中共乐山市委网络安全和信息化委员会办公室个人信息管理操作规程（试行）

第一章 总则

第一条 为规范中共乐山市委网络安全和信息化委员会办公室（以下简称网信办）个人信息的处置，明确信息化建设中对个人信息保护的管理要求，避免信息保护不当导致本部门及下属（驻场）单位、个人合法权益受损，按照《中华人民共和国个人信息保护法》、《中华人民共和国网络安全法》、《中华人民共和国刑法》等法律法规要求，特制定本规程。

第二条 本规范适用于网信办（含下属事业单位）的信息化建设中所涉及的个人信息采集、存储、使用、共享、开放、删除以及信息发布等环节。

第三条 根据国家法律法规和国家标准，本规范中个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于如下信息：姓名、出生日期、身份证件号码、个人生物识别信息、银行账号、住址、个人通信通讯联系方式、通信记录和内容、账号密码、财产信息等。

个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，包括但不限于如下信息：

身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、交易信息、14岁以下（含）儿童的个人信息等。

第四条 信息化建设中的个人信息保护应遵循如下原则：

（1）合法原则：不得违反相关法律、法规的规定；

（2）安全原则：信息化建设中应采用必要的安全技术措施和管理手段，保障个人信息的完整性、保密性及安全性，避免涉密的数据资源泄露、损毁和丢失。

（3）最小必要原则：以实现处理目的所必要的最小范围、采取对个人权益影响最小的方式处理个人数据。

（4）知情同意原则：对个人信息的收集利用，必须经过本人充分知情前提下的同意

第五条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第二章 个人信息管理

第六条 个人信息管理包含采集、存储、使用、共享、公开、删除、检查等工作。

第七条 个人信息采集应满足以下要求：

（1）信息化项目建设及日常办公中所需的个人信息采集，由采集数据的主管科室负责，其他业务科室、信息化项目不允许单独进行个人信息采集。

（2）个人信息主管科室应对采集的个人信息进行审核和及时更新，确保个人信息的准确性和完整性。职工如发生变更或采集的数据有误，应及时向该信息主管科室提出更新申请，主管科室应提供方便、快捷的信息更新渠道，保证及时更新个人信息。

第八条 个人信息存储应满足以下要求:

（1）在信息化项目建设及日常办公中，政数通平台是个人信息集中统一的存储平台。个人信息主管科室采集到的个人信息，除存储在相关的业务系统数据库中，还应通过数据交换平台，交换到政数通平台。

（2）原则上信息化项目建设中的个人信息均需要在政务云服务器存储，不得在其它公有云环境中存储。

（3）个人信息在存储和传输过程中必须进行加密处理，采取有效技术手段和管理措施保护存储个人信息的终端设备，避免个人信息的泄露、损坏或丢失。

第九条 个人信息使用应满足以下要求：

（1）本单位信息化项目建设中，各科室及下属单位信息化项目在使用个人信息时应严格遵循前款所述的合法原则、最小必要原则、安全原则和知情同意原则。

（2）各信息化项目应严格按照数据资源使用申请中所确定的用途使用个人信息，严禁将个人信息挪作他用。

（3）因信息化建设工作需要，可接触到个人信息的相关人员，对相关个人信息负有保密责任，严禁未经授权对外提供个人信息。

（4）各信息化项目中，对于个人信息的查询、修改等操作应保留不少于180天的最新操作日志，并提供审计功能，可审计对个人信息的各类操作。

（5）除个人信息的源数据系统，其他业务系统原则上禁止提供单独针对个人信息数据的批量导出功能。

（6）对个人信息的重要操作前（如批量修改、拷贝、导出等），需由相关数据主管科室负责人报分管领导审批通过后方可进行操作。

（7）各信息化项目应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化处理。

（8）本单位信息化建设中，依照本规程获取的个人信息，经过匿名化处理后无法识别特定个人且不能复原的，可直接应用于日常办公中。

（9）单位内部其他业务系统或线下业务工作需使用内部职工及驻场人员个人信息时需充分评估合法性、必要性和安全性。

第十条 个人信息共享应满足以下要求：

对于非信息化工作中的个人信息查询，原则上只接受公安部门以及上级主管部门依法依规的查询请求，查询请求受理部门为相关个人信息数据主管科室，其他业务科室不得接受查询请求,也不得进行个人信息查询和提供个人信息数据。

