北京环球优路教育科技股份有限公司

信息系统应急管理方案

互联网研发中心

2020年1月

北京环球优路教育科技股份有限公司

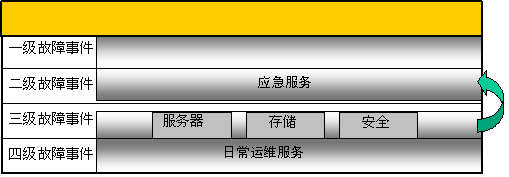
信息系统应急管理方案

1. 总 则
2. 为了保障北京环球优路教育科技股份有限公司网络与信息安全应急响应机制，规范信息安全突发事件的应急响应工作，全面提高网络与信息安全水平，切实防范和化解系统运行的风险，保障网络通信畅通，提高系统服务质量，特制定本规定。
3. 本应急恢复方案用于突发事件应急响应和恢复工作的参考文件和检查表。描述了北京环球优路教育科技股份有限公司应急恢复小组在处理造成线上阿里云服务器、线下机房的设备故障的非计划性的突发事件时所依据的策略、资源、步骤和流程。
4. 本方案适用于信息系统的突发事件，日常技术问题处理不适用本指南。
5. 此计划需要定期测试演练来不断更新，以使突发事件应急恢复小组成员熟悉恢复流程，同时验证其中所涵盖的策略、行动方案和流程准确的反应了恢复需求。
6. 本规范适用于互联网研发中心。
7. 目 的
8. 对北京环球优路教育科技股份有限公司所使用的信息系统软件由于软、硬件故障导致的非计划性停止进行快速反应；
9. 软、硬件故障发生后整个系统的切换和恢复；
10. 减少突发事件对信息系统技术和业务运营的影响，减少财务损失；
11. 减少突发事件造成的混乱；
12. 减少由于疏忽和遗漏造成的工作错误。
13. 假 设
14. 仅有北京环球优路教育科技股份有限公司互联网研发中心（数据中心）数据处理环境或者其关键组件由于非计划性事故或事件造成中止和中断。其它所有预先设计的备份中心都没有受到影响。
15. 对系统恢复所需的关键业务数据进行了全面有效的备份/复制。
16. 预先选择的恢复策略和解决方案已经实施并检验成功而且可用。（包括：备用主机、存储、数据复制系统，以及备份中心场地和备份的通讯线路等）。
17. 北京环球优路教育科技股份有限公司可以调配足够数量的具备所需技能的人员进行关键恢复工作。
18. 信息系统系统运维人员已对关键业务数据进行了全面有效的备份。
19. 在计划中存档的恢复策略和流程已经经过演练的检查且被证明是有效的。
20. 有足够数量的具备所需技能的人员可以调配来进行关键系统和业务的恢复。
21. 外部组织和机构（例如供应商和外部协作机构）在恢复期间能够提供合理的合作和响应。
22. 经常性的进行恢复预案的评估、过程维护和测试演练来保证恢复的可行性。
23. 在员工中进行了系统恢复的培训工作。
24. 有能力根据本计划的设定流程执行恢复。
25. 应急事件定义
26. 事件分级管理和定义

针对数据中心的特点，我们定义了四级故障事件，将按照以下的标准对故障事件进行分级：

1. 重大责任事故：超过一级故障限制时间的事件。
2. 一级故障事件：现有的系统硬件故障或者停机，或遭到严重攻击行为的安全事件，对业务运作有重大影响，持续小于4小时的事件。持续时间超过4小时则升级到重大责任事故。
3. 二级故障事件：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业务运作，持续小于4小时的事件。持续时间超过4小时则升级到一级事件。
4. 三级故障事件：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4小时的事件。持续时间超过4小时则升级到二级事件。
5. 四级故障事件：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48小时的事件。持续时间超过48小时则升级到三级事件。

我们定义，四级故障事件属于日常运维服务范畴，三级故障事件仍由日常运维服务处理，但需要向应急响应服务人员告知；二级故障事件和一级故障事件属于应急服务项目，故障事件从三级升级到二级时，由运维服务人员及时通知应急响应服务人员启动应急响应服务。



1. 机房故障应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 机房重大事故，断电，影响业务运行 | 一级 |  |
| 机房事故如空调等，引起系统平台故障，部分影响业务运行 | 二级 |  |
| 机房故障，未影响系统平台运行 | 三级 |  |

