当前的运维环境，定义了四级事件，按照以下标准对事件进行分级：

1. 一般事件（四级）

在服务器、存储设备、安全设备等的功能、安装或配置方面需要信息咨询或技术支持。本级故障事件对数据中心的业务运作几乎无影响，或根本没有影响，持续小于 24 小时的事件。持续时间超过 24 小时则升级到三级事件。

2. 较大事件（三级）

系统的操作性能受损，安全事件例如病毒在小范围内发作，但大部分业务运作仍可正常工作，持续小于 12 小时的事件。持续时间超过 12 小时则升级到重大事件。

3. 重大事件（ 二级）

现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响核心业务运作，持续小于 6 小时的事件。持续时间超过6 小时则升级到特别重大事件。

4. 特别重大事件（一级）

现有的系统停机，或遭到严重攻击行为或安全事件，对数据中心的业务运作有重大影响的事件。

（五）事件列表

根据甲方具体情况，确定了以下可能发生的安全事件，并初步确定其应急响应的建议优先级别：

|  |  |  |  |
| --- | --- | --- | --- |
| 事件 | 影响 | 可能性 | 优先级 |
| 主网网站被黑客攻击和篡改 | 社会影响非常大 ，是重点保障对象。 | 高 | 1 |
| 内网网络故障 | 业务中断 ，影响部分业务的提供（特别是财务系统）。 | 高 | 1 |
| 互联网病毒暴发 | 业务性能下降，影响部分业务的提供。 | 中 | 1 |
| 互联网网络入侵 | 重要服务器遭到入侵，影响服务提供，对网络其他部分形成威胁。 | 中 | 1 |
| 机房主机故障 | 部分主机或服务器出现故障，导致服务性能下降或者影响服务的提供。 | 中 | 2 |
| 在运行中的软件出现故障 | 部分应用软件出现故障，导致服务性能下降或者影响服务的提供。 | 中 | 2 |
| 人为破坏 | 系统中的硬件/软件设备遭到人为破坏，导致服务性能下降或者影响服务的提供。 | 低 | 3 |
| 灾难（不可抗力） | 自然灾难破坏，造成系统大面积破坏，业务完全或部分中断。 | 低 | 4 |

七、事前预测预警

预防预警是应急响应迅速启动的关键。利用自身的安全监控设备和工具，并结合社会其他信息源（如安全厂商的公告、各类应急响应机构的公告等），及时发现信息安全威胁或事件发生的迹象和趋势，分析导致信息安全事件的根源，为信息安全应急响应工作提供支持。

（一）信息监测与报告

应急领导小组负责项目的风险评估与控制的监督、检查、指导工作。信息安全执行小组组织开展风险评估，定期开展重要信息系统检查， 了解风险状况，根据需要建立风险源管理系统，加强风险管理，提高重要信息系统抗风险能力。为进一步完善网络与信息安全突发公共事件监测、预测、预警制度，落实责任制，制定信息通报制度。按照“早发现、早报告、早处理、早恢复 ”的原则，加强对各类网络与信息安全突发公共事件和可能引发突发公共事件的有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发公共应急事件时，由应急响应技术支持小组向信息系统应急执行小组报告并且通知应急响应领导小组人员，按安全事件定级的规定及时报告安全事件当前的影响程度和特征。主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

应急响应执行小组要加强信息安全监测、分析和预警工作，进一步提高信息安全监测和处理能力，加大对信息安全事件犯罪的处理力度。

建立信息安全事故报告制度。发现信息安全突发事件时应当在事件发生后，应急响应小组立即对发生的事件进行调查核实、保存相关证据，并在事件被发现或应当被发现时起5 小时内将有关材料报至应急工作领导小组。

（二）预警处理与发布

应急工作领导小组接到信息安全突发事件报告后，在经初步核实后，将有关情况及时向市信息安全应急协调小组报告。在进一步综合情况，研究分析可能造成损害程度的基础上，提出初步行动对策，视情况召集协调会，并根据市信息安全协调小组的决策实施行动方案，发布指示和命令。

对于可能发生或已经发生的网络与信息安全突发公共事件，应急响应小组应立即采取措施控制事态，并在最短的时间内进行风险评估，判定事件等级并在本系统内发布预警。必要时应启动相应的专项预案，同时向应急工作领导小组通报情况。

