**北京汇聚融达网络科技有限公司**

**—安全事件管理制度**

**文件编码：HJRD-5-10**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 安全事件管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-5-10 | | **牵头部门** | 技术部 | |
| **分发范围** | 制度管控员工 | | | | |
| **版本修订** | | | | | |
| **生效日期** | **版本号** | **版本说明** | **制作** | **复审** | **批准** |
| 上半年 | V1.0 | 第一版 | 刘少会/刘陵镇 | CTO | CEO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：文档基本信息记录本文档提交时的当前有效的基本控制信息，当前版本文档注有效期将在新版本文档生效时自动结束。文档版本小于1.0 时，表示该版本文档为草案，仅可作为参照资料之目的。

**第一条【编制目的】**为切实做好北京汇聚融达网络科技有限公司网络与信息安全突发事件的防范和应急处理工作，进一步提高公司预防和控制网络与信息安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保公司网络与信息安全，结合公司工作实际，制定本预案。

**第二条【适用范围】**本预案适用于全公司范围内自建自管的网络与信息系统，尤其是公司网主干设施和重要信息系统，由于自然或人为以及软硬件本身缺陷的原因，对网络与信息系统造成危害的安全突发事件的应急处置。

**第三条【编制依据】**教育部《教育系统网络与信息安全类突发公共事件应急预案》、《北京市实施<中华人民共和国突发事件应对法>办法》、《北京市网络与信息安全事件应急预案》、《北京市社会领域网络与信息安全事件应急预案》、《京汇聚融达网络科技有限公司突发事件应急预案》、《北京汇聚融达网络科技有限公司网络管理规定》、《北京汇聚融达网络科技有限公司网安全管理规程》、《北京汇聚融达网络科技有限公司网站管理办法》等相关文件。

**第四条【工作原则】**

（一）居安思危，预防为主

立足安全防护，加强预警，重点保护公司基础信息网络和数字公司信息平台等全公司性的重要信息系统，从预防、监控、应急处理和应急保障等环节，在法律、管理、技术等方面，采取多种措施，充分发挥各方面的作用。坚持提前防范，及时排查，争取早发现、早报告、早解决，化解风险，减少不良影响，共同构筑网络与信息安全保障体系。

（二）统一领导，快速反应

网络与信息安全工作领导小组统一领导、协调全公司网络与信息安全事件应急处置工作，领导小组下设办公室负责应急工作的日常管理，建立健全应急反应机制，充分发挥专家队伍和专业人员的作用。在网络与信息安全突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

（三）以人为本，减少损害

在处置网络与信息安全突发事件中，要根据实际，依法办事，合情合理，把保障公司的安全稳定及维护全公司员工的合法权益作为首要任务，防止事态扩大激化。以人为本，提前预防，及时报告，紧密衔接，及时采取措施，迅速处理，最大限度地避免信息资产遭受损失，将事态影响减至最小。

（四）自建自管，各负其责

公司各单位要按照“谁主管、谁主办、谁负责”的原则，加强对本单位建立和负责的网络与信息系统的安全管理，强化单位主要领导对网络与信息安全事件的处置职责。

**第五条【组织机构】**公司成立公司网络与信息安全事件应急处置工作领导小组，在公司网络与信息安全工作领导小组的领导下，全面负责和统一指挥公司网络与信息安全重大突发事件的应急处置工作。领导小组组长由主管网络与信息工作的副总经理担任，小组成员由公司办公室、宣传部、保卫处、网络与信息中心等部门主要负责人组成。领导小组下设办公室，办公室设在网络与信息中心。

**第六条【工作职责】**

（一）落实上级有关信息和网络安全的指示要求，制定公司网络安全与信息安全的相关规定和应急处置预案。

（二）加强公司网络与信息安全的管理，及时处置公司网络与信息安全的突发事件，保证公司网络和信息系统的正常运行。

（三）提供技术咨询、技术支持，参与重要信息的研判、网络与信息安全突发事件的调查和总结评估工作，进行应急处置工作。

**第七条【安全事件分类】**

根据北京市突发公共事件应急委员会印发的《北京市网络与信息安全事件应急预案》（京应急委发【2009】14号）和网络与信息安全突发事件的发生过程、性质和机理，网络安全事件主要分为以下几类：

