**中移在线服务有限公司**

**VPN帐号管理办法**

# 总则

1. 目的

为规范公司VPN帐号管理，有效预防和规避敏感信息泄露，保障系统安全运行，以及集团公司《中国移动帐号口令管理办法》，结合公司实际，特制定本办法。

1. 适用范围

本办法适用于在线服务公司各部门、各分公司（以下简称“各单位”）。

本办法适用于在线服务公司所有员工和合作伙伴人员。

本办法所指VPN帐号包括但不限于生产VPN帐号、办公VPN帐号、研发VPN帐号。

1. 原则
2. VPN帐号“谁申请、谁负责”、“谁使用、谁负责”；
3. VPN帐号分配需遵从“业务驱动”原则，即任何帐号的创建与权限的分配必须以业务需求驱动，严格禁止与业务活动无关的帐号或权限存在；
4. “可控”原则。所有VPN接入必须通过申请、审批、审计，保留申请记录，确保在安全可控的前提下实现VPN的远程接入；
5. 所有帐号均应落实责任人。

# 组织与责任

1. 各单位维护部门主管领导负责VPN帐号的审批、创建及删除、权限管理要求执行情况的审核机制，接受上级或者职能管理部门的定期审核。同时，应根据本单位部门设置、分工及维护模式等具体情况，明确指定审核责任人。
2. 各单位需按照VPN帐号审批流程申请所需帐号、修改权限或者撤销帐号。在帐号审批成功并创建后，应按照本办法要求严格保护帐号口令，不得泄露，否则需承担由此导致安全问题的责任。
3. 本部与分公司职责分工
4. 本部职责分工

1.贯彻落实国家及集团公司要求，制定VPN帐号管理办法；

2.明确VPN帐号管理工作的岗位及职责，制定VPN帐号管理制度；

3.负责规划、建设、运维本部VPN帐号及已纳入到本部管理的分公司VPN帐号工作，落实管理要求。

1. 分公司职责分工

1.明确VPN帐号管理工作的岗位及职责，落实VPN帐号管理要求。

2.依据VPN帐号管理办法，结合分公司实际情况，对未纳入本部管理的VPN帐号制定管理流程。

3.负责规划、建设、运维分公司VPN帐号管理工作，落实管理要求。

1. 岗位角色与职责分工：VPN帐号管理涉及的岗位及角色主要包括VPN帐号申请人、申请人直属负责人、申请人部门主管领导、VPN帐号支撑管理部门主管领导、VPN设备支撑管理部门运维负责人、VPN设备管理员，岗位及角色定义与管理职责分公司如下：
2. VPN帐号申请人员：帐号使用人员或代理申请人员

1.按照VPN帐号管理办法申请所需帐号，并在帐号创建成功后，及时进行各项权限验证，对帐号口令进行定期修改，并严格保护帐号口令，不得泄露，否则需承担由此导致安全问题的责任；

2.对持有的个人帐号安全负责，在申请、使用、过程中遵守安全要求；

3.及时发起VPN帐号回收、变更等申请，确保所填写的申请信息准确有效。

4.VPN帐号使用人在使用过程中发现问题应及时与VPN设备管理员联系。

1. 申请人直属负责人：需求合理性核对及帐号管理

1.按照VPN帐号管理办法核对申请人生产VPN、办公VPN、研发VPN帐号需求合理性进行审核；

2.定期组织核对离职人员信息，并组织发起帐号删除申请；

3.制定管理细则，做好VPN帐号使用人员的行为管理。

1. 申请人部门主管领导：负责本部门生产VPN帐号的审核与审批。
2. VPN帐号支撑归口管理部门主管领导:负责所管辖生产VPN帐号权限的审核与审批。
3. VPN设备支撑管理部门运维负责人：负责审核所管辖VPN帐号集中管理