工作领导小组接到报告后，应及时对信息作出判断，提出处理意见。对发生和可能发生的网络与信息安全突发公共事件时，应迅速召开应急工作小组会议，研究确定网络与信息安全突发公共事件的等级，决定启动应急预案，同时确定应急指挥人员，并迅速报送市信息安全应急协调小组报告，并向上级相关部门进行通报。

对需要向社会发布预警的网络与信息安全突发公共事件， 由应急工作领导小组根据其可能造成的危害程度、紧急程度和发展态势，及时向上级主管部门通报预警信息。由上级主管部门根据网络与信息安全事件的管理权限、危害性和紧急程度，统一发布、调整和解除预警信息，对严重、特别

严重或可能衍生其他安全事件的预警信息，应按照市政府的决定由授权部门发布。

（三）预警支持系统

应急工作领导小组应建立和逐步完善信息监测、传递网络和指挥决策支持系统，要保证资源共享、运转正常、指挥有力。

（四）预防机制

积极推行信息安全等级保护，逐步实行信息安全风险评估。各基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复，制定完善信息安全应急处理预案。针对基础信息网络的突发性、大规模安全事件，各相关部门建立制度化、程序化的处理流程。

八、应急响应

针对不同级别的应急事件，运维组建立了四级应急响应机制。每一级别的应急事件，都安排了现场值守人员给予处理，同时对于高级别的事件还积极借助信息系统运维应急响应专家组在内的第三方力量给予处理。

（一）四级响应

当发生四级信息服务运维应急事件时，启动四级响应，技术小组相关成员8 小时内到达岗位，5\*9 小时在岗在位，处理相关事件，并将事件处理结果 24 小时内报告给技术小组组长。

（二）三级响应

当发生三级信息服务运维应急事件时，启动三级响应，技术小组相关成员4 小时内到达岗位，5\*9 小时在岗在位，处理相关事件。并将事件处理结果 12 小时内报告给技术小组组长。

（三）二级响应

当发生二级信息服务运维应急事件时，启动二级响应，全部技术小组人员2 小时内到达岗位，7\*24 小时在岗在位，处理相关事件，并做好一级响应的准备工作，每 2 小时给技术小组组长和领导小组报告事件处理情况。

（四）一级响应

当发生一级信息服务运维应急事件时，启动一级响应，全部技术小组人员 1 小时内到达岗位，7\*24 小时在岗在位，处理相关事件，每 1 小时给领导小组报告事件处理情况。

一般定义，四级事件属于日常运维服务范畴，由 日常运维服务处理，需要向应急响应技术支持小组相关成员告知；三级事件和二级事件属于应急服务项目，故障事件从四级升级到三级时，由运维服务人员及时通知应急响应技术支持小组组长和副组长，同时技术启动应急响应服务，必要时同时报告执行小组相关成员并请求专家小组的支持；故障事件从三级升级到二级时， 由相关人员报告领导小组组长。

各级故障事件的最晚响应时间表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 响应时间 | 一级事件 | 二级事件 | 三级事件 | 四级事件 |
| 1 小时 | 技术支持小组 |  |  |  |
| 2 小时 | 技术支持小组执行小组 | 技术支持小组 |  |  |
| 4 小时 | 执行小组专家组 | 技术支持小组执行小组 | 技术支持小组 |  |
| 8 小时 | 领导小组 | 执行小组专家组 | 技术支持小组执行小组 | 技术支持小组 |

备注： 以上响应时间按照 7×24 小时计故障响应时间。将根据以上标准对故障事件进行定级，并根据故障事件的等级来制定运维服务指标。

九、专项应急预案

（一）服务器故障应急预案

服务器故障后，应急小组确定故障设备及故障原因，并通知相关厂商。

根据服务器修复和恢复系统所需时间，由应急响应执行小组人员和领导小组决定是否启用备份设备。

如启用备份设备，在服务器故障排除后，应急小组在确保不影响正常业务工作的前提下，利用网络空闲时期替换备用设备。如不启用备份设备，应急小组应积极配合相关厂商解决服务器故障事件。

