

信息安全岗位职责

一、 总则

1. 目的

为规范信息安全管理系统中各安全岗位的人员职责，特制订本文档。

2. 范围

本规范适用于信息中心各信息安全管理岗位和人员。

3. 职责

安全工作组负责分配、协调各信息安全管理岗位的人员角色和日常工作，各岗位人员负责本岗位的日常信息安全管理。

二、 岗位职责说明

信息安全各管理岗由信息安全工作小组授权或指定，是信息安全管理体的具体执行者，设有信息安全岗、系统管理岗、网络管理岗、数据库管理岗、文档管理岗。各岗位的人员组成参见《信息安全机构设置》，各岗位职责描述如下：

1. 信息安全岗

信息安全岗是信息安全策略和相关事务的具体推动、执行和实施者，是信息安全各项任务的具体落实者。信息安全岗主要职责包括：

（1） 网络安全设备的日常运维管理，防护策略调整，访问策略设置和调整。

（2） 在信息安全工作小组确定的实施范围内，具体推广并落实各项策略要求和控制措施。

（3） 监督推动安全策略和控制措施的落实，负责信息安全意识提升和协助信息安全事件的应急处理。

（4） 负责信息安全的日常工作，提供信息安全支持服务，配合完成信息安全相关项目，并引导、推广和监督执行安全策略。

（5） 为信息安全工作小组制定安全指标和采集数据提供支持，进行内审资料 and 数据的提取。

（6） 协助信息安全工作小组制定相关安全制度和应急预案，提供各

种参数依据。

2. 数据库管理岗

数据库管理岗主要负责各信息系统配套的数据库管理工作，主要职责包括：

- (1) 全面负责数据库系统的管理工作，保证其安全、可靠、正常运行。
- (2) 负责信息中心数据库服务器的管理工作，做好服务器的运行记录，当服务器出现故障时，迅速会同相关人员一同解决。
- (3) 负责数据库系统的建设，做好服务器的维护、数据库软件的安装、数据库的建立工作，定期对数据进行备份。
- (4) 负责数据库服务器的安全防范管理工作。
- (5) 协助软件开发人员完成数据库软件开发所需的各类数据库的信息。

3. 系统管理岗

系统管理岗主要负责各业务系统的日常运维和管理，主要职责如下：

- (1) 提供业务系统运行保障，维持业务系统稳定、正常运转，及时解决业务系统运行故障，确保用户能安全高效的使用业务系统；
- (2) 做好服务器配置、安装和改动记录，定期查看系统运行日志，并将系统故障、可疑日志及时上报安全管理员。
- (3) 定期对业务系统服务器硬盘进行整理，清除缓存或垃圾文件。
- (4) 严格按照信息安全账号管理规范，管理业务系统用户账号，划分账号角色和权限，及时删除废弃用户，监督用户设置账号强口令。
- (5) 按照病毒防护管理程序，负责对业务系统服务器安装防病毒软件，并及时升级病毒定义文件。定期对服务器进行全面的病毒检测查杀。对检测出的病毒要做病毒记录，并及时上报安全管理员。
- (6) 采用多种形式，进行系统重要数据的定期自动备份或手工备份，保证系统数据安全。
- (7) 与业务经办人员接口，按照相关安全管理规范，负责系统变更需求的响应和处理。

4. 网络管理岗

网络管理岗主要负责网络平台的日常运维和管理，主要职责如下：

文档密级：C

- (1) 负责公司网络的搭建、配置、管理和维护工作，为内部网的安全运行提供技术保障。
- (2) 负责网络设备的配置调整、更改，人员网络接入处理。
- (3) 依据 VPN 安全管理规定，负责 VPN 链路的运行维护，VPN 账号的审核、发放、注销。
- (4) 定期查看网络设备运行日志，并将可疑日志及时上报安全管理员。

5. 文档管理岗

文档管理岗主要负责信息安全管理体制制度文件的评审记录、授权修订、过程文档的归类整理，过程记录。具体职责如下：

- (1) 贯彻执行信息安全管理体制方针、政策，接受信息中心监督及检查，推动管理体制逐步标准化、系统化、规范化。
- (2) 负责管理体制过程文档的收集、整理、归档和保管工作。
- (3) 积极主动地收集各科室、岗位的过程文档，认真验收并办理好移交手续。
- (4) 将收集过程文档系统整理、编排、根据各管理模块分类归档。
- (5) 做好管理体制文件保密工作，不得将体系文件与配套的过程文档未经批准私自泄露给第三方。

三、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。
2. 本制度由公司信息安全局负责解释和修订。
3. 本制度自发布之日起开始执行。