（一）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其它有害程序事件。

（二）网络攻击事件分为拒绝服务攻击事件、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、干扰事件和其他网络攻击事件。

（三）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（四）设备设施故障分为软硬件设备自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障。

（五）灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

**第八条【网络安全事件分级】**

按照北京市突发公共事件应急委员会印发的《北京市网络与信息安全事件应急预案》（京应急委发【2009】14号）规定，网络与信息安全突发事件的应急响应级别分为特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级）四个级别。

（一）特别重大（Ⅰ级）：公司网络与信息系统发生全公司性大规模瘫痪，对公司正常工作造成特别严重损害，且事态发展超出公司控制能力的安全事件。

（二）重大（Ⅱ级）：公司网络与信息系统造成全公司性瘫痪，对公司正常工作造成严重损害，事态发展超出网络与信息中心控制能力，需公司各部门协同处置的安全事件。

（三）较大（Ⅲ级）：公司某一区域的网络或某一单个信息系统瘫痪，对公司正常工作造成一定损害，网络与信息中心可自行处理的安全事件。

（四）一般（Ⅳ级）：某一局部网络或某一单个信息系统受到一定程度损坏，对公司某些工作有一定影响，但不危及公司整体工作的安全事件。

**第九条【预防措施】**

进一步完善网络与信息安全突发事件监测、预测、预警制度；建立健全安全事件预警预报体系，严格执行公司网络与信息系统安全管理制度；加强对各类网络与信息安全突发事件和可能引发网络与信息安全突发事件的有关信息的收集、分析判断和持续监测。具体预防措施包括：

（一）加强宣传教育引导。加强对员工的思想教育工作，掌握舆情动态。按照早发现、早报告、早控制、早解决的原则，把问题解决在萌芽状态。

（二）完善应急管理制度。制定和落实各单位所属网络与信息系统的安全和保密相关制度，指定专门的网络与信息安全责任人及网络与信息管理员，提高有关人员的责任意识、安全意识和技术水平；建立严格的信息发布审查和检查制度，对可能引发公司网络与信息安全事件的信息，要认真收集、分析、判断，发现有异常情况时，及时防范处理并逐级报告。

（三）加强技术防范措施。公司网出入口安装必要的监测系统，对公司网进行安全扫描。坚持公司网络安全工作值班制度。加强对公司网络与公司网站等重点信息系统的监控和安全管理，做好相关数据日志记录，确定合理规则，对公司网络进出信息实行过滤及预警。

**第十条【基本响应】**

网络与信息安全事件发生后，要及时启动应急预案，实施处置并报送信息。如果有涉及到信息安全等级保护为三级的系统故障（包括停止运行、内容错误等），应将情况及时通报到北京市公安局文化保卫总队。

（一）对于软件系统类事件，及时通知公司网络与信息安全事件应急处置工作领导小组办公室，由办公室（网络与信息中心）组织技术人员采取措施及时处理，并记录处理步骤和结果，保留相关证据材料，并将处理情况上报公司网络与信息安全工作领导小组。必要时要追究相关当事人责任。

（二）对于信息安全类事件，首先及时联系信息主管单位负责人，同时通知公司网络与信息安全事件应急处置工作领导小组办公室，尽快消除不良信息。无法迅速消除或恢复系统、影响较大时要实施紧急关闭，并紧急上报公司网络与信息安全工作领导小组。属于管理不当或未遵守相关规定而导致的事件，要按规定追究相关责任。

（三）对于设施设备故障类事件，及时通知网络与信息中心或设施设备所属单位，同时通知公司网络与信息安全事件应急处置工作领导小组办公室。设施设备所属单位根据故障原因和性质，组织抢修，并上报公司网络与信息安全工作领导小组。对于人为破坏导致的设施设备故障，要按规定追究相关责任。

