|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | 融创物业集团规章制度手册文件 | | | | | 编号： | | |
| 版本：V1.0 | | |
| **融创物业集团**  **IT基础架构管理制度** | | | | | | | | | | |
| 主责部门： | | 物业集团信息管理部 | | | 日期： |  | | | |  |
| 会签部门： | |  | | | 日期： |  | | | |  |
|  | |  | | |  |  | | | |  |
|  | |  | | |  |  | | | |  |
|  | |  | | |  |  | | | |  |
| 修订记录 | | | | | | | | | | |
| 日期 | 修订状态 | 修改内容 | | 修改人 | | | 审核人 | | 批准人 | |
|  |  |  | |  | | |  | |  | |
|  |  |  | |  | | |  | |  | |
|  |  |  | |  | | |  | |  | |

目 录

[1 目的和原则 3](#_Toc488339235)

[2 范围 3](#_Toc488339236)

[3 术语和定义 3](#_Toc488339237)

[3.1 基础架构 3](#_Toc488339238)

[3.2 机房基础设施 3](#_Toc488339239)

[3.3 UPS系统 3](#_Toc488339240)

[3.4上网行为管理 3](#_Toc488339241)

[3.5 负载均衡 4](#_Toc488339242)

[3.6 数据库系统 4](#_Toc488339243)

[3.7 灾难备份 4](#_Toc488339244)

[4 职责 4](#_Toc488339245)

[4.1 集团基础架构负责团队 4](#_Toc488339246)

[4.2 区域分公司IT团队 4](#_Toc488339247)

[4.3 城市分公司IT团队 5](#_Toc488339248)

[5 基础架构服务总体要求 5](#_Toc488339249)

[5.1 基础架构整体质量要求 5](#_Toc488339250)

[5.2 值班制度 5](#_Toc488339251)

[5.3 巡检制度 5](#_Toc488339252)

[5.4 基础设施例行维护 6](#_Toc488339253)

[5.5 集团月度报告制度 6](#_Toc488339254)

[6. 机房基础设施管理 7](#_Toc488339255)

[6.1 分工和要求 7](#_Toc488339256)

[6.2 机房选址 7](#_Toc488339257)

[6.3 机房供配电 7](#_Toc488339258)

[6.4 机房消防 8](#_Toc488339259)

[6.5 机房空调 9](#_Toc488339260)

[6.6 机房UPS 9](#_Toc488339261)

[6.7 布线规范 10](#_Toc488339262)

[6.8 机房维护人员管理 11](#_Toc488339263)

[7 服务器管理 11](#_Toc488339264)

[7.1 分工和要求 11](#_Toc488339265)

[7.2 集团及分公司服务器硬件配置要求 11](#_Toc488339266)

[7.3 采购 12](#_Toc488339267)

[7.4 安装与配置 12](#_Toc488339268)

[7.5 退役与回收 13](#_Toc488339269)

[8 存储系统管理 13](#_Toc488339270)

[8.1 分工和要求 13](#_Toc488339271)

[8.2 集团及分公司存储架构要求 13](#_Toc488339272)

[8.3安装与配置 14](#_Toc488339273)

[8.4 维护 14](#_Toc488339274)

[9 数据库管理 15](#_Toc488339275)

[9.1 分工和要求 15](#_Toc488339276)

[9.2 远程登录管理 15](#_Toc488339277)

[9.3 应用系统连接账号 15](#_Toc488339278)

[10 备份管理 17](#_Toc488339279)

[10.1 分工和要求 17](#_Toc488339280)

[10.2 集团系统备份策略设计及调整 17](#_Toc488339281)

[10.3 集团系统备份执行 17](#_Toc488339282)

[10.4 集团备份检查及演练 18](#_Toc488339283)

[10.5 集团备份恢复 18](#_Toc488339284)

[10.6 分公司数据备份 19](#_Toc488339285)

[11 网络管理 20](#_Toc488339286)

[11.1 集团及分公司网络规划和架构设计 20](#_Toc488339287)

[11.2 集团及分公司网络工作分工 21](#_Toc488339288)

[11.3 数据中心机房互联网出口 21](#_Toc488339289)

[11.4 总部及分公司办公互联网出口 21](#_Toc488339290)

[11.5 总部与分公司的网络连接 22](#_Toc488339291)

[11.6 项目网络连接 22](#_Toc488339292)

[11.7 无线网络规划 23](#_Toc488339293)

[11.8 在公司外部访问信息的网络连接 24](#_Toc488339294)

[11.9 专用系统的特殊访问规定 24](#_Toc488339295)

[12 附录 25](#_Toc488339296)

# 1 目的和原则

本制度参考B级机房建设标准，通过关键链路、关键设备、关键部件的冗余配置以及备份措施，保障基础架构服务安全稳定，确保各应用系统不因基础架构服务故障导致中断运行。使基础架构的管理依据本制度开展工作，推动管理水平提升。

# 2 范围

本指引适用于集团、各分公司，物业公司以及合作公司视情况参照执行。

基础机构管理的范围包括集团及各分公司、机房基础设施、服务器、存储、网络、备份、操作系统和数据库。视频会议系统，电话系统，打印一体机系统，按照行政办公相关制度管理执行。

