**IDC机房管理制度**

**目录**

[一、 宗旨](#_Toc21700)

[二、 目标](#_Toc29498)

[三、 内容](#_Toc26887)

[1． IDC机房管理](#_Toc7487)

[2． IDC机房操作管理](#_Toc25644)

[3． IDC机房网络管理](#_Toc14168)

[4． IDC机房服务管理](#_Toc3568)

[5． IDC机房信息安全管理](#_Toc513)

[6． IDC机房资产管理](#_Toc17837)

[7． IDC机房应急管理](#_Toc17599)

[四、 处罚条例](#_Toc11323)

[五、 附录](#_Toc16091)

1. **宗旨**

为了规范蓝队网络公司IDC业务的日常运营和管理，提高公司IDC业务的运营水平和竞争力，更好地为蓝队网络已有客户提供快捷、高效、稳定的技术服务，同时彰显蓝队网络技术团队的整体技术和服务水平，以优质的服务质量和雄厚的技术保障为赢得更多潜在客户特制定本IDC机房管理制度。

1. **目标**

技术部所有员工必须严格遵守本管理制度，保证所有操作符合流程和操作手册的规定，做到“有章可循，有记录可查”以实现规范化操作和管理。

1. **内容**

IDC机房管理制度主要内容如下：

1. IDC机房管理
2. IDC机房操作管理
3. IDC机房网络管理
4. IDC机房服务管理
5. IDC机房信息安全管理
6. IDC机房资产管理
7. IDC机房应急管理

# IDC机房管理

1. 蓝队网络IDC机房为租赁昆明电信IDC机房，由昆明电信专人7\*24小时负责机房基础设施环境的管理和维护(包括温度、湿度、电力系统、空调系统、保洁卫生等)。
2. 进入IDC机房前，需先向昆明电信发送请求维护工单，经昆明电信相关负责人批准，到达值班中心后，需出示身份证件并填写登记表后方可进入。
3. 凡进入机房人员应遵守昆明电信IDC机房和蓝队网络IDC机房的管理制度；带客户进机房参观或进行维护操作时，客户需在蓝队网络工作人员的全程陪同下，进行参观或指导维护作业，未经许可客户不得擅自进入机房上机操作和对运行设备的各种配置进行更改。
4. 如因设备无法搬出维护，第三方人员或厂商必须进入机房维护的情况，需先向昆明电信申请并说明情况，遵照电信相关流程，待批准后发送维护请求工单方可作业。
5. 进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品。
6. 未发生故障或故障隐患时工作人员不可对中继、光纤等各类上行、下行链路及各种网络、系统设备进行任何调试；若有故障，应对所发生的故障、处理过程和结果等做好详细登记，并上报上级负责人。
7. 路由器、交换机和服务器以及存储是IDC业务的关键设备，人员离开现场时，需确保机柜门锁已上锁并处于关闭状态，未经部门负责人许可，任何人不得自行配置、变更或是移位操作。
8. 工作人员每次进入机房或保证每15天应对公司自有设备和客户设备进行运行状况日常巡检，如发现故障或异常情况应立即上报并详细记录，在上级负责人的指导下进行下一步操作和处理。

# IDC机房操作管理

1. 机器上架、搬出、维护等机器操作必须符合**《IDC机房操作指导手册》**的各项规定，以保证公司及客户的双方权利与义务。
2. 维护操作时，必须事先与客户沟通并确认问题后再进行操作，如操作有数据丢失的风险时（如系统重装、分区操作、数据删除等），务必先确保数据已经妥善备份成功再进行操作；如托管客户因遗忘系统登录密码而无法进入系统时，除非客户要求密码重置，且客户已提交工单，否则一律不得此类操作。
3. 如需对设备的硬件进行维护和更换操作，请确保设备已停机，所有电源已断开方能进行操作，以免导致数据丢失或是损坏设备而难以修复。

# IDC机房网络管理

1. 新网络设备上架，应由昆明电信分配管理标签，并粘贴于设备醒目位置。
2. 配置网络设备，确保本地控制口及远程连接口设置了强壮登录口令及验证方式。
3. 设备配置完成后，需保存配置输出并存档。
4. 更新现有网络拓扑图并确保实际网络连接线路与拓扑图保持一致。
5. 网络线路的连接，应根据链路类型不同采用不同颜色的连接介质进行区分，各类线路连接应确保美观、整齐有序，设备的源端及终端应采用统一命名规则并粘贴标签以便维护。
6. 网络设备及线路的增删、变更，需在公司管理后台添加相应记录。
7. 网络设备配置变更，需由网络管理员操作，其他人不得擅自操作或是更改，如变更影响到全局用户必须事先获得总经理的批准并提前发布维护通告，流程遵守**《维护通告流程图》。**
8. 网络管理员应开启设备日志功能并履行日志核查任务，如发现可疑登录行为或配置变更行为，须马上变更设备登录账号及口令。
9. 网络管理员应配置SNMP设备监控，以便监控平台对网络设备进行流量监控及分析
10. 如遇突发网络攻击，应借助网络分析工具快速锁定攻击源并进行IP封禁处理。

以上详细内容，请参考**《IDC机房网络管理规范》**

# IDC机房服务管理

1. 公司服务器日常维护主要涉及虚拟主机母机、数据库和云主机母机，应每天检查其运行状态并确保硬件及软件各项参数正常，以保证IDC业务的日常运营。
2. 所有客户服务内容必须有工单记录，形式不仅限于客户自行提交或后台提交。
3. 客户自行提交的工单，值班人员须在2分钟内进行工单回复以通知客户，您的工单请求已收到并正在处理中；对于营销QQ上的服务请求，值班人员须在30秒内响应客户并回复；对于24小时值班电话的来电，值班人员须在响铃3声内拿起话筒并接听。
4. 回复及沟通内容须采用敬语，回复规范请参考**《技术部服务标准用语规范》和《技术部快捷回复用语》。**
5. 虚拟主机、云主机、数据库、IDC服务租赁托管等相关服务规范请参考**《技术部IDC服务管理规范》。**
6. 24h值班人员，须做好工作交接，接班人员需提交10分钟到达接班地点，与当前值班人员就未完事宜进行工作交接，并在交接本上详细记录并签字确认。