1. 网络设备应急事件

网络设备包括：防火墙、交换机、行为管理设备

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 中心机房防火墙、核心交换机及各应用区交换机单机硬件故障。 | 一级 |  |
| 网络故障，非网络设备硬件故障，部分影响业务运营 | 二级 |  |
| 网络故障，不影响业务运营 | 四级 |  |

1. 主机设备应急事件

主机包括：虚拟机，虚拟机物理服务器

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 虚拟机物理主机硬件故障，导致系统无法正常启动。 | 一级 |  |
| 虚拟机单机硬件故障，系统无法正常启动 | 三级 |  |

1. 备份设备应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 线上备份数据异常，数据恢复不可用 | 重大事故 |  |
| 线上备份数据异常，数据恢复部分不可用（不影响业务） | 三级 |  |

1. 通信链路应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 中心机房信息系统互联网接入线路不通 | 一级 |  |
| 中心机房至总部、基地接入线路不通 | 二级 |  |

1. 系统软件应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 数据库主机、核心应用主机系统故障无法正常启动，影响业务正常运行。 | 重大事故 |  |
| 数据库主机、核心应用服务器单台系统软件故障，影响业务运行 | 一级 |  |
| 代码服务器、堡垒机服务器软件故障，不影响业务运行 | 一级 |  |

1. 日常办公应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 办公网络链路故障，无法进行互联网操作 | 四级 |  |
| 办公硬件故障，无法进行互联网操作 | 四级 |  |
| 办公软件故障，无法进行互联网操作 | 四级 |  |

1. 数据库系统应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 微服务数据库无法正常提供服务，影响业务正常运行。 | 重大事故 |  |
| 订单、客户营销数据库无法正常提供服务，影响业务正常运行 | 重大事故 |  |
| 老网站系统数据库无法正常提供服务，影响业务正常运行 | 重大事故 |  |
| 非关键业务模块数据库无法正常提供服务，影响业务正常运行 | 一级事故 |  |

1. 应用系统应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 由于系统软件故障造成负载均衡或应用软件无法提供服务 | 重大事故 |  |
| 内存资源、数据库资源或CPU资源不能及时释放，信息系统运行过程中几乎不响应，造成无法提供服务 | 重大事故 |  |
| 信息系统运行过程中响应速度下降，内存资源、数据库资源或CPU资源不能及时释放 | 一级 |  |

1. 应用系统信息安全应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 事件级别 | 备注 |
| 网站、网页被篡改 | 一级 |  |
| 网站服务器被黑客攻击 | 二级 |  |
| 病毒感染 | 二级 |  |
| 软件系统遭受破坏性攻击 | 一级 |  |

1. 应急场景与应急处理策略
2. 机房故障应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 恢复流程 | 备注 |
| 机房事故，断电，影响部分业务运行 | 1. 监控预警、运维人员报告，启动应急流程，通知北京环球优路教育科技股份有限公司相关领导责任人。 2. 协调集成人员现场支持、运维团队监控系统平台运行状况。 3. 如果断电故障持续，系统平台安全性无法保证，经北京环球优路教育科技股份有限公司领导及相关责任人确认，关闭各系统硬件平台。 4. 断电故障恢复后，需机房管理人员提供故障报告及后续改进措施 | 线下机房为研发开发测试环境，影响互联网研发开发与测试环境运行 |
| 机房事故如空调等，引起系统平台故障，部分影响业务运行 | 1. 监控预警、运维团队人员报告发生故障，启动应急流程，通知北京环球优路教育科技股份有限公司有关领导责任人。 2. 机房管理人员响应事故，紧急处理。 3. 在空调故障排除前，协调集成人员现场支持、运维团队监控系统平台实时运行状况。 4. 如故障未及时解决，为保证系统平台安全性，请示北京环球优路教育科技股份有限公司领导确认，是否关闭平台。 5. 应急故障处理完毕，需机房管理人员提交故障报告及后续改进措施 |  |
| 机房故障，未影响系统平台运行 | 1. 监控预警、运维人员报告发生故障，通知机房管理人员及相关责任人。 2. 机房管理人员解决。 3. 故障排除后，需机房管理人员提交故障报告及后续改进措施 |  |

