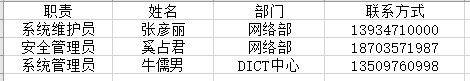
管理制度类：

1. 提供业务**公共安全影响程度**的报告。
2. 行业用户身份信息进行认证登记，应留存行业用户单位有效证件（**法人证书、经营许可证**等）、**责任人和经办人有效证件**、**责任人和经办人委托授权书**以及经办人办理业务时的现场照片。
3. 提供合作企业的安全保障能力进行评估，确保其信息安全管理工作及保障措施可以满足相关法律法规要求，可以保障应用的信息安全。补充**背景资质审查材料**、**数据安全协议**等）
4. 补充提供对5G行业应用建立安全人员配置制度并配备相应的安全人员，提供安全人员配置清单，明确各个角色的责任和权限。在内部人员发生变动（如换岗、离职）后，应及时对其相应权限进行变更、删除**（补充提供项目相关人员名单）**



1. 企业应记录和保存5G行业应用相关基本配置信息及更新情况，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。**（补充系统配置参数如、基站和OMC版本更新升级记录、基站和OMC等的版本号）**
2. 企业应针对5G行业应用制定不同事件的应急预案并建设应急处置能力，配套应急管理小组及相关资源保障，定期进行应急预案培训和演练，及时报告所发现的安全弱点和可疑事件，分析和鉴定事件产生的原因，做好记录并总结经验教训。**（补充应急演练报告、节前演练记录等）**
3. 企业应针对5G行业应用相关管理/运维系统，建立账号权限管理机制，指定专门的部门或人员进行账号管理，对申请账号、建立账号、删除账号等进行控制。（**提供相关流程工单记录等）**

数通命令截图：

1、5G专网应支持最小边界访问策略配置，仅允许必要的外部行业网络进行访问，默认禁止所有通信，不存在无效和多余的控制规则。

登录**防火墙查看访问策略配置**并提供完整截图，说明是否默认禁止，以及每条策略的功能和必要性。

2、说明5G专网与公网之间是否根据组网情况进行物理或逻辑安全隔离。

登录DCGW和防火墙查看组网配置，提供**VLAN和VPN配置截图**，说明是否利用划分不同VLAN和GRE隧道，对专网和公网进行隔离。

合作方材料：

1、中兴CPE终端说明文档，包括是否具备5G功能的终端和为行业终端提供接入服务的5G接入网关设备，应支持3GPP标准的认证机制，建议终端选择配备二次认证、安全芯片、GBA认证或AKMA认证机制。是否支持3GPP标准中要求的机密性和完整性保护算法，例如：128-NEA1,128-NEA2,128-NEA3,128-NIA1,128-NIA2和128-NIA3。

2、PAI平台的功能点截图：