**第十一条【分级响应】**

分级响应针对前述的分级信息安全事件，分别做出不同的响应。

（一）Ⅲ级或IV级突发事件响应：网络与信息中心和突发安全事件的部门自行负责应急处置工作，有关情况报分管领导。

（二）II级突发事件响应：网络与信息中心立即上报分管领导和公司网络与信息安全工作领导小组，由领导小组统一组织、协调指挥进行应急处置。

（三）I级突发事件响应：网络与信息中心立即上报分管领导和公司网络与信息安全工作领导小组，领导小组再上报至市公安局等相关部门，由北京市相关部门会同我公司网络与信息安全工作领导小组统一组织、协调指挥应急处置。

**第十二条【应急处理方式】**

（一）根据网络与信息安全事件分类采取不同应急处置方式。

1.网络攻击事件：判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的IP地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

（1）病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

（2）外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的IP地址，及时关闭入侵的端口，限制入侵的IP地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

（3）内部入侵：查清入侵来源，如IP地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

2.设备故障事件：判断故障发生点和故障原因，迅速联系IT运维部尽快抢修故障设备，优先保证公司网主干网络和主要应用系统的运转。

3.灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

4.信息内容安全事件：接到网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；对公安机关要求我公司协查的外网不良信息事件，根据公司网上网相关记录查找信息发布人。

5.其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理。不能处理的及时咨询信息安全部门或顾问。

（二）根据网络与信息安全事件分级采取不同应急处置方式。

1.发现信息系统紧急情况或故障发生后，应立即上报网络与信息中心针对该系统分派的归口管理人员。归口管理人员在初步了解故障现象后，要及时协调相关方面技术人员、分支机构指定联系人、事故上报人，在短时间内（一般要在半小时以内）依据故障情形和预计修复时间进行初判，确定故障分类级别，对属于II级以上（含）的重大事件，要立即报告应急办工作领导小组常务副组长；对II级以下的事件，要立即报告处室负责人，信息系统应急处理工作启动。

2.根据不同的故障分类级别，采取相应措施进行信息系统应急处理。故障处理过程中，必要时应急办可根据需要及时调整故障级别。

I级（特别重大）：应急工作领导小组常务副组长应立即向组长汇报情况，应急工作领导小组组长马上组织应急办各工作组召开会议，商议并部署相关工作，随时对事态发展情况进行监控了解。北京汇聚融达网络科技有限公司应及时向上级领导单位报告。

II级（重大）：应急工作领导小组常务副组长应立即向组长汇报情况，并按照预定方案组织部署相关工作，将事态发展情况随时向应急工作领导小组组长汇报。

III级(较大)：相关处室负责人应立即按照预定方案组织部署相关工作，将事态发展情况随时向应急工作领导小组常务副组长汇报。

IV级(一般)：系统归口管理人员应立即按照预定方案开展故障恢复工作，将事态发展情况随时向处室负责人汇报。

3.北京汇聚融达网络科技有限公司各级机构应按照应急办的指令进行处理操作，对客户、代理人、中介机构、业务人员等做好疏导和宣传解释工作。应急办业务组应根据故障具体情况，启动相应手工业务操作流程。

4.故障排除后，应急办向相关方面发出故障解除、系统恢复正常运行通知。

5.系统恢复运行后，相关操作人员应对在故障发生前半小时内所进行过的业务操作进行检查，认真核对业务数据是否正确或有无丢失，不正确或有丢失的应马上更正或补录，确保数据的正确和完整。对故障期间手工处理的业务，应及时在系统中补充办理。

6.相关部门必须总结和分析故障发生原因，排除隐患，提出改进措施，避免再次发生同样故障，并向应急办报告。

（三）突发信息网络事件专项应急预案

1.机房渗漏水应急预案

预案适用：机房出现渗漏水。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组；

（2）指挥人员：机房管理人员；

（3）操作人员：机房管理人员、维修人员。

应急流程：

（1）立即通知网络与信息安全工作领导小组。

（2）发现空调系统出现轻微渗漏水后，应立即将机房内的积水清除干净，如渗漏水较为严重，应在重要设备关闭以后，立即切断机房内电源，并即时联系设备供应方进行处理，如为墙体或窗户渗漏水，应立即通知相关部门进行维修。