1.落实部门主管领导要求，及时组织执行生产VPN帐号添加、删除、修改等申请。

2.负责所管辖办公VPN、研发VPN帐号权限的审核与审批。

3.制定VPN帐号集中管理办法，定期组织审查、核对。

1. VPN设备管理员：负责VPN设备的管理，VPN帐号添加、删除、修改等工作。

1.负责按照申请内容创建、变更或者删除VPN帐号。

2.分析VPN帐号的相关数据，包括登陆日志数据、接入状态等。

3.冻结存在安全风险的帐号。

# 用户管理

1. 在线服务公司员工应通过劳动合同等形式与本单位签订保密协议。
2. 第三方人员因对在线服务公司提供系统维护、调测、技术支持服务需要使用VPN帐号时，第三方公司应首先与本部或各分公司签订保密协议。保密协议应明确对第三方人员及归属单位提出执行本办法及《中国移动数据安全管理办法》相关要求。
3. 为便于审计和追查事故原因，要求第三方人员相对固定。

# VPN帐号管理

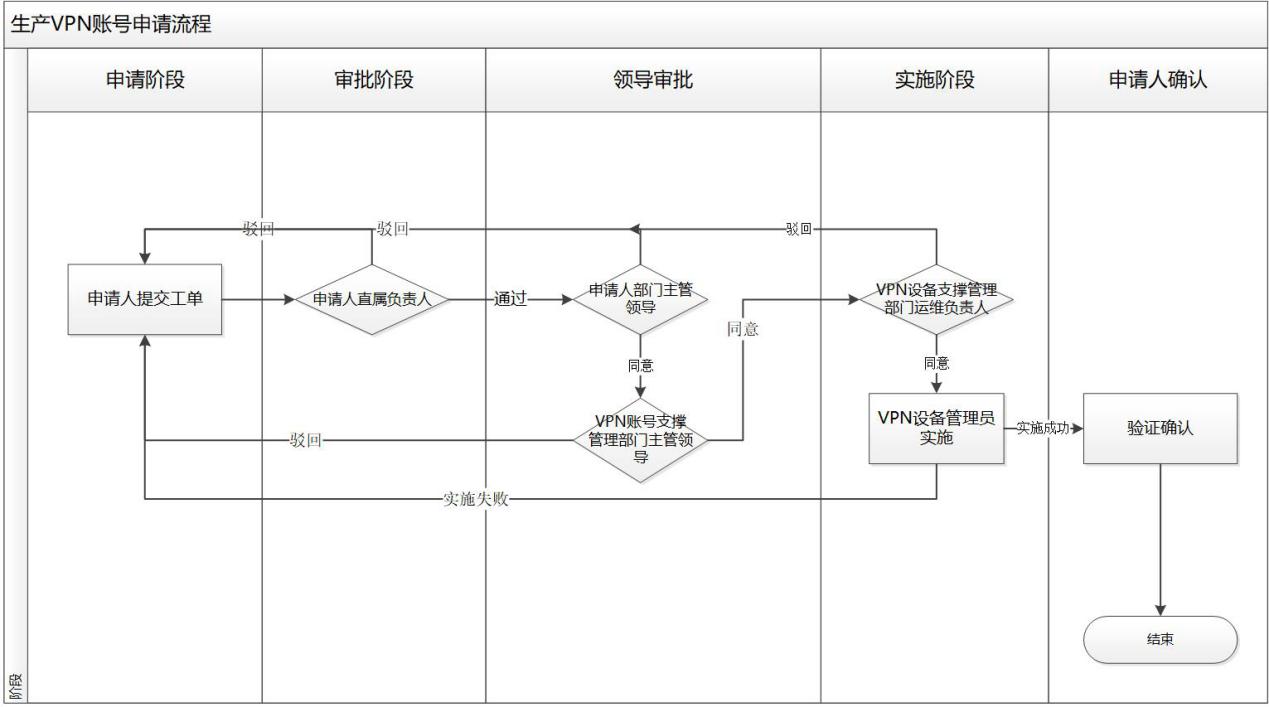
1. 帐号管理总体要求
2. VPN帐号支撑归口管理部门应指定专人负责帐号和权限的管理工作，明确所管辖系统的帐号权限申请审批流程，制定岗位角色和权限的匹配规范。
3. VPN帐号管理贯穿帐号创建、变更及帐号冻结全过程。
4. 应制定严格的审批和授权流程，规范帐号创建、变更、冻结等工作，授权审批记录应留档。
5. VPN帐号创建、变更和冻结申请审批通过后，应及时更新VPN设备中的帐号状态，确保与审批结论保持一致。
6. 对于第三方人员需使用VPN帐号访问涉及敏感信息系统的情况，应和第三方厂商签订相关的安全保密协议，以保证第三方厂商能够遵守在线服务公司的VPN帐号管理要求。对第三方用户帐号每季度进行检查，以保证第三方帐号得到有效控制，如发现过期或者未授权的访问帐号与权限应及时清除，以保证第三方帐号得到有效控制。
7. 禁止第三方人员拥有VPN设备管理员权限，禁止第三方人员拥有创建VPN帐号的权限，禁止第三方人员持有生产VPN帐号权限。
8. 特殊情况下，第三方人员若需要获得生产VPN帐号，需经部门主管领导/分公司主管领导临时授权，工作完成后及时收回权限。
9. 应对VPN帐号申请、回收、授权、有效期等环节进行严格管理，确保员工离职或岗位变动以及第三方人员发生离场时能及时清理或调整其VPN帐号。
10. VPN帐号有效期最长三个月，用户帐号到期后，按照帐号申请流程进行延期。
11. VPN客户端必须安装在在线服务公司配备的笔记本电脑，由资产责任人做好必要的安全防护措施。该电脑不得安装、使用与VPN相冲突的软件，确保运行安全。
12. 各单位应强化VPN安全配置，仅能通过生产VPN访问生产桌面云系统。通过研发VPN访问研发桌面云系统，通过办公VPN访问办公OA或研发云系统。
13. VPN帐号管理原则
14. “访问控制”原则：VPN帐号的创建与权限的分配由业务活动需求驱动，所有内外部用户必须与各自归属单位签署保密协议后方可为其创建帐号并授权，禁止任何未经正式授权的用户申请分配VPN帐号。
15. “帐号唯一性”原则：每个用户的帐号应是唯一的，必须明确每个帐号责任人，不得以部门或用户组作为最终责任人。
16. “权限最小化”原则：VPN帐号权限应根据该角色开展业务活动所需的最小权限进行设置，角色与权限的分配应明确使用者、使用期限等要素；帐号的角色权限分配应与用户的岗位职责及访问需求相匹配，避免不恰当的或超出范围的授权；所有帐号均应设置有效期限。

