**北京汇聚融达网络科技有限公司**

**——部门设置、岗位职责**

**文件编码：HJRD-2-01**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 部门设置、岗位职责 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-2-01 | | **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。

**一、岗位职责**

**1、安全主管网位职责**

1. 协调和规范公司信息安全工作； 根据上级领导工作部署，对信息安全工作进行具体安排、落实； 组织对重大的信息安全工作制度和技术操作策略进行审查，拟订信息安全总体策略规划，并监督执行；
2. 负责协调、督促各职能部门和相关部门的信息安全工作，参与信息系统工程建设中的安全规划，监督安全措施的执行；
3. 组织信息安全工作检查，分析信息安全总体状况，提出分析报告和安全风险的防范对策；
4. 负责接受各部门的紧急信息安全事件报告，组织进行事件调查，分析原因、涉及范围，并评估安全事件的严重程度，提出信息安全事件防范措施；
5. 及时向信息安全工作领导小组和上级有关部门报告信息安全事件。 组织信息安全知识的培训和宣传工作；
6. 决定相应应急预案的启动，负责现场指挥，并组织相关人员排除故障，恢复系统；
7. 定期组织对信息安全应急策略和应急预案进行测试和演练；
8. 对安全管理员、系统管理员、网络管理员、数据库管理员进行工作指导。

**2、安全管理员岗位职责**

1. 协助建立和完善信息安全管理制度，完善的信息安全管理体系；
2. 协助建立信息安全内部审计制度，定期对信息安全风险因素进行审计和评估；
3. 具体落实各项安全管理工作，组织相关人员审核信息化建设项目中的安全方案，组织实施安全项目建设、维护、管理信息安全专用设施；
4. 在系统应用开发、技术方案设计和实施、集成等工作中提出安全技术方案并组织实施，负责系统部署上线前的安全自测试方案的审核；
5. 负责系统的日常维护，定期检查网络和系统的安全运行状况，组织检查运行操作、备份、机房环境与文档等安全管理情况，发现问题，及时通报和预警，并提出整改意见，统计分析和协调处置信息安全事件；
6. 加强信息安全知识的学习和技能掌握，及时关注国内外信息安全动态，为贯彻落实信息安全策略和方案提出合理化建议。

**3、系统管理员岗位职责**

1. 认真记录系统安全事项，及时向信息安全人员报告安全事件； 对进行系统操作的其他人员予以安全监督；
2. 对爱信诺企业征信公共服务平台系统进行管理与维护。负责系统的运行管理，实施系统安全运行细则； 严格用户权限管理，维护系统安全正常运行。

**4、网络管理员岗位职责**

1. 对外网接入、病毒防护等进行监控和管理。负责网络的运行管理，实施网络安全策略和安全运行细则；
2. 安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行； 监控网络关键设备、网络端口、网络物理线路，防范黑客入侵，及时向信息安全人员报告安全事件；
3. 对操作网络管理功能的其他人员进行安全监督；
4. 向应急管理机构和领导机构报告重大的网络安全事件等。

**5、数据库管理员岗位职责**

1. 负责公司项目的数据库架构设计、分库分表、读写分离设计、数据路由设计、分布式缓存设计等，解决多种业务模式下的可扩展、高可用、负载均衡等关键技术问题；
2. 负责对系统相关数据库产品MySQL,hadoop,Hbase的日常维护，监控和问题跟踪处理。以及相关数据库产品的安装，备份，恢复，迁移和安全等工作；
3. 对相关环境的数据库系统做好定期性能数据采集，分析数据库系统性能瓶颈，提出优化建议和方案；
4. 参与建立并完善系统和数据库等系统平台建设的整体策略，标准和规范，独立撰写数据库相关操作手册、维护技术文档等；
5. 协助指导支持各类项目的MySQL数据库设计及开发；
6. 进行知识传递，完成部门内部和部门之间相关数据库知识的培训工作。

**二、安全管理机构人员配备**

1. 系统管理员、网络管理员、安全管理员、DBA各一名；
2. 安全管理员不兼任其它管理员系统管理员、网络管理员、安全管理员、DBA岗位。

**三、授权和审批**

1. 系统操作由申请人向部门主管提交申请，部门主管同意后，交由系统管理员及安全主管审核，同意后，系统管理员进行系统操作处理；
2. 网络操作由申请人向部门主管提交申请，部门主管同意后，交由网络管理员及安全主管审核，同意后，网络管理员进行操作处理；
3. 数据库操作由申请人向部门主管提交申请，部门主管同意后，交由数据库管理员及安全主管审核，同意后，数据库管理员进行操作处理。