工作要求：

（1）保持机房清洁和适当的温度、湿度；

（2）修好渗水设施或设备。

应急时限：12小时。

2.机房被盗应急预案

预案适用：机房被盗。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组、安保部门领导；

（2）指挥人员：网络与信息安全工作领导小组、安保部门领导；

（3）操作人员：机房管理人员、安保人员、公安人员。

应急流程：

（1）立即通知网络与信息安全工作领导小组、安保部门；

（2）拨打110匪警电话，告知被盗地点，并在公安机关到来前保护好现场；

（3）在公安人员到来前，由当日值班人员（或盗窃发现人）在现场初步确认失窃物品种类、数量；

（4）公安人员到来后，配合做好失窃物品的审核确认工作。

工作要求：

（1）查清财产损失；

（2）不影响信息系统正常运转。

应急时限：4小时。

3.机房火灾应急预案

预案适用：机房发生火灾。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组、安保部门领导；

（2）指挥人员：网络与信息安全工作领导小组、安保部门领导；

（3）操作人员：机房管理人员、安保人员、救火人员。

应急流程：

（1）如发现火情，应该利用手持式机房专用灭火器控制火情蔓延。发现人员在处置的同时要及时通知网络与信息安全工作领导小组、安保部门领导；

（2）如果火势失去控制，切断机房市电及UPS供电线路，启动应急照明系统；

（3）组织无关人员尽快有序疏散；

（4）经请示后立即拨打119火警电话，详细告知火灾发生地点、楼层、过火面积及起火设备类型等信息；

（5）保证机房门窗关闭，防止空气进入，造成对流；

（6）利用手持式机房专用灭火器控制火情蔓延，同时等待消防部队到来；

（7）消防部队到来后，配合进行灭火工作。

工作要求：

（1）查清财产损失；

（2）检查信息系统数据情况；

（3）保证信息系统正常运转。

应急时限：1小时。

4．机房长时间停电应急预案

预案适用：机房长时间停电。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组、各相关业务部门领导；

（2）指挥人员：机房管理人员；

（3）操作人员：机房管理人员、各相关业务部门操作人员。

应急流程：

（1）通过OA发布或电话通知停电通告，要求用户在停电前停止业务、保存数据；

（2）及时通知网络与信息安全工作领导小组及各相关业务部门领导；

（3）打电话询问供电部门停电原因和停电时间；

（4）如供电部门告知停电时间将超过UPS最大供电时间，停电时应启动备用发电设备或提前关闭相关设备。

工作要求：

（1）保证业务数据不丢失；

（2）保证信息系统正常运转。

应急时限：4小时。

5.通信网络故障应急预案

预案适用：通信网络故障。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组、各相关业务部门领导；

（2）指挥人员：网络与信息安全工作领导小组；

（3）操作人员：网络管理人员、相关维护人员。

应急流程：

（1）及时通知网络与信息安全工作领导小组、各相关业务部门领导；

（2）查清通信网络故障位置；

（3）告知相关通信网络运营商及设备集成商，要求查清原因；

（4）隔离故障区域(如：切断故障区与服务器的网络联接)；

（5）会同相关技术人员检测故障区域；

（6）逐步恢复故障区与服务器的网络联接；

（7）写出故障分析报告。

工作要求：

（1）恢复通信网络；

（2）保证信息系统正常运转。

应急时限：2小时。

6.网络病毒爆发应急预案

预案适用：网络出现病毒感染。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组；

（2）指挥人员：网络与信息安全工作领导小组；

（3）操作人员：系统管理员、各相关业务部门操作人员。

应急流程：

（1）通过技术手段找到被病毒感染机器，要求相关用户切断病毒源与网络系统的联接；

（2）及时通知网络与信息安全工作领导小组和相关部门人员；

（3）启动服务器杀毒软件，检测服务器是否感染病毒；

（4）要求各工作站用户自行杀毒；

（5）系统管理员到被病毒感染机器清除病毒；

（6）写出评估报告。

工作要求：

（1）清除网络病毒，恢复数据；

（2）保证信息系统正常运转。

应急时限：4小时。

7.服务器软件系统故障应急预案

预案适用：服务器软件系统出现故障、崩溃、瘫痪。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组、相关部门领导；