1. 网络设备应急处理

|  |  |  |
| --- | --- | --- |
| 故障事件 | 恢复流程 | 备注 |
| 中心机房防火墙、核心交换机及各应用区交换机单机硬件故障。 | 1. 监控预警、运维人员报告故障，启动应急流程，通知北京环球优路教育科技股份有限公司相关领导及责任人。 2. 协调集成人员，设备提供商及厂商排除故障，更换设备。 3. 更换设备到场后，恢复原有网络配置，网络测试完成，进行业务测试。 4. 落实故障原因，总结。 |  |
| 网络故障，非网络设备硬件故障，部分影响业务运营 | 监控预警、部分业务投诉、运维人员发现问题  通知相关领导责任人  运维人员排查故障，如无法解决，协调集成人员支持。   1. 故障解决后，网络测试，业务测试。 |  |
| 网络故障，不影响业务运营 | 1. 监控预警或运维人员发现故障按照日常操作维护手册解决。 2. 如碰到超出运维人员能力无法解决的问题，协调集成技术人员支持。 3. 总结故障原因。 |  |

1. 主机设备应急处理

|  |  |  |
| --- | --- | --- |
| 故障事件 | 恢复流程 | 备注 |
| 虚拟机物理主机硬件故障，导致 | 1. 监控预警、运维人员发现问题，启动应急流程，上报有关领导责任人。 2. 通知各方面人员，协调各方面人员紧急协调备机进行设备更换。 3. 设备到场后，利用原有备份数据恢复各系统。 4. 系统恢复后，启动业务，运维人员进行相关业务测试。 5. 故障总结。 |  |
| 虚拟机单机硬件故障，系统无法正常启动 | 1. 监控预警、运维人员发现问题，启动应急流程，上报有关领导责任人。 2. 通知各方面人员，协调各方面人员紧急协调备机进行设备更换。 3. 设备到场后，利用原有备份数据恢复各系统。 4. 系统恢复后，启动业务，运维人员进行相关业务测试。 5. 故障总结。 |  |

1. 备份设备应急处理

|  |  |  |
| --- | --- | --- |
| 故障事件 | 恢复流程 | 备注 |
| 线上备份数据异常，数据恢复不可用 | 监控预警、运维人员发现故障报告有关领导，启动应急流程。  备份系统故障，恢复数据异常。  运维人员远程登录，联系阿里云技术人员验证问题。  故障排除后，测试备份系统策略，保证备份策略正常运行。   1. 故障总结。 2. 调整备份策略。 |  |
| 线上备份数据异常，数据恢复部分不可用（不影响业务） | 监控预警、运维人员发现故障报告有关领导，启动应急流程。  备份系统故障，恢复数据异常。  运维人员远程登录，联系阿里云技术人员验证问题。  故障排除后，测试备份系统策略，保证备份策略正常运行。   1. 故障总结。 2. 调整备份策略。 |  |

1. 通信链路应急处理

|  |  |  |
| --- | --- | --- |
| 故障事件 | 恢复流程 | 备注 |
| 中心机房信息系统互联网接入线路不通 | 1. 系统监控预警、运维人员报告故障。启动应急流程，通知北京环球优路教育科技股份有限公司领导及有关责任人 2. 通知网络管理人员响应急故障。 3. 网络管理人员进行线路排查，解决故障。 4. 故障解决后，进行系统平台网络测试，业务测试。 5. 故障解决后，网络管理员提交故障报告及后续改进措施。 |  |
| 中心机房至总部、基地接入线路不通 | 1. 系统监控预警、运维人员报告故障。启动应急流程，通知北京环球优路教育科技股份有限公司领导及有关责任人 2. 通知网络管理人员响应急故障。 3. 网络管理人员进行线路排查，解决故障。 4. 故障解决后，进行系统平台网络测试，业务测试。 5. 故障解决后，网络管理员提交故障报告及后续改进措施。 |  |