**四、沟通和合作**

a)加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通；

b)加强与兄弟单位、公安机关、电信公司的合作与沟通。

**五、审核和检查**

安全主管、安全管理员、数据库管理员、系统管理员负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

**六、信息安全职能部门**

总经理策划公司的组织机构形式，确定信息安全组织结构图，规定各部门的职责和权限。各部门应了解本部门的职责、权限及相互关系，以便更好地开展工作，保证ISMS的有效性，各岗位具体信息安全职责见制度开始内容。各部门职责和权限：

法人

安全主管

业务部

风险、合规部

综合、人力部

技术部

运维部

总经理

1. 为加强公司等级保护保障工作的组织协调，建立健全等级保护管理制度和运行机制，切实提高公司等级保护保障工作水平，全面提高信息系统信息安全管理能力,根据中国人民银行颁布的《金融行业信息系统信息安全等级保护实施指引》以及《国家信息化领导小组关于加强信息安全保障工作的意见》、《GB/T22239-2008信息安全等级保护基本要求》等政策要求，特制定本制度。
2. 本规定依照信息安全管理的主要领导负责原则、全员参与原则、依法管理原则、分权和授权原则和体系化管理原则编制，具体原则为：
3. 主要领导负责原则：确保公司主要领导参与并确立组织统一的信息系统信息安全保障宗旨和政策，组织有效的安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效；
4. 全员参与原则：信息系统所有相关人员普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统的安全；
5. 依法管理原则：信息系统信息安全管理工作应保证管理主体合法、管理行为合法、管理内容合法、管理程序合法；
6. 分权和授权原则：对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限。
7. 体系化管理原则:信息系统应符合信息安全相关政策的体系化管理目标和要求。
8. 本规定适用于公司。
9. 本制度旨在实现信息安全管理组织的以下目标：
10. 管理组织内的信息系统安全保护工作；
11. 管理外部组织访问组织内信息处理设施和信息资产的安全。
12. 为加强对公司信息安全管理工作的领导，贯彻落实监管部门的信息安全保护要求，经研究决定成立公司信息安全管理委员会。
13. 信息安全管理委员会为公司信息安全工作的最高管理机构。
14. 由公司总经理担任信息安全管理委员会主席，成员包括：
15. 信息技术部主管领导；
16. 各部门主管领导。
17. 信息技术部是信息安全管理工作的执行机构，负责执行信息安全管理委员会交办的各项工作，由信息技术部总经理担任负责人，成员包括：
18. 信息技术部；
19. 系统开发部；
20. 运营维护部。
21. 信息技术部应设立信息安全管理岗位，分别为安全管理员、安全审计员、网络管理员、系统管理员、数据库管理员、应用管理员，负责执行网络、系统、数据库和应用的安全管理和运维工作。
22. 信息安全管理委员会负责领导信息系统安全工作，组织职责为：
23. 根据国家和行业有关信息安全的政策、法律和法规，确定信息安全工作的总体方向、总体原则和安全工作方法；
24. 根据国家和行业有关信息安全的政策、法律和法规，批准信息系统的安全策略和发展规划；
25. 确定各有关部门在信息系统安全工作中的职责，领导安全工作的实施；
26. 监督安全措施的执行，并对重要安全事件的处理进行决策；
27. 指导和检查信息安全职能部门的各项工作；
28. 建设和完善信息系统安全组织体系和管理机制。
29. 信息技术部负责贯彻、落实和执行信息安全管理委员会下达的各项工作，组织职责为：
30. 贯彻、落实和解释国家及行业有关信息安全的政策、法律、法规和信息安全工作要求，起草信息系统的安全策略和发展规划；
31. 落实和执行信息系统信息安全工作的日常事务，对具体落实情况进行总结和汇报；
32. 负责安全措施的实施或组织实施，组织并参加信息安全重要事件的处理；
33. 负责内、外部组织和机构的信息安全沟通、协调和合作工作；
34. 组织编制和落实信息安全规划工作；