# 3 术语和定义

## 3.1 基础架构

支持应用系统运行的底层设备和服务，例如机房基础设施、服务器、网络、存储、操作系统、数据库、备份等，统称为基础架构。

## 3.2 机房基础设施

机房基础设施是指机房内部的装饰装修、供电、消防、制冷等环境因素，这些因素支持计算、网络和存储设备能够安全可靠的运行。

## 3.3 UPS系统

UPS指不间断电力供应系统，能在机房计划内或计划外断电情况下保持一定时间的电力供应。

## 3.4上网行为管理

上网行为管理是以深度包检测技术为核心，以用户、时间、位置、协议、内容格式管控用户上网行为。并结合最大带宽限制、保证带宽、应用优先级等一系列带宽管理功能，保证关键业务带宽，限制非业务带宽，改善整体网络的服务质量。

## 3.5 负载均衡

负载均衡是为减轻某个或某些设备的负载，将任务通过某种策略分配到多个设备或者链路上去，实现负载在不同实体间的平衡。

## 3.6 数据库系统

数据库是按照一定数据结构来组织、存储和管理数据的仓库，它是存储在一起的相关数据的集合，可以为多种应用提供数据服务，例如财务管理、生产管理、仓库管理等。

## 3.7 灾难备份

灾难备份是信息系统应用中为预防出现各类灾难损毁系统而进行的备份，可以分为数据备份、软件备份、硬件备份。出现系统损毁后，运用备份的设施迅速恢复系统运行。

# 4 职责

## 4.1 集团基础架构负责团队

1. 负责集团整体基础架构服务的规划、实施
2. 负责维护集团基础架构服务的正常运行，保证服务质量
3. 负责管理集团基础架构资产和资源
4. 负责管理集团基础架构服务供应商
5. 负责指导各地分公司完成区域公司、城市、项目的IT基础架构实施和日常维护工作，并进行评价
6. 负责定期向上级领导汇报基础架构服务水平

## 4.2 区域分公司IT团队

1. 负责区域分公司基础架构服务的规划和建设
2. 负责维护区域公司基础架构服务的正常运行，保证服务质量
3. 负责管理区域分公司基础架构资产和资源
4. 负责管理各分公司基础架构供应商
5. 负责贯彻集团基础架构管理制度，接受集团基础架构团队指导，并给出反馈意见
6. 负责指导城市、项目的IT基础架构实施和日常维护工作，并进行评价

## 4.3 城市分公司IT团队

1. 负责城市分公司基础架构服务的规划和建设
2. 负责维护区域公司基础架构服务的正常运行，保证服务质量
3. 负责管理区域分公司基础架构资产和资源
4. 负责管理各分公司基础架构供应商
5. 负责贯彻集团基础架构管理制度，接受区域IT团队指导，并给出反馈意见。
6. 负责项目的IT基础架构实施和日常维护工作

# 5 基础架构服务总体要求

## 5.1 基础架构整体质量要求

1. 集团基础架构要求

集团基础架构服务应保障稳定、安全、高性能的运行，进而保障上层业务系统的可靠运行，不会因为基础架构服务故障导致业务系统中断服务。同时，基础架构服务的搭建还应支持可管理性以及可扩展性，以满足集团未来业务不断发展的需要。

1. 分公司基础架构要求

分公司基础架构服务应确保分公司基础架构安全、稳定，能够满足员工使用内网及外网服务的需求，可以为员工提供高质量IT服务。

## 5.2 值班制度

各级基础架构相关负责人，工作时间为公司规定的正常工作时间。非工作时间保持手机待机，随时可以联系并处理紧急问题。

如果有对公司影响重大的事件发生，集团基础架构团队和分公司IT 团队应配合相关业务系统团队，安排人员值守，确保业务运行平稳，有问题可以及时恢复。

## 5.3 巡检制度

1. 机房巡检：

机房应安排人员定期巡检。巡检过程中，要及时记录机房内相关设施的工作状态和告警信息，包括UPS 负载、UPS 故障告警、环境温湿度、空调漏水告警等。 发现故障及时维修。 表格见《机房巡检记录表》（附件二12.2）。

1. 服务器巡检：

机房内所有服务器需要定期巡检，检查硬件有无故障，网络连通性，各项资源使用率等，并做相关记录。及时掌握服务器使用情况和状态，发现故障及时更换备件或报修。

1. 存储设备巡检：

存储设备需要定期巡检，检查硬件有无故障，存储空间使用情况等，并做相关记录。发现故障及时更换备件或报修。

1. 网络巡检：

所有网络设备需要定期巡检，检查硬件有无故障，端口流量状态等，并做相关记录。发现硬件故障及时更换备件或报修，发现端口流量异常及时分析并做处理。

## 5.4 基础设施例行维护

机房基础设施需要定期安排例行维护，每次维护完成后要有书面报告记录维护情况，给出建议。

1. 机房空调维护

主要维护内容有：室外机清洗，更换滤网，检查主机工作状态，检查冷媒管、冷凝水管状态等。各分公司可以根据当地情况合理安排维护内容。

1. UPS维护

主要维护内容有：负载检查、故障及告警检查、电池组放电测试等。各分公司可以根据当地情况合理安排维护内容。

1. 消防维护

主要维护内容有：控制箱检查、告警测试、气压测量等。各分公司可以根据当地情况合理安排维护内容。

## 5.5 集团月度报告制度

基础架构负责人每月出具一份月度运行报告，显示基础架构服务当月总体运行情况。报告内容应包括：当月人员进出机房情况，机房温湿度情况，UPS负载情况，互联网带宽使用情况，服务器资源使用情况，存储资源使用情况，备份任务执行情况，事件及处理情况等。