1. 系统软件应急处理

|  |  |  |
| --- | --- | --- |
| 故障事件 | 恢复流程 | 备注 |
| 数据库主机、核心应用主机系统故障无法正常启动，影响业务正常运行。 | 1. 监控预警、运维人员报告，启动应急流程，通知北京环球优路教育科技股份有限公司有关领导责任人。 2. 运维人员恢复快照备份，利用原有备份数据恢复OS等。 3. 系统软件恢复后，恢复应用业务软件，进行业务测试。 4. 测试完成，恢复系统运行。 5. 故障总结。 |  |
| 数据库主机、核心应用服务器单台系统软件故障，影响业务运行 | 1. 监控预警、运维人员报告，启动应急流程，通知北京环球优路教育科技股份有限公司有关领导责任人。 2. 运维人员恢复快照备份，利用原有备份数据恢复OS等。 3. 系统软件恢复后，恢复应用业务软件，进行业务测试。 4. 测试完成，恢复系统运行。 5. 故障总结。 |  |
| 代码服务器、堡垒机服务器软件故障，不影响业务运行 | 1. 运维人员发现故障，解决。 2. 现场运维人员无法解决故障协调厂家技术人员协助。 3. 故障总结。 |  |

1. 日常办公应急事件

（链路、打印机、PC）

|  |  |  |
| --- | --- | --- |
| 故障事件 | 处理恢复流程 | 备注 |
| 办公网络链路故障，无法进行互联网操作 | 查询网络节点故障与原因  运维处理网络故障或更换网络接口 |  |
| 办公硬件故障，无法进行互联网操作 | 查询办公主机硬件故障与原因  运维处理网络故障或更换网络接口 |  |
| 办公软件故障，无法进行互联网操作 | 查询办公主机软件故障与原因  运维处理网络故障或更换网络接口 |  |

1. 数据库系统应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 处理恢复流程 | 备注 |
| 微服务数据库无法正常提供服务，影响业务正常运行。 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知后，立即检查微服务数据库所有节点是否都出现问题, 根据检查结果来决定下一步操作； 3. 通知DBA和技术支持远程解决，收集联机库运行日志； 4. 故障排除后，故障总结。 |  |
| 订单、客户营销数据库无法正常提供服务，影响业务正常运行 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知后，立即检查订单、客户营销数据库所有节点是否都出现问题, 根据检查结果来决定下一步操作； 3. 通知DBA和技术支持远程解决，收集联机库运行日志； 4. 故障排除后，故障总结。 |  |
| 老网站系统数据库无法正常提供服务，影响业务正常运行 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知后，立即检查数据库所有节点是否都出现问题, 根据检查结果来决定下一步操作； 3. 通知DBA和技术支持远程解决，收集联机库运行日志； 4. 故障排除后，故障总结。 |  |
| 非关键业务模块数据库无法正常提供服务，影响业务正常运行 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知后，立即检查联机数据库所有节点是否都出现问题, 根据检查结果来决定下一步操作； 3. 通知DBA和技术支持远程解决，收集联机库运行日志； 4. 故障排除后，故障总结。 |  |

1. 应用系统应急处理

应用系统包含智能运营平台、crm系统等公司自主开发业务平台系统。

|  |  |  |
| --- | --- | --- |
| 故障事件 | 处理恢复流程 | 备注 |
| 由于系统软件故障造成负载均衡或应用软件无法提供服务 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知系统异常后，立即检查负载均衡或tomcat应用节点是否都出现问题, 根据检查结果来决定下一步操作； 3. 如果发现某一节点异常，停止该节点； 4. 如果发现节点都异常，重启所有节点； 5. 如果无法解决问题，收集加日志，协调架构部门技术支持远程解决； 6. 故障排除后，故障总结。 |  |
| 内存资源、数据库资源或CPU资源不能及时释放，信息系统运行过程中几乎不响应，造成无法提供服务 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知系统异常后，立即检查系统主机是否出现问题； 3. 如果发现主机异常异常，清理系统资源、重启服务； 4. 如果无法解决问题，收集日志，协调架构不技术支持远程解决； 5. 故障排除后，故障总结。 |  |
| 信息系统运行过程中响应速度下降，内存资源、数据库资源或CPU资源不能及时释放 | 1. 启动监控预警、运维人员发现故障报告有关领导，启动应急流程； 2. 运维人员应在接到通知系统异常后，立即检查系统主机是否出现问题； 3. 如果发现主机异常异常，清理系统资源、重启服务； 4. 如果无法解决问题，收集日志，协调架构不技术支持远程解决； 5. 故障排除后，故障总结。 |  |