（二）安全系统应急预案

为提高应对信息系统在运行过程中出现的各种突发事件的应急处置能力，有效预防和最大程度地降低信息系统各类突发事件的危害和影响，保障信息系统安全、稳定运行，

结合实际，制定安全专项应急预案。各处室根据职责分工，及时收集、分析、汇总本处室基础网络与信息系统安全运行情况信息、安全风险及事件信息，及时报告应急响应领导小组。

信息系统突发事件分为网络攻击事件、信息破坏事件、信息内容安全事件、网络故障事件、软件系统故障事件、灾难性事件、其他突发性事件等。

（三）软件故障应急预案

发生计算机软件系统故障后，系统使用人员应立即保存数据，停止该计算机的业务操作，并将情况报告应急小组，不得擅自进行处理。

应急小组应立刻派出技术人员进行处理，必要情况下，通知各业务部门停止业务操作和对系统数据进行备份。

应急小组组织有关人员在保持原始数据安全的情况下，对计算机系统进行修复；修复系统成功后，利用备份数据恢复丢失的数据。

（四）灾害性事件应急预案

一旦发生灾害性事件，应急小组每一位成员都应有责任在第一时间进入机房抢救服务器及存储设备。

应急小组对服务器及存储设备的损坏程度进行评估。如服务器损坏或存储设备损坏无法使用，立即联系相关厂商，进入维保服务程序。

根据服务器或存储设备修复和恢复系统所需时间，由市总应急响应领导小组决定是否启用备份设备。

十、应急预案基本流程

应急预案的基本流程如下图所示：

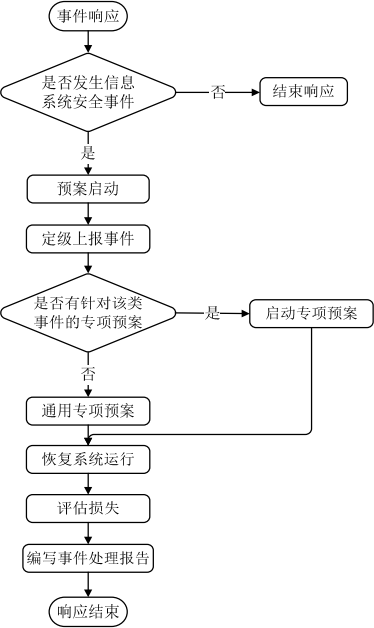


图 2 流程图

（一）判断事件类型

通过上报事件排除误报行为，确定事件类型，启动相关专项应急预案，并通知相关负责人。

（二）启动专项预案

确定事件类型后，由负责人启动该专项预案，确定事件级别，是否向应急领导小组汇报情况，由专项负责人协调有关人员，调用相关资源，快速高效地解决应急事件。

十一、后期处置

（一）调查评估

应急响应小组对网络与信息安全事件的起因、性质、影响、责任、经验教训和恢复重建等问题进行调查和评估。

责任确定。应急处置工作结束后，应当分析产生该次事件的原因，对事件进行调查，确定责任人。如果涉及违法犯罪行为， 由司法机关及时追究当事人的刑事责任。

事件备案与归档。应急处置工作结束后，实施事件处置的过程和结果须备案。

预案维护。应急处置工作结束后，需根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。

（二）恢复重建

在对可利用的资源进行评估后，制订重建和恢复生产的计划，迅速采取各种有效措施，恢复网络与信息系统的正常

运行。

（三）信息发布

信息发布由应急响应小组统一管理。

十二、宣传和演练

（一）预案宣传

运维组制定对本预案的宣传教育规划，由甲方宣传，相关负责人审核方案。

（二）预案演练

本预案原则上每年至少组织两次（上半年第一季度末、下半年第一季度末）应急演练，演练内容可包括技术演练、人员装备拉动演练。通过演练模拟实施应急支援工作，检验应急动员能力，修订完善流程。

十三、预案修订和培训

运维总体应急预案原则上每年年末（每年 12 月）修订一次，如果有重大变化，随时修订。各专项预案每年根据演练情况进行修订。

原则上每年年中（每年6 月）组织一次部内信息系统应急响应执行小组成员、信息系统应急响应技术支持小组人员预案培训，当各小组人员变动较大时或预案进行修订后，一个月内进行培训。