# 6. 机房基础设施管理

## 6.1 分工和要求

集团基础架构团队主要负责集团机房的选址、建设以及维护，同时指导分公司IT 团队进行机房建设和管理。要确保机房安全稳定运行，保障服务器、网络、存储等设备有可靠的外部环境。

分公司IT 团队主要负责分公司机房的选址、建设和维护，同时接受集团基础架构团队的业务指导，保障机房能为设备提供安全稳定的运行环境。

## 6.2 机房选址

1. 集团数据中心和核心机房选址

基础设施负责人参照B级机房建设标准，充分考虑承重、层高、位置等环境因素提出选址要求。行政部门根据要求选择符合条件的场所，并由集团基础架构负责人确认。

数据中心和核心机房尽量不要在顶层或者地下室，避免外界水渗漏造成问题，影响机房正常运行。如客观条件限制只能选在顶层或者地下室，要做好相关的防水排水措施。

要远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的场所，以免这些有害物质影响机房内设备正常运行。还要远离常见的潜在隐患区域，例如如茶水间，楼宇强电竖井等。

1. 集团及分公司非核心机房选址

基础设施负责人根据C级普通机房标准，考虑设备数量、布线距离、周围环境等因素提出选址要求。行政部门根据要求选择符合条件的场所，并由分公司基础架构负责人确认。

要远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的场所，以免这些有害物质影响机房内设备正常运行。远离常见的潜在隐患区域，例如如茶水间，楼宇强电竖井等。

## 6.3 机房供配电

1. 集团数据中心及核心机房供电要求

根据机房内设备用电总体情况评估用电量，按用电量要求使用符合标准的线缆。数据中心及核心机房应独立供电，与办公区供电分离。数据中心和机房内要有配电箱，可以控制机房内所有设备的电源供电。

1. 分公司机房供电要求

根据分公司机房内设备用电总体情况评估用电量，按用电量要求使用符合标准的线缆。机房内要有配电箱，可以控制机房内所有设备的电源供电。

1. 集团数据中心机柜供电要求

机房内每个机柜要安装双路供电PDU ，供电PDU 负载要考虑机房三相负载均衡问题。PDU 插座数量需满足机柜内所有设备的供电需求。PDU 工业连接器可以位于机柜下方或上方。

1. 分公司机房机柜供电要求

分公司可以根据当地情况安装机柜供电，应保障使用双路供电，可以使用普通插线板替代PDU。

1. 防静电措施

所有机房内应采取防静电措施，防静电地板、机柜、桥架、天花以及其它金属管线，均应良好接地并相互妥善连通。

1. 市电安装

所有机房内部应安装市电插座，并与UPS 插座区别标识，用于设备检修。

## 6.4 机房消防

1. 集团数据中心及核心机房气体灭火设备安装

数据中心及核心机房应安装独立气体灭火系统，可以在火灾发生的情况下发出告警信息，及时灭火，又不至损坏机房其它设备。

1. 分公司及非核心机房消防要求

分公司及非核心机房可不安装独立气体灭火系统，但需要放置气体灭火器。

1. 集团消防配套设施

数据中心及核心机房内应安装应急照明和疏散指示标志，并做定期检修，方便险情发生时人员可以及时疏散。

所有机房需要安装防火门，以隔离火灾烟雾等。

1. 培训制度

基础设施负责人需要对团队新入职员工进行机房消防知识培训，使新员工了解该如何处理火灾情况。

基础设施负责人原则上应每年组织进行一次团队全员消防培训，可邀请消防专业人员讲解机房消防知识，组织机房消防演练。分公司可根据当地情况执行。

1. 机房隐患消除

所有机房内禁止使用干粉及水消防喷淋设备，防止在灭火过程中对其它设备造成损害。

原则上，所有机房内应保持清洁，定期清理，禁止堆放易燃物品等杂物。各分公司可根据当地情况执行清理。

所有机房内严禁吸烟，禁止见火。施工过程中需要见火的情况，施工方需提前向基础设施负责人及相关单位报备，并做好防火措施。对违反规定的施工方人员，可以要求其离开现场，终止其施工资格并通知施工单位负责人。严重情况下，可以终止与施工方合作关系。

## 6.5 机房空调

1. 集团及区域核心机房空调设计与安装要求

所有机房内空调要有2台以上，以实现冗余配置，保证机房制冷工作不因空调故障而中断。

空调安装时，需要做好减震防噪，减轻噪声污染。不将空调主机设备放置在机柜或其他设备上方，并做好防漏水工作。

1. 冷热循环

空调可以采用下送风或者上送风的形式，出风口位于机柜前方以增加散热效率。如果有回风口，可以位于机柜后方。

1. 分公司机房空调设计要求

各分公司可以根据当地实际情况安装机房空调。在保证机房温度不超过23摄氏度的情况下，分公司可以自主选择是否安装独立空调，或者使用大厦中央空调，或不安装空调出风口。

## 6.6 机房UPS

1. 集团及区域分公司核心机房设备要求

UPS 电源是保证机房内计算机设备及其他设备正常运行和数据安全的重要设备，应使用市场主流品牌，UPS 容量根据机房UPS 供电设备总负载计算，并考虑未来扩展需求。

