中共四川省委组织部
中共四川省委网络安全和信息化委员会办公室 文件

川组通〔2020〕16号

中共四川省委组织部
中共四川省委网络安全和信息化委员会办公室
关于印发《四川省党员和干部基本信息网络安全管理暂行办法》的通知

各市（州）、县（市、区）党委组织部，省委各部委、省直各部门组织人事部门，省属高等学校、科研单位党委（党组），国有重要骨干企业党委：

为贯彻落实中央、省委有关信息化发展战略部署，全面提升我省组织系统信息化水平，根据工作实际，我们研究制定了《四川省党员和干部基本信息网络安全管理暂行办法》，现印

发给你们，请结合实际认真抓好贯彻落实。

中共四川省委组织部　　中共四川省委网络安全和信息化委员会办公室

2020年 5月 21日

四川省党员和干部基本信息网络安全管理暂行办法

第一章　总 则

第一条 为保障全省党员、干部基本信息网络安全，保护党员、干部和各级组织人事部门的合法权益，规范党员、干部基本信息网络管理，提高网络安全管理水平，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 本办法所称党员、干部基本信息，是指党员、干部的证件号码、家庭住址、家庭成员、出生日期、指纹信息等与个人直接相关并专属个人的特有信息，以及能由此反映组织结构和层级关系详情的相关信息。

第三条 各级组织人事部门在职权范围内，通过网络方式（包括互联网、涉密内网、局域网、虚拟专网等）采集、管理和使用党员、干部基本信息，开发、建设和运维与党员、干部基本信息有关的信息化应用等，适用本办法。

第四条 党员、干部基本信息网络安全遵循“谁管理、谁负责”的原则，各级组织人事部门在职责范围内负责对所管辖的党员、干部的基本信息进行管理，对其基本信息网络安全负有责

任。

第五条 各级组织人事部门根据党员、干部管理权限，通过网络等信息化手段管理和维护管辖范围内党员、干部的基本信息，其他任何个人或单位未经授权，不得开展相关信息化应用的开发、使用和运维。

第二章　采集、传输、查询和存储

第六条 各级组织人事部门根据工作需要，严格按照有关标准及规范，准确、完整、及时地采集和更新党员、干部基本信息，确保基本信息采集安全可控。

第七条 通过网络方式采集党员、干部基本信息的，应保证网络环境达到相应的安全级别，并采取相应的安全加密措施。

第八条 基本信息采集须明确采集信息的目的、方式和范围，不得超范围过度采集，采集到的基本信息不得以任何形式向超出管理权限或未经授权的个人或单位提供。

第九条 重要敏感信息，包括反映组织结构和层级关系的详细信息，党员领导干部不宜公开的党内职务、证件号码、家庭住址等敏感信息，不得通过互联网等非涉密网络采集、传输和存储。

第十条 对基本信息进行批量操作，如批量修改、传输、复制、下载等，应设置内部审批流程，按最小授权原则授予完成

职责所需的最少数据操作权限。

第十一条 党员、干部基本信息原则上不得公开，如法律法规要求公开的，公开内容应严格按规定执行，应充分重视风险。

第十二条 更换、废弃存储过基本信息的信息化设备，应将之前的内容全部删除，并采取措施防止通过技术手段恢复。

第十三条 管理、使用和运行党员、干部基本信息，特别是敏感信息和重要数据的信息化应用，不得部署或托管在商业性网站或第三方技术服务公司。

第十四条 因工作需要对基本信息进行共享、查询和数据交换时，应严格限定在对方管理权限范围内，对双方数据安全进行评估，并采取相应安全保障措施。

第三章　基本信息相关信息化应用

第十五条 通过网络等信息化技术手段对党员、干部基本信息进行管理，必须遵循国家和中央组织部有关保密和信息安全相关规定，做好系统安全设计，强化安全防护技术手段。

第十六条 与党员、干部基本信息相关的信息化应用的开发建设，应选择国家认可的具有相应资质的单位，按国家保密法律法规要求实施，委托合同中载明基本信息保护责任条款，并签订保密协议，开展安全教育，严防信息泄露。