# VPN帐号口令管理

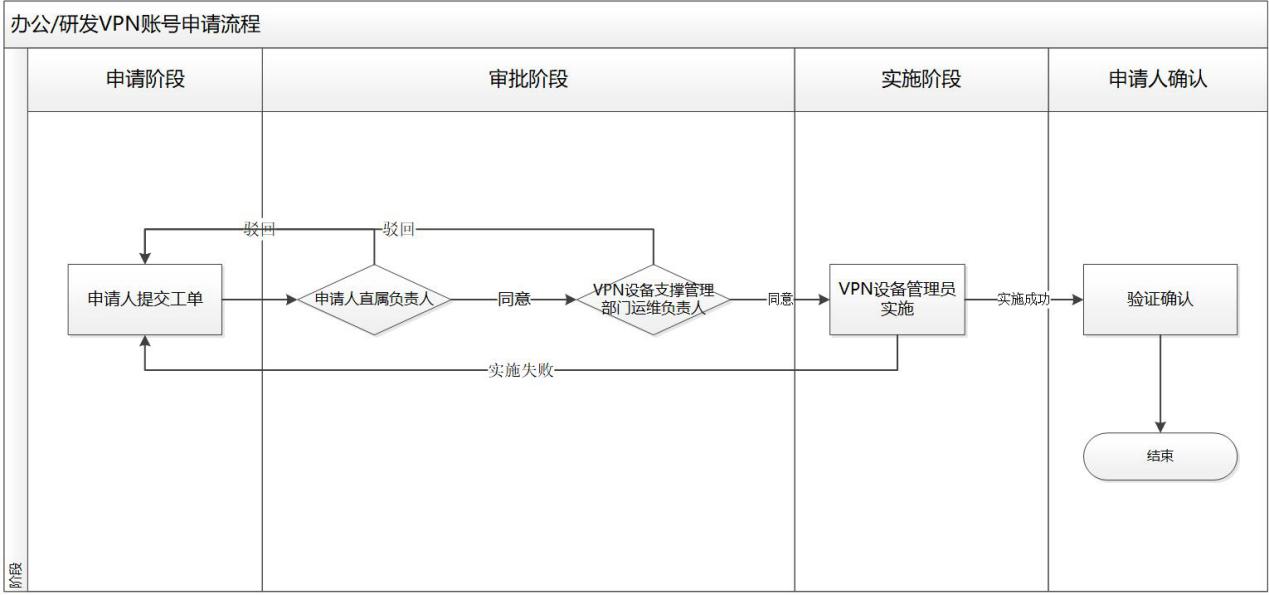
1. VPN帐号口令至少由8位及以上大小写字母、数字及特殊符号等混合、随机组成，尽量不要以姓名、电话号码以及出生日期等作为口令或者口令的组成部分，详细要求请参考《中移在线服务有限公司帐号口令管理办法》。