所有UPS 电池组后备时间要大于1小时。

除基础设施负责人外，未经许可其他人员不得随意触碰UPS 主机控制面板和开、关机。

1. 设备安装

数据中心和办公核心机房应安装在线单机式UPS 系统，即主机 + 电池组。电池组重量达到或超过楼板承重重量时，需要安装散力架。

楼层分机房可以安装在线机架式UPS 电源，每个机架式UPS 仅为单个机柜里的设备提供供电。

1. 停电通知

机房计划停电时间超过电池组后备的情况下，要至少提前两天通知服务器负责人和网络负责人关闭机房内的设备，待供电恢复之后重新打开。

1. 分公司非核心机房要求

分公司非核心机房，可以根据当地情况自主选择是否安装UPS系统。

## 6.7 布线规范

1. 强电布线要求

强电线缆配线时，所用导线横截面积应满足用电设备的最大输出功率，杜绝不同线径混用或并用。

强电线缆需延强电桥架铺设。强电桥架可以位于机柜上方，也可以位于机柜下方。在强电线路铺设安装时，需严格按照行业安全规范，避免发生安全事故。

1. 弱电布线要求

机房内设备间布线系统，使用6类UTP 线缆。

办公区水平布线系统，使用超5类或6类UTP 线缆。

弱电线缆延弱电桥架铺设，弱电桥与强电桥架分开架设，可以位于机柜上方，也可以位于机柜下方。

线缆不能放成死角（即小于90度夹角）或打结，以保证线缆工作性能良好，在水平线槽中敷设电缆时，电缆应顺直，尽量避免交叉。

所有信息点与配线架之间的线路必须经过专业网线测试设备（如Fluke 、安奈特）针对电气指标进行测试，并且全部合格。

## 6.8 机房维护人员管理

第三方维护人员进入机房，需要出示相关工作证件。进入机房后要有公司员工陪同，并在机房人员出入表登记信息，见附件一《机房人员进出登记表》。

未经许可，不得在机房内进行拍照和摄影，不得触碰维护内容以外的任何设备和设施。

维护结束后，应归还所借材料和工具，并保持工作区清洁。

# 7 服务器管理

## 7.1 分工和要求

集团基础架构团队主要负责集团所有生产及测试服务器的采购、安装、维护、监控、退役，保障服务器稳定运行，可以支持业务系统安全无中断运行。

分公司IT团队主要负责分公司机房内的服务器采购、安装、维护、监控、退役，要求保障分公司机房内的服务器稳定运行，出现故障可以及时恢复。

## 7.2 集团及分公司服务器硬件配置要求

1. 硬件配置要求

为降低设备复杂度，提高服务器可运维性，机房内服务器集中选用市场占有率高的两家主流品牌。

数据中心内服务器使用虚拟化环境，应根据需求选择CPU 、内存、硬盘配置，新采购服务器应当达到当年市场中高端配置水平，保障业务系统可以持续高性能运行，资源可以得到合理充分利用。

1. 服务器设备清单

应建立并维护服务器设备清单。见《服务器资产清单表》（附件八12.8）。

1. 服务器管理

原则上，服务器应由集团集中维护管理，区域及城市分公司不得私自安装服务器到内网。如分公司需要在当地机房安装服务器，需由分公司IT 团队向集团基础架构团队提出邮件申请，经过批准后方可安装。分公司服务器由当地IT 团队依照本制度负责管理。

## 7.3 采购

1. 项目系统采购

项目系统负责人根据项目实际需求填写硬件需求提报单，见附件十一《系统硬件需求提报单》。服务器负责人根据项目系统所提要求评估资源，并在约定期限内分配所需资源。如需采购新服务器，按公司采购流程执行。每次采购需要有3家以上不同代理商参与招标。

1. 设备更新采购

服务器因为性能及可靠性等原因需要更新的，根据旧服务器的配置情况，并考虑未来资源需求，采购当前市场主流配置服务器。

1. 服务要求

服务器采购需包含上架服务。 数据中心和机房服务器需要3年原厂专业技术支持，服务标准通常情况下为5x8下一工作日上门。关键应用服务器，可选择7x24 4小时上门服务。

## 7.4 安装与配置

1. 服务器放置

所有服务器要上架安装在服务器机柜里，并连接双路电源供电。禁止将尚未退役的服务器搬出机柜和机房。

1. 服务器检测

供应商安排工作人员上门安装服务器，安装完成后需要做加电测试，发现硬件问题及时报修处理。

1. 服务器硬盘配置

服务器硬盘组要求配置Raid ，并且硬盘组有热备份硬盘保证可靠性。

1. 操作系统安装

服务器负责人负责安装操作系统，安装之前要检查服务器硬件工作状态，如无问题再进行安装。操作系统和版本，需根据需求确认，并按照集团要求，安装稳定版本。

服务器管理员密码必须复杂，且定期修改，并有书面记录。表单禁止与基础架构团队以外人员分享密码。

1. 补丁更新

所有Windows 系统，需要每月安装重要补丁更新。安装之前要通知系统负责人，并由系统负责人审核，审核通过后方可安装。安装补丁更新后，应检查系统工作状态，发现问题及时卸载所安装的补丁。