# IDC机房信息安全管理

1. 公司自有设备系统帐号口令密码长度不得低于8个字符，且密码复杂性至少包含大写字母、小写字母、数字及特殊字符中的3种组合，并开启连续登录失败达到设定次数帐户锁定策略，不允许设置连续完整单词或是数字的简易密码；客户设备应引导客户设置高强度密码并增强安全意识。
2. 域管理系统应强制指定密码策略，包括但不仅限于密码的最短有效期、最长有效期、最短长度及复杂性。
3. 公司IDC核心业务设备，其密码至少应该保证每半年更换一次，包括：Linux系统root用户的密码、网络设备的Telnet和特权密码、Windows 系统Administrator用户的密码，以及应用系统的管理用户密码。
4. 公司员工不能将密码告诉除需处理IDC机房业务的本公司员工以外的人，如果系统密码已泄漏，必须立即更改。
5. 对于不同的业务管理人员，需设置不同权限的管理员帐号，不得共享同一个业务管理帐号，各系统应根据“最小授权”的原则设定帐户访问权限，控制用户仅满足当前工作需要，相关人员离职或是调岗后，应立即注销或是禁用相关人员帐号。
6. 各系统应设置审计用户的权限，包括但不仅限于登录成功、登录失败、注销、访问对象、系统日志记录。
7. 密码尽量采用加密方式保存，且密码尽量不以明文的方式通过未加密的电子邮件、QQ或者其它不安全的网络传输方式进行传输。
8. 所有业务系统服务器应当安装相应的病毒防护软件或采用了相应的病毒防护措施。
9. 应当确保防病毒软件每天进行病毒库自动更新，并设置定期（每周或每月）对全部硬盘进行病毒扫描。
10. 如果发现业务系统服务器已感染病毒，应先拔掉网线，根据病毒类型进行查杀，无法查杀及清除干净的病毒，需要格式化硬盘并重装系统后再重新接入业务系统网络。

# IDC机房资产管理

1. IDC机房资产管理的范围主要分为公司自有资产和客户租赁托管资产。
2. IDC机房资产管理的对象主要包括但不权限于服务器、存储设备、网络设备、PC、工作站、通信设备等。
3. 资产管理的流程主要分为新添加资产、资产变更、资产下架和资产报废四大流程。
4. 资产管理系统必须设置权限组，分配资产管理角色者相应的管理权限。
5. 资产管理系统的操作须由专门的资产管理组人员进行独立操作，其他人无权修改及删除操作，只有查询权限。
6. 公司自有资产或客户资产，上架前必须详细登记资产信息，包括但不权限于资产类型、资产型号、资产规格、数量、上架日期、电信流水号，所属机柜、机柜位置、客户用户名等信息，并核对是否与客户合同中提供的资产配置一致，如不一致，需与客户再次确认，并在合同中注明最后上架时的资产配置和数量。
7. 将所有资产信息录入公司资产管理系统，设定资产状态、上架日期、并分配资产使用或管理负责人。
8. 资产发生状态变更时，需及时更新资产管理系统，确保资产实时状态与资产管理系统中的记录一致。
9. IDC机房资产须每6个月进行资产盘点，核对所有资产是否与资产管理系统中的记录一致，如不一致，以最终盘点时的状态为准，更新资产管理系统并作备注说明。

# IDC机房应急管理

1. IDC机房应急管理主要覆盖蓝队网络当前IDC机房的所有业务，包括但不仅限于虚拟主机、云主机、服务器租赁托管、CDN、数据库、域名管理及各类宿主服务器及集群。
2. IDC机房应急机制分为一线技术支持和二线技术支持，根据事件类型，一般情况下处理原则应遵循先由一线技术工程师处理，如短时间内无法正常修复，应立即上报部门主管，将事件问题升级到二线技术支持，并详细汇报事件问题所呈现的故障现象及已经所做的操作和排错方法，以便二线技术工程师节省重复操作时间在最短的时间内进行修复。
3. 一线技术支持工程师应具备对所发生应急事件的快速判断能力，对于超出自己解决能力范围或是岗位职责范围外的事件，应立即上报部门主管，不得隐瞒不上报或是拖延上报以耽误事件解决时间，从而引发更大的故障或是灾难性事件。
4. 重大事件或是影响范围大的事件，应在第一时间排除故障后，尽快查明根本原因，详细分析并找出解决方案，要详细记录和总结并收录于事件管理文档。
5. 应急响应机制和紧急联系人，详情请参考**《蓝队网络应急处理紧急联系人》。**
6. **处罚条例**
7. 为了统一规范和管理IDC业务，就技术部服务标准及流程两部分建立相关处罚条例
8. 本条例目前正在逐步完善中，当前执行生效日期为**2016年6月1日**
9. 如有未尽相关事宜，将在以后补充完整，并讨论后发布重新
10. 具体相关规定，请参考**《技术部服务标准及流程处罚条例》**
11. **附录**
12. IDC机房服务管理流程



1. IDC机房操作指导手册



1. IDC机房网络管理流程



1. IDC机房资产登记及管理

*正在准备中。。。。*

1. IDC机房应急处理紧急联系人



1. 维护通告流程



1. 技术部服务用语及快捷回复规范



1. 技术部服务标准及流程处罚条例



1. 蓝队网络工单处理规范