（2）指挥人员：网络与信息安全工作领导小组；

（3）操作人员：系统管理人员、各相关部门操作人员。

应急流程：

（1）及时通知网络与信息安全工作领导小组；

（2）启动备份服务器系统，由备份服务器接管业务应用；

（3）将故障服务器脱离网络，保持系统状态不变，保持原始数据；

（4）重新启动故障服务器系统；

（5）重启系统成功，则检查数据丢失情况，利用备份数据恢复；

（6）重启失败，立即联系相关集成商或厂商进行维护。

工作要求：

（1）恢复服务器系统和数据；

（2）保证信息系统正常运转；

（3）各业务科室工作不受影响。

应急时限：3小时；

8.核心设备硬件故障应急预案

预案适用：当核心设备硬件（如服务器、空调、交换机、路由器等）出现故障。

负责部门：网络与信息中心。

支持部门：

（1）知情领导：网络与信息安全工作领导小组、相关业务部门领导；

（2）指挥人员：网络与信息安全工作领导小组；

（3）操作人员：系统管理人员。

应急流程：

（1）确定故障设备及故障原因；

（2）通知网络与信息安全工作领导小组、相关业务部门领导；

（3）如故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；

（4）进行故障排除工作；

（5）如果故障排除，在网络空闲时期，替换备用设备；

（6）故障仍然存在，立即联系相关厂商进行上门维修；

工作要求：

（1）保证网络正常运转；

（2）各业务系统不受影响。

应急时限：2小时。

**第十三条【后期处置】**加强网络与信息安全事件后期处置工作，实施网络与信息安全事件责任追究机制。I级特大网络与信息安全事件由公司在上级部门的指导下，组织事件的调查处理和总结评估，部署公司各相关部门负责系统的恢复重建，事件处置完成后，公司将根据调查结果追究相关责任人责任。Ⅱ级以下网络与信息安全事件由公司网络与信息安全事件应急处置工作领导小组指导相关部门进行事件调查总结和系统重建，事件处置完成后，在必要情况下，公司将根据调查结果追究相关责任人责任。

**第十四条【保障措施】**

（一）队伍保障

加强网络与信息中心的技术队伍建设，进一步完善公司各部门信息员制度，确保公司网公共服务符合技术标准和管理规范。通过技术培训、研讨、对外交流、参与会议等方式不断提高技术人员的业务水平，为公司网络和信息的安全保障提供强大技术支撑。

（二）技术保障

重视信息系统的建设和升级换代，重视网络安全整体方案的不断完善，加强技术管理，确保信息系统的稳定与安全，聘请信息安全顾问为应急处置过程和重建工作提供咨询和技术支持。

（三）经费保障

公司和各单位对于网络和信息安全方面要有必要的投入，从技术和管理上为日常管理和事件应急工作提供经费支持。公司网络与信息系统突发事件应急处置资金，应列入年度财政预算，切实予以保障。

**第十五条【宣传培训与演练】**公司宣传部、保卫处、网络与信息中心要利用适当时机，加强网络与信息安全的法律法规、新闻动态和知识技能的宣传教育，提高员工的网络与信息安全意识和应对水平。

本预案是《北京汇聚融达网络科技有限公司突发事件应急预案》的重要组成部分。公司各部门要加强网络与信息安全特别是网络与信息安全应急预案的培训，将网络与信息安全事件的应急知识列为管理干部和有关人员的考核内容，提高防范意识和技能。公司网络与信息安全事件应急处置工作领导小组加强与公司各部门的联动，组织协调公司网络与信息安全应急预案演练工作。公司网络与信息安全事件应急处置工作领导小组每年联合公司办公室、宣传部、保卫处等部门组织至少一次的安全培训和针对不同级别安全事件的预案演练，同时加强人事联动、部门联动等的联合演练，有效提高公司网络与信息安全应急处置能力和水平。公司网络与信息安全事件应急处置工作领导小组将演练情况报告公司网络与信息安全工作领导小组。