除非有明确需求，否则Linux/VMWare 不需定期更新。

1. 服务器变更

服务器的停机维护和升级必须有预案和实施记录。对服务器配置的重大修改原则上应当做到一人操作，一人监督。服务器配置发生变化的，需及时记录。见《设备配置变更表》（附件三12.3）。

## 7.5 退役与回收

服务器使用超过3年以后，应采购原厂维保服务继续使用。超过5年以后，不再采购维保服务，应根据情况评估，如果可以继续使用，转做测试环境服务器。如果不再继续使用的，将数据和服务迁移后下架，按照相关资产管理规定做回收处理。

# 8 存储系统管理

## 8.1 分工和要求

集团基础架构团队负责集团机房内存储系统的采购和维护，确保存储系统高可靠性。

分公司一般不使用专业存储系统。如果要使用存储系统，分公司IT 团队主要负责存储系统的采购和维护，确保存储系统的高可靠性。

## 8.2 集团及分公司存储架构要求

1. 总体要求

存储负责人负责存储架构设计，应使用主流品牌SAN 存储系统，支持将不同应用的数据存储在集中的存储设备中。具备冗余性，使整个存储系统有高可靠性、可扩展、易管理、易使用、性能优良等一系列优势，可以满足公司中长期发展的数据存储需求。

1. 集团整合要求

为降低机房内系统复杂度，提高存储系统可维护性，未来将逐步精简和整合目前使用的多个存储设备，使所有数据集中存储在一个平台上。

1. 分公司使用要求

原则上，分公司不使用SAN 存储系统，分公司IT 团队无需管理SAN 存储系统。如需使用存储系统，应由分公司IT 团队向集团基础架构团队提出邮件申请，经过批准后方可使用。

分公司可以根据当地具体需求，使用简单管理的NAS 存储系统，而无须经过集团批准。

## 8.3安装与配置

1. 设备安置

存储设备由厂家安排工作人员安装上架，在机柜中连接双路电源供电，并做加电测试，发现问题及时修复。

1. 多路径配置

存储系统应保持多路径连接，相关组件都有冗余配置，以保障访问的可靠性。

1. 硬盘配置

存储系统硬盘组要求配置Raid ，并且硬盘组有热备份硬盘保证可靠性。

存储总容量根据系统实际需求确定，并考虑将来扩展。单盘容量根据总容量需求，及盘柜和硬盘插槽数确定。

## 8.4 维护

1. 备件

库房应准备一定数量的硬盘备件，发现故障第一时间更换备件。如无可更换备件，应及时向供应商报修。

1. 维保服务

存储设备要有维保服务，维保服务到期之前需要及时续保，确保硬件问题可以得到及时修复，保障数据安全。

1. 存储扩容

存储需要扩容时，由存储负责人向基础架构负责人提出申请，审核通过后再进行扩容。扩容操作需保证已存在的数据不受影响，不做调整。

# 9 数据库管理

## 9.1 分工和要求

集团基础架构负责集团业务数据库的安装、管理和维护，确保数据库的高可靠性、高可用性和安全性。

分公司一般不使用数据库系统。如果使用数据库系统，分公司IT团队负责数据库的安装、管理和维护，确保数据库的高可靠性、高可用性和安全性。

## 9.2 远程登录管理

1. 登录人员管理

数据库管理员及甲方开发人员具有直接登录业务数据库权限，如有第三方人员登录操作的情况需经过IT负责人审批，并在信息化人员监督下远程操作。测试、开发数据库经过批准可提供第三方人员使用。

1. 登陆权限控制

数据库管理员具有数据库操作最高权限，项目开发人员经过批准后具有数据库表、视图操作权限，数据库管理员具有操作数据库文件、底层参数的权限，项目人员如需要对数据库进行底层修改，需向数据库管理员提报申请，由数据库管理员进行操作。