1. 应用系统信息安全应急事件

|  |  |  |
| --- | --- | --- |
| 故障事件 | 处理恢复流程 | 备注 |
| 网站、网页被篡改 | 1. 运维人员应在接到通知后立即清理非法信息，强化安全防范措施，并将网站网页重新投入使用。 2. 网站维护员应妥善保存有关记录及日志或审计记录。 |  |
| 网站服务器被黑客攻击 | 1. 通过入侵检测系统发现有黑客正在进行攻击时,首先应将详细情况作记录，同时向运维人员反映攻击情况。 2. 技术人员立即进行被破坏系统的恢复与重建工作。 |  |
| 病毒感染 | 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，应立即向领导报告。 5. 经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即向信息技术人员报告，并迅速研究解决问题 |  |
| 软件系统遭受破坏性攻击 | 1. 软件遭到破坏性攻击，应立即向技术人员、网络管理员报告，并将系统停止运行。 2. 立即进行软件系统和数据的恢复。 |  |

1. 应急事件响应处理流程
2. 应急处理的原则

|  |  |  |
| --- | --- | --- |
| **应急处理原则** | **方 法** | **备注** |
| 替换 | 灾难发生后，用备用设备和系统替换现有设备和系统 |  |
| 切换  (Switching) | 灾难发生后，将主业务和交易切换至另一套设备和系统 |  |

1. 应急处理流程

**应急处理流程应遵循《HQYL-YW-0002-系统业务持续性管理规定v1.1docx》的工作要求**



1. 恢复工作职责

以下是北京环球优路教育科技股份有限公司运维团队在恢复工作中需要履行的恢复职能，以保证在恢复工作时保持正确的记录和控制：

1. 对于任何针对标准操作流程的变化，准确记录恢复工作，保持书写整齐的文档记录。
2. 严格执行处置方案，若执行过程中发现事件存在方案制定时未能查明，未能预料的不利情况，应及时向指挥小组汇报。
3. 在执行过程中，有必要对处置方案进行调整的，提出建议。根据事件汇报流程，向上级机构汇报建议处置方案。
4. 保证在行动状态中最新状态通知突发事件指挥小组，按照时间顺序记录任务的执行成果，使用表格来追踪执行的任务。对恢复工作的关键里程碑的执行情况进行详细记录和跟踪。
5. 突发事件指挥小组定期分析评估事件状态等级，根据事件升、降级的决策流程和权限，决定执行事件的升级和降级程序。
6. 根据恢复要求，定期提交恢复状态报告。
7. 确保恢复工作中采取的临时变化和改动工作策略，不要带入恢复正常后的工作流程中去。
8. 恢复后验证

关键系统进行切换或者替换后，应该进行恢复后验证，检查各项IT配置和业务配置，验证关键业务和关键数据是否正常。恢复后验证包含以下几个方面：

1． 各项系统环境，应用配置通过IT检查。IT 检查清单：

|  |  |
| --- | --- |
| 系统网络配置 | 暂无 |
| 数据库配置 | 暂无 |
| 核心应用软件配置 | 暂无 |
| 其它配置 | 暂无 |

2． 各项业务测试成功，符合预期结果。业务测试清单：

|  |  |
| --- | --- |
| 正常登录综合业务系统 | 可测试登录智能运营平台 |
| 正常订单开课 | 可测试录单、开课 |
| 正常查询客户数据 | 可测试信息系统正常查询客户数据 |
| 正常查询客户数据 | 可测试信息系统正常查询客户数据 |

1. 应急演练
2. 应急演练场景01

**场景一：Nginx负载均衡服务器系统恢复事件**

1. Nginx负载均衡服务器一宕机；
2. 请求自动切换到nginx负载均衡服务器二。
3. 应急演练场景02

**场景二：前端系统服务器恢复事件**

1. 前端应用某业务节点异常，网络监控可观察节点状态，网络请求自动切换到另外一个会员前台节点。
2. 支付网关应用某业务节点异常，网络监控可观察节点状态，网络请求自动切换到另外一个支付网关节点。
3. 观察相关节点tomcat日志是否切换成功。
4. 应急演练场景03

**场景三：数据库恢复事件**

1. 数据库读节点服务器一宕机。
2. 请求自动切换到读节点服务器二或三。
3. 观察数据库日志是否切换成功。