第十七条 信息化应用部署运行前应由具有相应资质的专

业检测机构进行系统检测，开展安全评估，出具安全性能测试报告。定期进行系统加固、补丁升级、漏洞修复、病毒查杀等安全维护工作。

第十八条 党员、干部基本信息有关的信息化应用，应当具有用户管理、权限管理、日志审计等安全功能，不得留有后门程序或者绕过安全机制，软件源代码留存备案。

第十九条 未经组织部门批准，任何单位和个人不得建立与党员、干部基本信息系统的联接，不得将党员、干部基本信息有关的信息化应用延伸到未建立党组织的单位。

第二十条 不得越权使用、调用和访问党员、干部基本信息有关信息化应用的数据资源，不得超出管理权限和层级开展党员、干部基本信息的统计分析或学术研究。

第二十一条 任何个人和组织不得扫描、探测、入侵党员、干部基本信息有关的信息化应用，不得篡改相关数据资源和有关审计信息。

第二十二条 应做好党员、干部基本信息相关信息化应用的数据备份和存档，保留真实、完整、可追溯的安全审计日志。

第二十三条 信息化应用的用户应当配合相关部门进行安全检查和事故调查，不得蓄意干扰、屏蔽、卸载、拆除有关安全监控程序或监测设备。

第二十四条 信息化应用承建单位、运维单位、技术服务单

位及相关人员，不得违规携带、备份或操作有关基本信息，组织部门应对其操作行为进行监督。

第二十五条 对党员、干部基本信息系统开展攻防安全演练测试，应报上一级组织部门同意后方可实施，跨单位、跨区域开展的安全攻防测试演练，由中共四川省委组织部统一安排实施。

第四章　管理职责

第二十六条 各级组织人事部门对管辖范围内党员、干部的基本信息进行采集、管理、使用、公开等过程中，应严格按照有关规定执行，强化基本信息日常管理监督，增强技术防护手段。

第二十七条 各级组织人事部门负责对管理和使用党员、干部基本信息的各类组织和相关人员进行管理，开展身份合法性核查，对信息安全、使用范围、管理手段等进行审查。

第二十八条 中共四川省委组织部统一制定党员、干部基本信息网络安全管理规划、技术规范等，提供全省性基本信息网络安全管理基础保障。

第二十九条 信息化应用的建设和管理严格执行《中共四川省委组织部关于规范全省组织系统信息化项目建设和管理的指导意见》（川组通〔2019〕31号）有关要求，各级组织人事部

门信息化工作职能处（科）室对基本信息网络安全等定期进行检测、抽查。

第三十条 各级组织人事部门通过信息化手段管理和使用党员、干部基本信息时，应充分征求网信、保密、公安等相关部门意见，对系统进行定密、定级。

第五章　保障措施

第三十一条 各级组织人事部门建设党员、干部基本信息有关的信息化应用时，应同步规划网络安全建设措施，保证网络安全经费投入，强化安全防护设施建设。

第三十二条 各级组织人事部门应当将党员、干部基本信息网络安全管理工作落实到具体处（科）室，指定专人负责。

第三十三条 安全检测发现严重网络安全隐患的，应立即停止运行，检测结果做好记录存档，整改合格后方可继续运行。安全检查及整改情况纳入信息化工作目标考核。

第三十四条 发生危害国家安全、重要信息泄露、关键系统瘫痪、遭受严重网络攻击及其他妨碍组织工作业务正常开展，产生严重负面影响的网络安全事件，应立即采取处置措施，并上报中共四川省委组织部。

第三十五条 违反本办法、造成严重后果的，追究当事人和有关领导的责任；造成泄密或者存在严重保密违法违规行为的，

予以处分；构成犯罪的，移送司法机关依法追究刑事责任。

第六章　附 则

第三十六条 各级组织人事部门要根据本办法，结合本地实际，认真抓好贯彻落实。

第三十七条 本办法自印发之日起执行，由中共四川省委组织部负责解释。

中共四川省委组织部办公室　　2020年 5月 21日印发