1. 操作记录

登录数据库的日常操作和巡检动作需进行记录，由数据库管理员存档备查。

## 9.3 应用系统连接账号

1. 账号安全

在系统正式使用前，数据库管理员应修改系统默认密码，将对不需要的账号进行删除或锁定。

数据库管理员为每一个应用系统根据需要的权限建立专门的账号，以区分责任，提高系统的安全性。对账号权限的设置遵循从最小化原则。

1. 用户权限

针对每个数据库账户按最小权限原则设置其在相应数据库中的权限，权限需求由系统项目经理提供，数据库管理员审核并分配权限。包括如下几种权限：

系统管理权限：包括账户管理、服务管理、数据库管理等；

数据库管理权限：包括创建、删除、修改数据库等；

数据库访问权限：包括插入、删除、修改数据库特定表记录等。

1. 口令管理

登录口令由数据库管理员设置，正式业务数据库口令必须满足复杂策略，满足长度、数字英文、大小写混合要求。

应定期或不定期修改数据库管理员口令，在下述几种情况下必须修改口令：

数据库正式使用之前；

数据库系统或相关的应用系统遭到入侵；

数据库管理员轮换；

数据库管理员口令泄露；

1. 紧急事故处理

应对系统安装、设置更改、账号变更、数据库文件变更、数据库备份等系统维护工作进行记录，以备查阅。

结合应用系统、制定紧急事故预防措施和应急处理措施，并配备应急处理人员，基础架构负责人定期检查紧急事故预防措施的执行情况。

对出现紧急情况影响面大的核心应用系统，设立专门应急处理小组（成员包括：IT主管领导、业务部门对接人、数据管理员、软件实施团队、基础机构运维团队），实现快速协调。

# 10 备份管理

## 10.1 分工和要求

集团基础架构团队负责管理集团内备份系统，计划并执行数据备份任务，检查备份作业执行情况并定期验证，确保数据安全性和可靠性，需要时候可以在要求的时间内恢复历史数据。

分公司IT 团队负责为用户提供集中的数据保存空间，管理和执行用户关键数据备份，保障用户数据的安全可靠。

## 10.2 集团系统备份策略设计及调整

1. 备份范围

为确保所备份的内容可再现系统的运行环境，数据备份内容需包括数据中心所有关键业务数据，包括：应用系统、数据库、文件类系统。

1. 备份条件

当进行软件安装、系统升级或更改配置时，应进行系统和数据、设备参数的完全备份。应用系统更新后，应对原系统及其数据的完全备份资料保存三个月以上。

1. 备份策略

对数据库、操作系统、服务器文件等数据要求每天进行定时自动备份。备份时间窗口设置在晚间，以避开业务高峰期，避免影响业务性能。

1. 备份申请

各信息系统的备份需求应统筹安排，系统项目经理根据实际情况提出备份需求，填写《信息系统备份申请表》（附件四12.4）提交备份系统管理员，备份系统管理员根据系统级别、数据量、备份窗等需求制定备份计划。

## 10.3 集团系统备份执行

1. 执行责任人

由备份系统管理员执行备份工作，负责制定灾备方案和运维管理。备份系统管理员负责汇总每日备份记录，检查备份系统运行情况，定期备份恢复演练，发现流程缺陷，持续优化灾备程序。对新上线系统提出合理化备份建议，监督实施。

1. 备份数据管理

建立备份档案库，详细记录备份数据的信息，重要备份数据应保留一年以上，备份应保存两份备份，一份本地机房存放，保证数据正常快速恢复，另一份异地保存，保证重大灾难后数据恢复。

## 10.4 集团备份检查及演练

1. 备份检查

备份系统管理员应定期检查备份结果，形成《备份检查记录表》（附件九12.9），如出现备份任务失败，应第一时间查看备份日志查找原因，进行分析解决。如同一备份作业连续两次任务失败，需形成分析报告上报基础架构负责人，升级事件处理级别。

1. 恢复演练

恢复作业需形成《备份恢复演练操作指引》，恢复作业应严格按照指引规范操作。

重要业务备份要求定期恢复验证，确保备份机制有效。恢复验证需进行详细记录，形成《备份恢复演练表》（附件五12.5），定期上报主管领导。

## 10.5 集团备份恢复

1. 恢复确认

进行恢复前，首先由备份系统管理员确认造成故障的原因，进行故障分析，确认需要进行恢复操作后，由相应系统项目经理提交《备份恢复申请表》（附件六12.6）进行故障说明。

1. 制定恢复计划

备份系统管理员在收到故障分析报告后与系统项目经理一起制定恢复计划，包括应恢复的内容、恢复的时间、恢复的操作步骤、恢复对应用造成的影响，最后形成书面恢复计划。备份系统管理员将故障分析报告与恢复计划一起提交IT主管领导审批。主管领导应确认恢复对生产造成的影响，在批准执行恢复前与相关业务部门进行沟通。

1. 恢复操作

在进行实际恢复前，备份系统管理员与系统项目经理确认无误后进入实际恢复操作，恢复前做相应的备份。进行恢复操作时应将每一步的执行过程进行记录，以备后用。

1. 恢复验证

完成恢复后，应测试恢复效果。测试恢复成功后进行相应备份。将执行恢复操作的参与人，恢复操作的时间、过程、完成情况形成书面报告，报IT主管领导审批。审批用过后恢复应用。

## 10.6 分公司数据备份

1. 目的

分公司原则上应提供数据存储和备份服务，为员工提供一定大小的存储空间，目的是方便员工工作文档的保存和恢复。

1. 申请和开通

需要保存数据的员工，应发送邮件申请给分公司IT团队，经分公司IT团队批准后开通。

1. 数据保存

备份数据应集中存储在分公司文件服务器上，对于员工保存在服务器上的数据应做严格的权限控制，确保只有员工本人可以访问自己的数据，以实现保密性。

1. 数据备份

针对员工存放的数据，原则上应定期做备份，并保留一定期限，确保员工需要时可以恢复数据。

# 11 网络管理

## 11.1 集团及分公司网络规划和架构设计

1. 设计要求

网络负责人应定期更新网络规划设计，保证整体网络的可靠性、安全性、以及可扩展性，使网络可以支持业务无中断运行和高性能服务，也可以满足日后发展需要。

网络设备应使用具有可维护性、可替换性的主流厂商产品，并且能够支持主流网络管理协议和工具。

1. 设备安装

除无线AP 外，所有网络设备要安装在机柜并做好固定。

通常情况下，网络设备要具备双电源模块，并机柜双路电源供电，以提高设备可靠性。

1. 网络架构调整

如需对网络架构做优化调整，需经基础架构负责人批准后方可执行。未经基础架构负责人批准，不得擅自进行更改网络架构的行为。如需对网络配置做重大修改，需要有执行预案，并将变更情况记录在《设备配置变更表》（附件三12.3）。