# VPN帐号申请流程

1. VPN超级帐号由VPN系统支撑归口管理部门主管领导以授权的方式授予具体的VPN设备管理员，应按照《附件二：系统/应用超级帐号授权表》进行授权授权。
2. 帐号权限的申请包括帐号创建、变更、删除，应通过研发云VPN帐号权限申请流程（研发云—>本部流程—>帐号权限管理流程）进行申请：
3. VPN帐号申请由用户所属部门主管领导以及系统支撑归口管理部门主管领导进行审批，重点检查所申请权限与申请人职责的一致性。VPN用户所属部门主管领导以及系统支撑归口管理部门主管领导审批职责可通过授权的方式授予指定人员，授权书至少应包括系统名称、超级帐号名、授予人姓名、职责描述、有效期等。
4. VPN设备管理员负责创建、变更或者删除帐号。
5. 员工工作调动或离职后，由系统管理员对其帐号进行删除或禁止使用处理。
6. VPN帐号申请包括VPN帐号权限申请、变更申请及删除申请，其流程共包含VPN帐号申请、VPN帐号审批、VPN帐号配置、VPN帐号确认四个环节，各VPN帐号申请流程如下：
7. 生产VPN：申请人—>申请人直属负责人—>申请人部门主管领导—>VPN帐号支撑管理部门主管领导—>VPN设备支撑管理部门运维负责人—>VPN设备管理员—>申请人



1. 办公VPN/研发VPN：申请人—>申请人直属负责人—> VPN设备支撑管理部门运维负责人—>VPN设备管理员—>申请人



# 审核管理

1. VPN帐号和权限的审核必须依据《中移在线服务有限公司帐号口令管理办法》。
2. 各单位应定期（至少每季度一次）以及业务流程发生重大变更时，对VPN系统的超级用户进行审核，并参照《中移在线服务有限公司帐号口令管理办法》中《附件四：系统用户帐号核查表》对不符合要求的及时进行整改。并由业务部门主管领导对超级用户的权限进行审阅签字，确保超级用户合理合规使用。
3. 各单位应定期（如每半年）以及业务流程发生重大变更时，由系统管理员导出系统普通用户帐号及访问权限清单，填写《附件四：系统用户帐号核查表》对不符合要求的及时进行整改。并组织相关部门对用户的权限进行审阅签字，以合理确保用户在系统中的权限与其职责相符。如果发现存在多余或不恰当的帐号、不相容职责（如应用层管理员应独立于操作系统层和数据库层管理员）或系统权限设定与用户职责不相符时，业务部门应及时通知系统管理员进行相应处理。
4. 各单位应定期对VPN帐号申请审批、权限变更等流程执行情况进行审核，避免违规创建VPN帐号、权限与职责不相容等情况的出现。

# 第七章 附则

1. 本管理办法自发布之日起执行。
2. 本管理办法由公司云平台部每年回顾一次，根据回顾结果修订本管理办法。
3. 本管理办法的解释权归在线服务公司所有。