**北京汇聚融达网络科技有限公司**

**——信息安全审核控制程序**

**文件编码：HJRD-2-02**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 信息安全审核控制程序 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-2-02 | | **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** |
| 上半年工作日 | V1.0 | 第一版 | 刘少会 | CEO | CTO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

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。

# 目的

按计划的时间进行信息安全管理体系的内部审核，以验证管理活动和有关结果是否符合信息安全管理体系标准及北京汇聚融达网络科技有限公司有限责任公司（以下简称：公司）信息安全管理体系文件的要求,是否符合相关法律法规要求、客户和相关方的要求，确保信息安全管理体系与标准的符合性、适宜性和有效性。

# 范围

适用于公司内部信息安全管理体系审核的策划、实施、检查与改进。

# 术语和定义

无

# 职责

最高管理者：确保信息安全管理体系内部审计的实施，批准《年度内审方案》。

管理者代表：负责审核《年度内审方案》，批准《内审实施计划》和《内部审核报告》，成立内审小组，任命内审组长及内审员，协调纠正措施、预防措施中的有关问题；并负责程序文件的审批。

信息安全审计小组：负责编制年度内审方案。

内审小组：负责实施和协调内部审核，编制《内审实施计划》和《内部审核报告》，并归档保管内审资料。

各部门：配合内审实施，落实内审纠正措施。

# 工作程序



## 内审策划

# 5.1.1内审组织

1. 管理者代表根据《年度内审方案》，任命具备资格的内审组长和内审员，组成内部审计小组。内部审核组成员应在各室挑选,要求必须接受过信息安全管理体系标准及内部审核员培训并取得内审员资格证书。
2. 审核员应与被审核的活动无直接责任，审核员不应审核自己的工作,以保证审核的独立性。

# 5.1.2内审周期

信息安全审计小组每年年初编制《年度内审方案》，报管理者代表审核，总经理批准。主要内容包括：

1. 内部审核的目标、范围、频次和准则；
2. 参与内部审核人员的职责；
3. 内部审核所需的各项资源；
4. 对内部审核活动的监视、评价和改进的安排。

内部审核可分为集中审核和滚动审核两种方式，通常情况下，内部审核对所有各部门每12个月至少审核一次；对重要和薄弱的部门可适当增加审核次数。

当出现下列情况时，由管理者代表决定追加内部审核的次数和范围：

* 方针、目标、管理方案有重大调整时；
* 组织结构和职能分工出现重大变化时；
* 内、外部审核出现严重不符合时；
* 信息安全体系出现重大变化时；
* 采用标准、适用法律法规或验证方法出现重大变化时；
* 出现重大客户投诉或信息安全事故时；
* 其它需要增加内审的情形。

## 内审前准备

### 编制《内审实施计划》

内审组长根据《年度内审方案》在内部审核前，编制《内审实施计划》，内容包括：审核的目的、方法、审核范围、审核依据、审核时间、被审核部门、审核条款、审核员和审核地点，报管理者代表审批后，信息安全审计小组须及时发给全体受审核部门。若被审部门对计划安排有异议时，应及时通知审计小组协商调整。

### 内审小组准备会议

内部审核前，召开内审小组准备会议，内容包括：

* 说明审核的目的、范围、准则、日期、覆盖时期；
* 确定审核活动分工及日程安排，根据需要进行分组，并向内审员分配任务；
* 要求内审员熟悉审核部门使用的文件规定，编制这些部门的《内部审核检查记录表》，制定检查表的依据为信息安全管理体系标准要求、法律法规要求、体系文件、合同要求、相关方要求、体系运行中出现的和上次内审中出现的问题等；
* 解决《内审实施计划》中不明确的问题。

### 熟悉文件

在内审小组准备会议后，掌握分工审核部门的职责和文件。

### 编制《内部审核检查记录表》

内审小组在内部审核前，根据审核活动安排，按过程审核的方法，编制分工审核部门的《内部审核检查记录表》，将受审核部门在以往审核时存在的问题，列为审核重点，充分考虑审核抽样的合理性。

### 准备审核工作文件

内审小组在内部审核前，准备现场审核中使用的文件：

* 《内审实施计划》
* 编制完成并经内审组长审核后的《内部审核检查记录表》
* 《内部审核首、末次会议签到表》
* 《不符合项报告表》
* 《不符合项分布表》
* 《内部审核报告》