1. IP 地址规划

各分公司IP 地址段由集团统一分配使用，分公司不得擅自使用其它内部地址。

1. 维保要求

集团以及分公司所有使用中的网络设备应当购买原厂维保服务，确保硬件发生故障的时候，可以联系供应商处理。

紧急情况下，可以邀请供应商进行远程协助维护，但要在网络负责人的监督之下进行。

1. 设备退役

网络设备使用超过3年后，可根据设备情况做评估。如果不再适合继续使用，应迁移业务后将设备下架，按资产处理流程做相关回收处理。

## 11.2 集团及分公司网络工作分工

1. 集团基础架构团队网络工作主要职责

集团基础架构团队主要负责集团数据中心互联网，集团办公互联网的开通和管理；审批和协助分公司IT 团队开通专线业务；为分公司分配内部IP 地址段；维护和管理集团网络设备；指导分公司IT 团队进行网络建设。

1. 分公司IT 团队网络工作主要职责

分公司IT 团队主要负责分公司及项目办公互联网的开通和管理；分公司到集团的专线开通和维护；项目到分公司的VPN 链路建立和维护；管理和维护分公司及项目IP 地址的使用；管理分公司网络设备；接受集团基础架构团队的指导。

## 11.3 数据中心机房互联网出口

1. 链路

数据中心机房需要具备电信、联通互联网双线专线，并保证有足够带宽支持系统服务。使用负载均衡设备做出口链路负载均衡，以保障服务的访问效果。

1. IP 地址

确保每条互联网专线附带足够固定IP 地址，如需将内部应用发布到外网，应当由应用负责人向网络负责人提出申请，填写《外网IP及域名申请表》（附件十12.10）。审核通过后设置生效。

1. 域名

需要使用外网域名的，由系统负责人向网络负责人提出申请，填写《外网IP及域名申请表》（附件十12.10），审核通过后设置生效。

1. 安全

数据中心机房互联网出口，应使用防火墙防止外部攻击，提高网络安全性。

## 11.4 总部及分公司办公互联网出口

1. 链路

办公互联网要求使用电信或者联通的互联网专线，上下行带宽对称，并且使用固定IP地址。

1. 带宽

应按办公人数确定互联网专线带宽，并随时监控使用情况。带宽需要扩容时，网络负责人向基础架构负责人提出申请，批准后方可执行扩容。

1. 行为管理

应使用上网行为管理器规范员工上网行为，保障正常办公流量，禁止访问与工作内容无关的网站。禁止使用P2P等多线程下载工具。员工要求访问被禁止的网站或内容时候，应提出申请，由员工上级和网络负责人审核，通过后方可执行。

