**北京汇聚融达网络科技有限公司**

**—备份和恢复管理制度**

**文件编码：HJRD-5-09**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 备份和恢复管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-5-09 | | **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【目标】**为了保证北京汇聚融达网络科技有限公司系统持续稳定的运行，加强各业务系统备份工作管理，明确和规范业务支撑网备份的各项工作和流程，提高备份工作效率，确保备份工作得到较好执行，防止系统出现异常事故造成的数据丢失，并确保系统、数据的及时恢复，特制定本管理规定。

**第二条【适用范围】**本管理规定适用于公司各个应用系统。

**第三条【职责分工】**

（一） 网络与信息中心负责制定北京汇聚融达网络科技有限公司系统的数据备份策略。

（二）系统管理员负责操作系统和数据库的备份和管理，并执行本地网数据备份策略、记录和检查相关备份操作内容。

（三）应用管理员负责应用系统和应用数据的备份和管理，并执行本地网数据备份策略、记录和检查相关备份操作内容。

（四）安全管理员负责对本地网数据备份策略执行情况的周期性审核工作。

（五）网络与信息安全工作领导小组组织各部门编写《业务连续性影响分析报告》。

（六）网络与信息安全办公室制订《业务连续性管理战略计划》。

（七）网络与信息安全办公室组织各部门编制《业务连续性管理实施计划》。

（八）网络与信息安全办公室负责对《业务连续性管理实施计划》进行测试，形成《业务连续性管理计划测试报告》。

（九）网络与信息安全工作领导小组负责对《业务连续性管理计划测试报告》进行评审，形成《业务连续性管理计划评审报告》。

**第四条【数据备份】**

（一）数据备份工作由专人（目前为“系统管理员”）负责。电子化数据必须定期、完整、真实、准确地转移到异地存储设备以进行保存。需要备份的数据包括：

1、数据库；

2、主机系统文件；

3、数据库日志文件；

（二）备份数据的介质由系统管理员负责保管，统一存放在介质保管柜中。核心数据定期通过备份软件由数据中心传至备份服务器，以确保数据的异地备份。

（三）备份数据介质的存放地点应有防火、防潮、防尘、防磁、防盗等设施，其温湿度应符合国家相关规定。

（四）网络与信息中心须对备份数据介质的内容和查询等进行登记记录，每半年对照备份数据介质的目录清单进行盘点。

（五）备份介质销毁须经相关负责人审核批准，并做好完整记录。销毁前必须清除介质中的敏感数据备份，在负责人的监控下进行彻底的物理销毁，对保密性较高的存储介质未经批准不得自行销毁。

**第五条【备份策略制定】**根据系统的重要性和业务部门的要求分别对系统的应用程序、操作系统和数据库制定备份策略并形成完整的备份策略文档，备份策略文档中必须包括备份介质恢复测试的各项要求、步骤和流程，备份策略必须通过网络与信息安全工作领导小组审批，审批通过后必须对备份策略文档及审批文档进行妥善保管，备份策略应指定专人负责执行。由专人负责填写《信息备份计划》，并定期更新。

**第六条【备份策略要求】**

（一）数据库：各系统根据数据量及系统能力每周或每月执行一次完全备份，每天必须执行一次增量备份，日志备份必须采用连续备份的方式，按需要做数据库日志归档。对于重要数据库应采取双机备份的形式；

（二）操作系统：操作系统必须每月执行一次完全备份，在对系统配置参数进行修改，或对系统补丁进行升级等系统改变后必须进行一次完全备份；

（三）应用系统：应用程序必须每月执行一次完全备份，在对应用程序进行修改后必须进行一次完全备份；

（四）网络设备配置备份：网络设备必须每月执行一次完全备份，在对设备系统配置参数进行修改，或对系统补丁进行升级等系统改变后必须进行一次完全备份

**第七条【备份策略回顾】**必须定期对备份策略进行回顾，审查备份策略是否满足数据安全和业务部门需要，根据审查结果进行调整，以确保备份能够满足数据安全和业务部门需要，并填写《备份策略回顾表》。

**第八条【备份检查】**

（一）备份任务执行情况检查

备份必须由专人负责，对于由备份软件自动执行的备份任务必须定期（每季度一次）进行检查（手工执行的备份任务则在备份完成后进行检查），以确保备份任务能够正常完成，并填写《备份结果检查表》进行登记。备份主管人员应定期（每季度）对备份结果进行审查，并填写《备份结果审查表》。

（二）备份数据恢复检查

1、必须建立备份恢复测试步骤文档，定期对备份介质（本地和异地存放）进行恢复检查，以确保备份介质数据可用。各系统根据系统能力对于数据库备份至少每半年进行一次恢复测试，把数据库恢复到测试环境，对于应用程序和操作系统的备份要求至少每个季度进行一次检查，确保备份介质存储的文件可读，每次检查均需要填写《备份恢复测试报告》对检查结果进行登记，并根据测试结果及时修改或更新灾难恢复计划；备份负责人员必须定期（每半年）对备份恢复测试情况进行检查并填写《备份恢复测试审查表》。

2、若系统所限无法进行完全恢复性测试，则可以对相关数据进行读取测试，并合理计划读取测试的频率和数据覆盖范围,使读取测试的效果接近完全恢复测试的效果.并作好相关记录和测试效果评估。

（三）备份介质寿命检查

备份介质应定期对其寿命进行检查（不少于半年），对于到达使用寿命的介质应及时更换，并填写《备份介质更换记录表》，对更换情况进行详细记录。备份主管人员应定期（每半年）对备份介质更换情况进行检查，并填写《备份介质更换审查表》。