十四、政务企云

（一） 网络攻击事件应急预案

1. 告警

收到安全部门网络攻击事件报告。

2. 确认

登录服务器，查看日志文件

/home/taihao/logs/qiyun.log，根据请求 IP 地址及请求频次，确认是否受到网络攻击。

3. 上报

上报信息系统应急响应领导小组。

4. 处置

如确认受到网络攻击，联系云服务运营商，封禁相关 IP地址或相关 IP 段，持续监控是否继续受到网络攻击。

根据网络攻击情况判断是否存在数据库数据被恶意篡改的情况，若出现篡改数据的情况则根据系统备份恢复方案中突发事件时数据库数据备份方案备份数据库当前数据，再恢复最近的日常备份数据。

5. 反馈

将处置情况反馈信息系统应急响应领导小组。

6. 总结

根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。

（二）信息破坏事件应急预案

1. 告警

收到安全部门信息破坏事件攻击报告。

2. 确认

登 录 服 务 器 ， 查 看 日 志 文 件

/home/taihao/logs/qiyun.log，查看是否收到信息破坏。

3. 上报

上报信息系统应急响应领导小组。

4. 处置

1) 运 行 /home/taihao/tomcat-9/bin/shutdown.sh停止服务。

2) 根据系统备份恢复方案中突发事件时数据库数据备份方案备份数据库当前数据，并恢复最近的日常备份数据。

3) 通 过 命 令 重 新 启 动 服 务 ： home/taihao/tomcat-9/bin/startup.sh。

4) 通过 navicat 链接数据库：192.166.153.100。

5) 查看表 SYS\_LOG 分析请求记录，查找信息被破坏的原因和相关责任人。

6) 将备份的突发事件数据库备份数据恢复至应急处理数据库（测试数据库 10.192.116.91）。

7) 对比已恢复的正式数据库数据和应急处理数据库数据，修复被篡改的数据。

5. 反馈

将处置情况反馈信息系统应急响应领导小组。

6. 总结

根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。

（三） 网络故障事件应急预案

1. 告警

通过监控平台收到服务无法响应的通知。

2. 确认

查看服务是否能够正常访问。

登录服务器，查看服务是否正常运行。

3. 上报

上报信息系统应急响应领导小组。

4. 处置

1) 通知机房人员恢复网络。

2) 查看服务是否宕机，若服务宕机则通过命令重启服务 ： home/taihao/tomcat-9/bin/shutdown.sh,home/taihao/to mcat-9/bin/startup.sh。

5. 反馈

将处置情况反馈信息系统应急响应领导小组。

6. 总结

根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。

（四）服务器故障应急预案

1. 告警

通过监控平台收到服务无法响应的通知。

2. 确认

查看服务是否能够正常访问。

查看服务器是否能够正常登录，服务器是否宕机。

3. 上报

上报信息系统应急响应领导小组。

4. 处置

1) 通知机房人员恢复服务器使用。

2) 查看服务是否宕机，若服务宕机则通过命令重启服务 ： home/taihao/tomcat-9/bin/shutdown.sh/home/taihao/to mcat-9/bin/startup.sh。

5. 反馈

将处置情况反馈信息系统应急响应领导小组。

6. 总结

根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。

（五）软件故障事件应急预案

1. 告警

通过监控平台收到服务无法响应的通知。

2. 确认

查看服务是否能够正常访问。

查看服务器是否能够正常登录，服务器是否宕机。

3. 上报

上报信息系统应急响应领导小组。

4. 处置

1) 通 过 命 令 关 闭 服 务 ： /home/taihao/tomcat-9/bin/shutdown.sh。

2) 根据系统备份恢复方案中突发事件时数据库数据备份方案备份数据库当前数据。

3) 通 过 命 令 查 看 项 目 运 行 日 志 中 错 误 信 息 ： /home/taihao/logs/qiyun.log。

4) 根据错误信息排查系统故障原因，若非软件功能问题则尝试通过重启服务来恢复软件功能。

5) 若属于软件功能问题则联系开发维护人员修复软件问题。

6) 其他，如网络，服务器等故障则联系机房管理人员进行修复。

7) 故障修复后通过最近的日常备份文件恢复丢失的数

据。

8) 通 过 命 令 重 新 启 动 服 务 ： home/taihao/tomcat-9/bin/startup.sh

9) 查看服务是否宕机，若服务宕机则通过命令重启服务：home/taihao/tomcat-9/bin/startup.sh。

5. 反馈

将处置情况反馈信息系统应急响应领导小组。

6. 总结

根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。