中共乐山市委网络安全和信息化委员会办公室

个人信息内部管理制度（试行）

**目** **录**

1 范围 [2](#_bookmark2)

2 规范性引用文件 [2](#_bookmark3)

3 术语和定义 [2](#_bookmark4)

4 管理机制 4

1. 应急处置 5
2. 自查整改 7
3. 监督检查 8
4. 责任追究 8

为规范市委网信办及下属事业单位在日常办公中有关个人信息处置、信息化项目建设及办公文件编撰、印发、流转等流程，避免个人信息处置不当造成职工及其他工作人员利益受损，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，根据国标《GB/T 35273—2017信息安全技术个人信息安全规范》及公安部《互联网个人信息安全保护指南》意见，特制定本制度。

**1 范围**

本制度适用于网信办及下属事业单位信息化项目建设及日常办公中所涉及的个人信息采集、存储、使用、共享、公开及删除等各环节的个人信息保护。非信息化手段采集的数据可参考本办法执行。

**2 规范性引用文件**

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 35273—2017 信息安全技术个人信息安全规范

GB/T 25069-2010 信息安全技术术语

GB/T 22239 信息安全技术网络安全等级保护基本要求

**3 术语和定义**

3.1 个人信息

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、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、成绩信息等。

3.2 个人敏感信息

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、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

3.3 个人信息所有者

个人信息所标识的自然人。

3.4 个人信息持有

对个人信息及相关资源、环境、管理体系等进行计划、组织、协调、控制的相关活动或行为。

3.5 个人信息持有者

对个人信息进行控制和处理的组织或个人。

3.6 个人信息收集

获得对个人信息的控制权的行为，包括由个人信息主体主动 提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。

3.7 个人信息使用

通过自动或非自动方式对个人信息进行操作，例如记录、组 织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。

3.8 个人信息删除

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.9 个人信息生命周期

包括个人信息持有者收集、保存、应用、委托处理、共享、转让和公开披露、删除个人信息在内的全部生命历程。

**4 管理机制**

4.1 管理机构

网信办信息化项目建设及日常办公过程中个人信息保护工作由数据管理和应用科统筹协调，市大数据中心负责技术指导，各科室及下属单位负责具体落实本科室、本单位信息化项目建设及日常办公过程中的个人信息安全保护工作。

4.2 个人信息所有者权利

网信办及下属单位职工作为其个人信息所有者，有权查询本人的个人信息，有权更正错误的个人信息，有权对信息化建设中违规处置个人信息的行为进行反馈和报告。对于各信息化项目中的违规行为可以向项目主管科室反馈，主管科室应予以及时处理并反馈处理结果。

4.3 个人信息所有者义务

网信办及下属单位职工作为个人信息的所有者，有义务及时更新信息化建设中使用到的个人信息，保证信息的准确性和完整性，并在信息化应用过程中妥善保管个人信息。由于个人原因造成的个人信息泄露、损坏、丢失，由本人承担相应责任；如对他人个人信息造成不良影响，将根据有关追责条款，追究相关责任人的责任。

4.4 个人信息安全保障

根据“谁主管谁负责、谁批准谁负责、谁使用谁负责”的原则，不得将个人信息用于商业用途。信息发布使用前必须先经过脱敏处理，不得直接公开完整的个人信息。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办法采集、存储的个人信息，应依法依规删除相关个人信息数据。

**5 应急处置**

5.1 应急机制和预案

(a) 应制定个人信息安全事件应急预案，包括应急处理流程、事件上报流程等内容；

(b) 应定期组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程，留存应急培训和应急演练记录；

(c) 应定期对原有的应急预案重新评估，修订完善。

5.2 处置和响应

(a) 发现个人信息安全风险时，应及时采取措施，进行整改并消除隐患；

(b) 发生个人信息安全事件后，应记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

(c) 应对安全事件造成的影响进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大；

(d) 应将事件的情况告知受影响的个人信息主体，并及时向社会发布与公众有关的警示信息。

**6 自查整改**

6.1 个人信息收集与对外共享情况排查

按照“谁发动采集、谁负责排查”、“谁共享数据、谁负责排查”的原则，各科室、下属单位定期开展个人信息收集与对外共享情况排查工作，做到底数清、去向明。

6.2 存在问题的整改与落实

对于自查中发现的问题需要及时整改，认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，尽力杜绝类似事件再次发生。

**7 监督检查**

数据科负责各科室、下属单位个人信息保护工作落实情况的监督检查，建立健全个人信息安全监督检查机制，及时发现问题并督促进行相应整改。

**8 责任追究**

对于各科室、下属单位所采集、共享的个人信息数据，实行科室责任人安全周期负责制度。在监督检查中发现问题，若在收到问题整改通知后，整改不力的，科室负责人为第一责任人，由市委网信办给予通报批评；造成重大损失或严重安全后果，移交上级执法部门进行追责处罚。对于违反国家法律法规的行为，将配合公安、国安等主管部门进行处理。