**第九条【备份数据存放】**

（一）对备份介质定期（至少每月）执行异地存放操作，把介质（核心数据库备份必须为全备）从备份所在地转移到异地（本地和异地必须为不同的建筑物）进行存放。

（二）对于永久保存的备份介质同样需要永久保存，对于循环使用的备份介质，存放在异地的同一数据备份介质不能少于2份。

（三）把备份介质转移到异地存放和把介质从异地转移出来进行循环使用时均需要进行登记，并填写《异地保存记录表》对介质转入转出情况进行详细登记。

（四）备份负责人员应定期（每季度）对备份介质异地保存情况进行审查，并填写《异地保存审查表》，对备份介质实体和登记表的一致性进行核对，并在登记表上签名确认，如发现异常情况则必须及时整改。

（五）备份介质（本地或异地）存放地点必须安全，应存放在专用的保险柜里并上锁，钥匙由专人保管。备份负责人员需要提交一份允许使用备份介质人员名单，只有在允许使用备份介质人员名单当中并且由于工作需要而使用备份介质的的人员才可以使用备份介质，使用时必须填写《备份介质使用记录表》进行登记。备份负责人员需要定期（每季度）对允许使用备份介质人员名单进行审查，并填写《允许使用备份介质人员名单审查表》，以确保该名单的准确性。安全管理员必须定期（每季度）对《备份介质使用记录表》进行审核，并填写《备份介质使用审查表》，以确保备份介质的访问都是合法及获授权的。

**第十条【数据保密】**

（一）各应用系统必须建立按照用户类别的不同授予不同数据访问权限的控制机制。

（二）公司员工应自觉保护本校数据信息，严禁任何私自泄露、外借和转移本校内部数据信息的行为，违者将追究相关责任。

（三）公司员工在使用办公电脑时，只能拥有一般用户权限，不允许私自下载或安装与工作无关的文件和软件；如需使用新的软件，需联系系统管理员进行安装。

（四）关键业务数据和公司机密文件需要进行加密存储，经互联网或其他外部线路传输的业务数据也必须经过相应的加密技术处理。

（五）公司各部门在与外部机构开展各类协作、交流、信息系统合作开发时，必须与对方签订保密协议，并经各级法律合规部门的审核。

**第十一条【业务连续性影响分析报告】**在信息安全风险评估后进行业务连续性和影响的分析。在网络与信息安全工作领导小组的统一组织协调下，网络与信息中心及其他与业务有关的部门分别开展以下活动：

（一）对本部门的信息安全进行风险评估；

（二）识别出对本部门业务连续性造成严重影响的主要事件，如系统漏洞、设备故障等；

（三）分析这些事件一旦发生对公司业务活动造成的影响和损失，以及恢复业务所需费用等；

（四）编写本部门《业务连续性影响分析报告》，其内容应包括：

1、可能引起业务活动中断的主要事件名称；

2、识别关键业务的管理过程；

3、主要事件对本部门管理的信息系统的影响；

4、信息系统故障或中断对业务活动的影响；

5、主要事件的等级。

**第十二条【业务连续性管理战略计划】**网络与信息安全办公室根据《业务连续性影响分析报告》制订《业务连续性管理战略计划》，并提交网络与信息安全工作领导小组讨论，经公司主管信息安全领导批准后予以实施。

**第十三条【业务连续性管理实施计划】**

（一）根据《业务连续性管理战略计划》，各部门分别编制本部门管理信息系统的《业务连续性管理实施计划》，并由公司主管信息安全领导批准，以便在这些系统发生中断时实施。

（二）《业务连续性管理实施计划》应包括以下方面的内容：

1、计划实施所涉及的部门及人员的职责、权限及接口关系的描述；

2、系统中断的汇报程序及要求；

3、系统中断的恢复程序及方法；

4、系统中断的恢复时限要求；

5、保持业务运作连续应采取的应急措施与备用措施；

6、必要的技术支持及资源要求。

（三）《业务连续性管理实施计划》的实施要求：重要系统一旦受到重大影响或中断后，有关部门应立即执行《业务连续性管理实施计划》，对系统采取应急措施、进行恢复，确保业务活动的持续运行；同时按照《信息安全事件管理规定》应做好事故处理记录，记录内容应包括：

1、对系统中断原因的调查分析；

2、系统中断造成损失的统计；

3、采取的纠正措施；

4、应吸取经验教训及预防措施等。

**第十四条【业务连续性管理计划测试报告】**每年下半年由网络与信息安全办公室组织对相关部门的《业务连续性管理实施计划》进行测试，以判断计划的可行性和有效性。测试可采用以下方法进行：

（一）对已发生过的业务中断及恢复措施实例进行讨论。

（二）组织有关部门进行业务中断及恢复的模拟演练。

（三）采用技术手段对系统运行及中断恢复的相关参数进行测量。

（四）由设备供应商提供测试服务，确保所提供的服务和产品符合合同要求。

（五）测试完成后填写《业务连续性管理计划测试报告》。

**第十五条【业务连续性管理计划评审报告】**

（一）网络与信息安全办公室根据各部门的业务连续性测试报告及结果，参考学校最高信息安全策略，结合计划的适用性和有效性两项原则进行评审，形成《业务连续性管理计划评审报告》。

（二）根据《业务连续性管理计划评审报告》的要求，决定是否对《业务连续性管理战略计划》和《业务连续性管理实施计划》进行修改。