1. 安全

使用防火墙保护内网安全，防止外部攻击，提高内网安全性。

## 11.5 总部与分公司的网络连接

1. 链路

总部与分公司之间使用专线作为首要连接，同时要有备用连接，保障内网连接稳定可靠，出现问题可以及时恢复连接。

1. 带宽

分公司按人数确定专线带宽，并定期巡检带宽使用状态。发现带宽不足要及时扩容。

1. 开通和关闭

专线统一由各区域公司通过总部所在地一级运营商发起。区域及城市IT 团队负责申请业务，集团网络负责人协助开通业务。

分公司申请专线，当地区域或城市IT 团队需填写《网络专线申请表》（附件七12.7）交集团审核，通过后方可向运营商申请业务。

专线不再使用的，由分公司IT 团队向运营商申请拆除，同时通知总部做变更，释放专线资源。

## 11.6 项目网络连接

1. 互联网链路

项目可以使用电信或联通互联网专线提供上网服务，上下行对称带宽，并且使用固定IP 地址。带宽根据项目工作人数确认。

项目的互联网资源由项目所在地区域或城市IT 团队负责申请开通。

1. 项目与内网的连接

项目无需使用专线连接集团总部，应使用网络设备，通过IPSec VPN 链路连接到项目所在地分公司。

1. 安全

项目互联网专线要实现内网流量与外网流量分离，提高内网安全性。

项目售楼处需要给客户提供无线上网服务的，需要给客户划分出单独的Vlan 实现网络隔离。有条件的项目应使用独立的互联网线路及网络设备，与办公网络物理隔离。

## 11.7 无线网络规划

1. 设计要求

网络负责人进行无线规划，确保无线网络稳定、安全、可靠。

无线信号应确保全面覆盖办公区。还要考虑信道设置，信号强度，单个AP 负载等因素，保证无线网络服务质量。

基于安全及性能考虑，在要求高质量网络访问服务的情况下，推荐员工尽量使用有线网络。

1. 策略

无线网络应区分不同的用户和客户端。

用户分为内部用户与外部访客用户，不同用户采取不同策略。限制外部访客用户使用网络，保障内部用户正常办公使用。禁止外部访客访问内网资源，仅允许其访问外部网页服务。

内部用户分为PC 端用户和移动端用户，应对不同的客户端使用不同的安全策略和规则。原则上应限制移动端设备可以使用的外网服务及带宽，仅允许其访问与工作相关的服务。

1. 验证

外部访客来访使用的无线网络，应使用单独的访客账号或密码，该访客账号具有效期，过期失效。使用密码验证的访客网络，应定期修改密码。

内部无线网络使用的验证密码要对外保密，并定期修改。具备条件之后，应使用企业级802.1x方式，员工通过使用自己的域用户名和密码做连接验证。

1. 注意事项

任何员工未经批准，禁止私自连接无线网络设备到公司内网，以免影响公司无线网络的正常运行。一经发现，信息化部门可以要求员工拆除私自安装的设备。

应注意收集用户使用情况，及时解决用户反馈问题，定期安排巡检，排查无线网络中可能存在的问题。

无线网络是有线网络的补充和延伸，有线网络会影响到无线网络的使用状况，所以应保障有线网络的正常工作。

## 11.8 在公司外部访问信息的网络连接

1. 连接方式

员工在公司以外地点可以通过SSL VPN 连接内网进行办公。SSL VPN 应控制访问权限，保障内网安全性。

1. 员工使用要求

员工需使用本人电脑连接SSL VPN ，禁止在网吧等公共电脑上连接公司内网。员工本人电脑请使用正版操作系统并保持系统更新，安装杀毒软件并保持更新。

员工在公司外部访问内网资源时候，不要离开电脑。离开员工电脑屏幕前，请先关闭公司系统，并断开内网连接。

## 11.9 专用系统的特殊访问规定

1. 服务器安全

专用系统服务器应保证物理安全。服务器所在机柜平常应关闭机柜门并上锁，钥匙由基础设施负责人妥善保存。具体可以参照信息安全制度相关条款执行。

1. 通信安全

对专用系统的网络访问，需通过安全的通讯协议，例如https，IPSec 等，保证访问安全。具体可以参照信息安全制度相关条款执行。

1. 访问授权

专用系统不对普通用户开放网络访问。用户如需访问专用系统，需经过上级和系统负责人的批准。

# 12 附录

12.1 附件一：《机房人员进出登记表》

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 姓名 | 公司 | 证件号 | 联系电话 | 进入原因 | 日期 | 陪同员工 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

12.2 附件二：《机房巡检记录》

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 日期 | 时间 | 巡检人 | 机房温度 | 机房湿度 | UPS负载 | UPS状态 | 其它 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

12.3 附件三：《设备配置变更表》

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 日期 | 时间 | 申请人 | 操作人 | 设备 | 原配置 | 变更内容 | 结果 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

12.4 附件四： 《信息系统备份申请表》

|  |  |  |  |
| --- | --- | --- | --- |
| 申请人 |  | 申请日期 |  |
| 业务系统 |  | 开始日期 |  |
| 服务器 |  | | |
| 备份内容 |  | | |
| 备份周期 |  | | |
| 保存期 |  | | |
| 审核人 |  | | |

12.5 附件五：《备份恢复演练表》

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 |  | 执行人 |  |
| 目标服务器 |  | | |
| 来源服务器 |  | | |
| 恢复内容 |  | | |
| 恢复时间点 |  | | |
| 开始时间 |  | 结束时间 |  |
| 执行结果 |  | 验证人 |  |

12.6 附件六： 《备份恢复申请表》

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 |  | 申请人 |  |
| 业务系统 |  | 执行人 |  |
| 目标服务器 |  | | |
| 来源服务器 |  | | |
| 恢复内容 |  | | |
| 时间点 |  | | |
| 开始时间 |  | 完成时间 |  |
| 执行结果 |  | 验证人 |  |

12.7 附件七： 《网络专线申请表》

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 |  | 申请人 |  |
| 联系电话 |  | 邮件 |  |
| 城市 |  | 区域 |  |
| 办公人数 |  | 申请带宽 |  |
| 安装地址 |  | | |
| 集团审批意见 |  | | |
| 审批日期 |  |  |  |

12.8 附件八： 《服务器资产清单表》

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 设备名 | 厂商 | 型号 | 序列号 | 采购日期 | 维保到期日 | CPU | 内存 | 硬盘 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

12.9附件九： 《备份检查记录表》

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日期 | 巡视人 | 备份作业 | 完成状态 | 故障处理 | 备注 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

12.10 附件十： 《外网IP及域名申请表》

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 |  | 申请人 |  |
| 业务系统 |  | | |
| 服务器 |  | |  |
|  | |
| 内网IP |  | 内网端口 |  |
| 外网IP |  | 外网端口 |  |
| 域名 |  |  | |
| 审核人 |  | 验证人 |  |
|  |  |  |  |

12.11附件十一：《系统硬件需求提报单》

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 主 题 |  | | | | |
| 项目名称 |  | | | | |
| 项目负责人 |  | 基础架构对接人 | |  | |
| 项目背景  （项目组填写） | 备注：背景包括系统类型，用户数，访问形式，并发量，未来两年变化预期。 | | | | |
| 需求概要说明  （项目组填写） | 备注：需求包括服务器数量、角色、配置、拓扑；存储数量、IO；内外网需求；使用时间。 | | | | |
| 基础架构评估与意见 |  | | | | |
| 费用预估，采购形式 |  | | | | |
| 业务条线负责人 |  | | 信息化负责人 | |  |