## 内审实施

### 首次会议

由管理者代表主持，信息安全管理委员会发起，最高管理者、信息安全管理小组、信息安全审计小组、受审核部门主要负责人及内审员参加，与会者签到，会议时间不超过30分钟。主要内容：

* 介绍审计小组成员及分工；
* 确认审核的目的、范围和准则；
* 确认审核日期和审核活动安排；
* 介绍审核方法；
* 确认向最高管理层汇报和末次会议的时间和地点；
* 审核计划中需说明的其他细节问题。

### 收集审核证据

首次会议后，内审小组根据审核活动安排的分工，进行现场审核：

* 内审员简要说明审核的目的、范围和方法；
* 被审核部门负责人介绍本部门的基本情况；
* 内审小组按照事先编好的《内部审核检查记录表》进行审核，使用正向、逆向、独立抽样等方法，通过面谈，查阅文件和记录，观察现场环境、标识和操作，收集、核实审核证据，记录在《内部审核检查记录表》上；
* 在对每一个部门审核结束后，内审员应对记录的不符合项与被审核部门负责人交换意见，进行确认。

### 内审小组交流

在每天现场审核工作告一段落后，内审组长在必要时召集内审组成员，进行内部交流：

* 交流审核中跨部门的审核线索；
* 评价各部门通用要求的审核发现；
* 协调对各部门的审核进度，必要时调整审核分工；
* 内审组长检查内审员记录的《内部审核检查记录表》，必要时安排补充审核或追踪审核。

### 形成审核结果

现场审核全部完成后，召开内审小组总结会。会议内容包括：

* 内审员将《内部审核检查记录表》记录的审核证据与审核准则比较，确定符合或不符合的事项，在《内部审核检查记录表》上标注；
* 内审员汇报审核发现的不符合项；
* 内审员依据《内部审核检查记录表》上的相关记录，填写《不符合项报告表》，描述不符合项事实，判定不符合项的性质、不符合的准则和条款，与所有《内部审核检查记录表》一并交内审组长；
* 内审组长根据《内部审核检查记录表》，审核汇总《不符合项报告表》，填写《不符合项分布表》，准备《内部审核报告》，内容包括：审核的目的、范围、准则、覆盖时期、抽样的客观性和局限性、审核综述、体系有效性评价、审核结论、纠正措施及验证要求。

### 向管理层汇报

内审组长在末次会议开始前，向总经理和管理者代表汇报内部审核整体情况和《内部审核报告》内容，征求总经理和管理者代表意见和指示。

### 末次会议

根据内审实施计划安排的时间，由管理者代表主持，最高管理者、信息安全管理小组、信息安全审计小组、受审核部门主要负责人及内审员参加，举行末次会议，与会人员签到，会议的主要内容：

* 感谢公司领导和受审核部门的支持、配合；
* 宣读《不符合项报告表》和《内部审核报告》；
* 澄清疑问；
* 请管理者代表讲话；
* 请总经理讲话；
* 再次感谢并宣布现场审核结束。

### 内审报告

末次会议结束后内审组长将《内部审核报告》报管理者代表批准后，随同《不符合项报告表》分发到各部门。

## 纠正不符合项

内部审核中发生不符合项的部门，在收到《不符合项报告表》后，由部门负责人在《内部审核报告》要求的期限内，按《纠正与预防控制程序》要求进行原因分析、制定纠正措施。

## 跟踪和验证

内审小组在《内部审核报告》要求的整改期限到期后，根据《纠正与预防控制程序》的要求，对纠正措施的实施效果进行跟踪验证，填写《不符合项报告表》的措施验证栏，提交信息安全审计小组，审计小组将效果验证的结果反馈给管理者代表。

## 记录归档

信息安全审计小组收集保管内部审核过程中形成的所有记录，在管理评审时提交讨论评审。

# 全面安全检查

每季度进行全面的安全检查

检查项包括：安全制度落实情况，安全防范措施，应急响应机制，安全隐患排查及整改。具体检查内容见《ISMS-2-D-05 信息系统安全检查表》

# 相关文件

《文件管理控制程序》

# 记录与表格

1. 《内部审核检查记录表》
2. 《内部审核报告》
3. 《年度内审方案》
4. 《信息系统安全检查表》
5. 《安全检查报告结果》