天津市红桥区信用信息共享平台
应急预案
（试行）

第一条 总述

天津市红桥区公共信用信息平台项目涉及范围广、信息多，因此必须保证系统安全稳定运行。另外，在系统出现故障、遭到攻击或其他原因导致的故障之后，应根据应急预案，安全稳妥处置各类应急故障，保证系统正常运行。

第二条 系统应急预案的目的

为科学应对信息安全突发事件，建立健全信息安全应急响应机制，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，制订本应急预案，旨在解决以下几种故障：

1.应对系统自身出现的各类故障；

2.应对应断电、硬件设备故障等原因引起的各类故障；

3.应对因遭到攻击等恶意入侵引起的各类故障；

针对本系统，我们建议采取以下应急工作原则，

（1）预防为主。立足安全防护，加强预警，定期检查维护，保证系统稳定运行。

（2）快速反应。及时获取充分而准确的信息，果断决策，迅速处置，最大程度地减少损失和影响。

（3）分级负责。按照“谁主管谁负责”的原则，建立和完善安全责任制及联动工作机制。加强各部门间的协调与配合，形成合力，共同履行应急处置工作的管理职责。

（4）常备不懈。规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发公共事件应急处置的科学化、程序化与规范化。

第三条 应急组织机构和职责

建议在项目的建设过程中，成立专门的应急组织机构，成员包括用户信息化部门、信息系统商、系统硬件提供商、安全防护和数据库等应用软件提供商、系统运行网络商，各单位必须制定专人负责，安全小组组长由用户信息系统安全管理人员担任。

浪潮针对项目可能出现的不同故障，提供不同的解决思路。

第四条 预测与预警

浪潮针对系统运行中各种可能发生的事件，建立了完善预测预警机制，整合监测信息资源，借助于浪潮的 IT 运维体系的相关管理流程，建立健全系统运行各类事件预测预警系统，开展风险分析，做到早发现、早报告、早处置。以下应急方案内容可以在项目实施之前和客户一同修改和完善确认。

第五条 应急处置

本项目的应急处置分为四个阶段，具体如下：

1.信息报告

系统运行中一旦发生突发事件，所在部门或当事人员要保持镇静，在第一时间向本单位应急办公室和有关部门报告。报告内容包括时间、地点、事件的性质、影响范围、事件发展趋势和已经采取的措施、单位全称和联系电话等。重大事件必须在 15 分钟内向用户突发事件应急领导小组报告，不得迟报、谎报、瞒报和漏报。

2.先期处置

事件发生后，事发地突发事件应急办公室要立即采取措施控制事态进一步发展，组织开展应急工作，并及时向上一级领导报告。

各职能处室、单位在报告重大突发事件信息的同时，要根据职责和规定的权限启动相关应急预案，及时、有效地进行处置，控制事态。

3.应急响应

对已处置但未能有效控制事态或需用户协调处置的重大或特别重大的事件，由突发事件应急办公室向用户领导报告，经批准后启动相应应急预案。

4.指挥与协调

需要用户处置的事件，由用户突发事件应急领导小组统一指挥或指导各有关地区和部门开展处置工作。主要包括：

（1）组织协调有关地区和部门负责人及专家参与应急处置；

（2）制定并组织实施应急处置方案，防止引发次生、衍生事件；

（3）及时向教育部领导报告应急处置工作进展情况。

事发地所在的单位负责成立现场应急指挥机构，在用户突发事件应急领导小组的指挥或指导下，负责现场的应急处置工作。

但针对不同的故障，我们除按照上述方式处置外，提出一些针对性的措施。

第六条 系统出现故障处置

系统自身出现故障后，浪潮现场服务人员第一时间根据系统运行日志、错误日志等定位故障原因，并提出解决方案，及时消除故障；如果现场人员第一时间不能解决问题，则及时向项目经理汇报情况，项目经理及时组织人员，直接去现场或远程协助解决故障。

第七条 数据库故障处置

在平台运行过程中，必须确保系统数据安全。为此，各数据库系统必须实现异地备份，防止出现数据故障。在出现数据库故障后，必须采取正确有效的应对措施，尽快恢复数据，将损失降至最小：

1.一旦数据库崩溃，应立即向安全责任人报告，同时通知各级单位暂缓上传上报数据。

2.安全责任人协调技术人员，尽快恢复数据，保证系统正常运行，并查明故障原因，及时维修，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。

3.如果数据无法恢复，应立即向有关厂商请求紧急支援。

第八条 系统遭受攻击处置

在平台运行过程中，要采取安全防范措施，重要的软件系统平时必须存有备份，与软件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，确保系统正常运行，如果系统遭到恶意攻击，则应启动相应的应急措施，保证系统安全运行：

1.一旦软件遭到破坏性攻击，应立即向系统安全负责人员报告，并将系统停止运行。

2.如果数据遭到破坏，系统安全负责人员负责软件系统和数据的恢复。

3.系统安全负责人检查日志等资料，确认攻击来源。

4.安全领导小组认为情况极为严重的，应立即向管理部门或上级机关报告。

第九条 病毒紧急处置

在平台运行过程中，要安装病毒防护系统，如果发现病毒，则应启动相应的应急措施，保证系统安全运行：

1.当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。

2.对该设备的硬盘进行数据备份。

3.启用反病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。

4.如发现反病毒软件无法清楚该病毒，应立即向安全小组负责人报告。

5.信息安全小组相关负责人员在接到通报后，应在十分钟内赶到现场。

6.经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即向信息安全领导小组组长报告，并迅速联系有关产品商研究解决。

7.安全领导小组经会商后，认为情况极为严重，应立即向管理部门或上级机关报告。

8.如果感染病毒的设备是服务器或者主机系统，经领导小组组长同意，应立即告知各下属单位做好相应的清查工作。

第十条 其他安全处置

当系统网络出现故障、电源中断、发生资源灾害后，也应启动相应的应急措施，保证系统安全运行，此类故障的软件处理措施基本同以上几种处理方式。