第十一条 个人信息公开应满足以下要求：

（1）在日常办公中只有相关法律法规有明确规定需要公示的个人信息，才可进行公开。

（2） 公开个人信息遵循最小化原则，严禁超范围公开其他相关信息，相关个人信息需进行去标识化处理，不得直接公开完整的个人信息。

（3）对于前款所述的个人敏感信息不宜公开。

（4）不得在互联网上（QQ、微信、云盘、钉钉等）发布、传递包含单位职工及驻场人员个人隐私（如身份证号、手机号、家庭住址、准考证号等）的文件及信息。

第十二条 个人信息删除应满足以下要求：

注销的、废止的存储设备或信息化系统要确保承载的个人信息已被清理才可进行注销或报废处理。对于违反法律法规及本规程采集、存储的个人信息，应依法依规删除相关个人信息数据。

第十三条 个人信息检查及安全教育

（1）数据科依照本规程对各信息化项目中个人信息处置相关的审计记录进行检查，或者通过其他网络安全检测手段检查个人信息的采集、存储、使用及处理情况。

（2）对于出现的违规行为将按照网络安全事件进行处置，单位相关科室及个人应按照本办法及相关整改通知，及时、彻底的整改相关问题。

（3）网安科要围绕个人信息安全，定期组织开展数据安全教育、技术培训。

第三章 信息发布管理

第十四条 网信办信息发布工作需严格遵循个人信息管理要求。

第十五条 信息发布审核机制：

信息发布必须严格按照“三审”制度执行，首先由信息员发布信息，然后经审核员审核通过后，再由审发员审发后才能在网站上公开。

审发机制应通过账号管理来严格区分，严禁采用同一账号设立全部权限，“初审”、“审核”、“审发”必须落实对应的责任人。

第十六条 信息发布内容要求：

信息员、审核员和审发员对发布内容进行审核，严格遵守“九不准”，凡含有下列内容的，一律不准发布：

（一）反对宪法基本原则的。

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

（三）损害国家荣誉和利益的。

（四）煽动民族仇恨、民族歧视，破坏民族团结的。

（五）破坏国家宗教政策，宣扬邪教和封建迷信活动的。

（六）散布谣言，扰乱社会秩序，破坏社会稳定的。

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

（八）侮辱或者诽谤他人，侵害他人权益的。

（九）含有法律法规禁止的其他内容的。

第十七条 网站发布信息由信息发布人员统一做好登记。

第四章 人员管理

第二十一条 所有信息系统相关岗位人员，在上岗前均要签署保密协议（包括在岗期间的保密责任和离岗期间的保密责任），关键岗位人员必须从内部人员中选拔。

第二十二条 人员调离的，必须立即更换或归还之前发放的身份证件、钥匙，单位提供的软硬件设备及文档资料等资产，并办理详尽的交接手续。必须立即终止其所有的访问权限，涉及相关信息系统账号、口令时，先采取更换密码或冻结账号的措施，避免直接删除账号。必须签署保密承诺书，承诺在调（离）岗后根据保密承诺书的内容履行相关的保密责任和义务，涉密人员实行脱密期管理制度。

第二十三条 个人信息数据接触者应满足以下要求：

（1）对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限。

（2）对个人信息数据资源的重要操作设置内部审批流程，如批量修改、拷贝、下载等。

（3）对特定人员超限制处理个人信息数据资源时，由业务主管科室配置相应的责任人进行审批，并对这种行为进行记录。

第五章 责任认定及追责

第二十四条 个人信息数据资源涉及的平台原则上按照等级保护第三级实施安全保护，建立数据分类分级的安全保证机制，监督检查数据安全策略的执行情况属于平台方的责任和义务。

第二十五条 个人信息资源提供方应主动管理并基于权属关系对数据安全使用提出约束要求。

第二十六条 个人信息资源需求方应履行数据安全使用约束要求，遵循“最小化授权使用”原则严格按照约定的方式和使用范围使用共享数据，建立必要的“数据防泄漏机制”和“数据溯源机制”，数据提供方应知道到数据流向和使用主题，以便日后数据追责。

第六章 附则

第二十七条 法律、法规、规章对个人信息保护已有规定的，从其规定；没有规定的，参照本规范执行。

第二十八条 本规程自印发之日起试行。