35. 指导和检查运维单位对信息系统安全工作落实情况；
36. 监控信息系统安全总体状况，提出安全分析报告；
37. 协同有关部门共同组成应急处理小组，组织处理信息安全应急响应工作；
38. 负责组织信息系统安全知识的培训和宣传工作。
39. 系统开发部负责信息系统建设开发相关工作，组织职责为：
40. 负责信息系统开发过程中的项目管理工作；
41. 负责信息系统运行维护过程中软件版本升级、功能定制等方面的开发工作；
42. 配合信息技术部完成信息系统建设规划、方案设计及编写工作；
43. 配合信息技术部完成公司管理层安排的其他相关技术工作。
44. 运营维护部负责信息系统运行维护的相关工作，组织职责为：
45. 负责信息系统上线后的运行维护工作，具体为机房管理、基础设施日常巡检、应用系统监控等；
46. 负责定期维护机房环境设施及重要信息系统设备等；
47. 负责提出应用系统非功能性需求；
48. 负责定期分析信息系统运行过程中的日志、周报、月报，并定期汇总上报管理层；
49. 负责协调并组织应对信息系统运行过程中的突发事件；
50. 配合信息技术部完成其他信息科技方面的相关工作。
51. 应建立信息安全岗位，明确信息安全岗位职责。
52. 项目计划岗位职责为：起草和编制信息系统信息安全总体规划以及计划方案，收集信息系统安全需求。
53. 项目管理岗位职责为：
54. 负责信息系统项目实施的组织、协调和验收工作；
55. 负责项目合同的管理及监督。
56. 运行维护岗位职责为：
57. 起草和编制信息系统信息安全方针、信息安全保障体系框架和信息安全策略、制度和技术规范；
58. 推动信息系统信息安全方针、信息安全策略、信息安全管理制度及信息安全技术规范的实施落实。
59. 设备资源管理岗位职责为：负责信息系统设备的管理，包括设备的报废等。
60. 安全管理员的岗位职责为：
61. 定期组织信息系统漏洞扫描和信息安全风险评估工作，形成信息系统和整体安全现状报告，并向信息安全管理委员会进行汇报；
62. 负责制定信息系统总体网络访问控制策略和规则，并对其进行监控和审计工作，定期发布策略执行情况；
63. 对网络、系统、应用、数据库管理员进行安全指导；
64. 定期收集信息安全漏洞和公告信息，告知相关安全运维管理人员；
65. 协调信息安全应急响应组织和技术支撑单位。
66. 安全审计员的岗位职责为：
67. 定期审计信息系统信息安全策略执行情况，收集信息系统日志和审计记录，并提供审计报告；
68. 对安全、网络、系统、应用、数据库管理员的操作行为进行监督，安全职责落实情况进行检查；
69. 系统管理员的安全职责为：
70. 根据信息系统安全策略定期对系统进行自评估；
71. 依照安全策略对系统进行安全配置和漏洞修补，确保安全补丁保持2个月内最新补丁；
72. 对系统进行日常安全运维管理，定期更改系统账号，并定期提交安全运行维护记录或报告；
73. 在发生系统异常和安全事件时，应能对系统进行应急处置。
74. 网络管理员的安全职责为：
75. 根据信息系统安全策略定期对网络设备、网络架构进行自评估；
76. 依照安全策略对网络设备进行安全配置和漏洞修补；
77. 对网络设备、安全设备进行日常安全运维管理，并定期提交安全运行维护记录或报告；
78. 在发生系统异常和安全事件时，应能对网络设备、安全设备进行应急处置。
79. 信息技术部应设立专职的信息安全管理岗位，并由专人负责，根据信息安全管理的实际工作情况，人员编制1人。
80. 各部门应设立专职的安全管理员。
81. 关键事务岗位应配备多人共同管理，定期轮岗，关键岗位人员配备坚持“权限分散、不得交叉覆盖”的原则，安全管理员和安全审计员不能由一人身兼。
82. 各部门应根据岗位职责，确定岗位所需要的安全技能，并对所有信息安全岗位人员进行对应的安全技能培训。
83. 信息系统的安全技术岗位可由其他相关管理员兼任，其中网络安全管理、系统安全管理、数据库安全管理以及应用安全管理工作可分别由网络管理员、系统管理员、数据库管理员以及应用管理员执行。
84. 重要业务系统操作人员应在日常工作中认真执行信息系统安全策略和技术安全规范中的各项要求。
85. 为了保证本策略文件的时效性、可有性，必须根据相关审核规定进行评审和修订，修订后重新发布。
86. 本规定的解释权归公司信息技术部。
87. 本规定自发布之日起生效。