互联网个人信息安全保护指引

Guideline for Internet personal information security protection

（征求意见稿）

目　　次

目　　次.....II
引　　言.....III
1 范围.....1
2 规范性引用文件.....1
3 术语和定义.....1
4 管理机制.....2
4.1 管理制度.....2
4.2 管理机构.....3
4.3 管理人员.....3
5 技术措施.....4
5.1 基本要求.....4
5.2 增强要求.....8
6 业务流程.....8
6.1 收集.....8
6.2 保存.....8
6.3 应用.....9
6.4 删除.....9
6.5 第三方委托处理.....9
6.6 共享和转让.....9
6.7 公开披露.....10
6.8 应急处置.....10

引　　言

为指导互联网企业建立健全公民个人信息安全保护管理制度和技术措施，有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会、北京邮电大学和公安部第三研究所相关专家，研究起草了《互联网个人信息安全保护指引（征求意见稿）》。

对指引中的具体事项，法律法规另有规定的，需遵照其规定执行。

个人信息安全保护指引

1 范围

本指引规定了个人信息安全保护的安全管理机制、安全技术措施和业务流程的安全。

本指引适用于指导个人信息持有者在个人信息生命周期处理过程中开展安全保护工作，也适用于网络安全监管职能部门依法进行个人信息保护监督检查时参考使用。

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 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 35273—2017 信息安全技术 个人信息安全规范

3 术语和定义

3.1

个人信息 personal information

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。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、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、交易信息等。

[GB/T 35273-2017，定义 3.1]

3.2

个人信息主体 personal data subject

个人信息所标识的自然人。

[GB/T 35273-2017，定义 3.3]

3.3

个人信息生命周期 personal information life cycle

包括个人信息主体收集、保存、使用、委托处理、共享、转让和公开披露、销毁个人信息在内的全部生命历程。

3.4

个人信息持有者 personal information holder

对个人信息进行控制和处理的组织或个人。

3.5

个人信息持有　personal information hold

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。

3.6

个人信息收集 collection of personal information

个人信息持有者获取个人信息的行为

3.7

个人信息使用 usage of personal information

通过自动或非自动方式对个人信息进行操作，例如收集、记录、组织、排列、存储、改编或变更、检索、咨询、使用、披露、传播、保护或以其他方式提供、调整或组合、限制、删除或销毁等。

3.8

个人信息删除 removal of personal information

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。
[GB/T 35273-2017，定义 3.9]

4　管理机制

4.1　管理制度

4.1.1　管理制度内容

a) 应制定个人信息保护的总体方针和安全策略等相关规章制度和文件，其中包括本机构的个人信息保护工作的目标、范围、原则和安全框架等相关说明；
a) 应制定个人信息的保护管理制度，其中包括个人信息生命周期的工作内容；
b) 应制定工作人员对个人信息日常管理的操作规程；
c) 应建立个人信息管理制度体系，其中包括安全策略、管理制度、操作规程和记录表单；
d) 应制定个人信息安全事件应急预案。

4.1.2　管理制度制定发布

a) 应指定专门的部门或人员负责安全管理制度的制定；
b) 应明确安全管理制度的制定程序和发布方式，对制定的安全管理制度进行论证和审定，并形成论证和评审记录；
c) 应明确管理制度的发布范围，并对发文及确认情况进行登记记录。

4.1.3　管理制度执行落实

a) 应对相关制度执行情况进行审批登记；
b) 应保存记录文件，确保实际工作流程与相关的管理制度内容相同；

c） 应定期汇报总结管理制度执行情况。

4.1.4 管理制度评审改进

a） 应定期对安全管理制度进行评审，存在不足或需要改进的予以修订；应定期对安全管理制度进行评审，发现存在不足或需要改进应及时进行修订；
b） 安全管理制度评审应形成记录，如果对制度做过修订，应更新所有下发的相关安全管理制度。

4.2 管理机构

4.2.1 管理机构的岗位设置

a） 应设置指导和管理个人信息保护工作机构，明确定义各个机构的职责；
b） 最高管理者或最高管理者应设置专门岗位从事个人信息保护的工作；
c） 应明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员和安全管理员等各个岗位，清晰、明确定义其职责范围。

4.2.2 管理机构的人员配置

a） 应明确安全管理岗位人员的配备，包括数量、专职还是兼职情况等；配备负责数据保护的专门人员；
b） 应建立安全管理岗位人员信息表，登记机房管理员、系统管理员、数据库管理员、网络管理员、安全管理员等重要岗位人员的信息，安全管理员不应兼任网络管理员、系统管理员、数据库管理员等岗位。

4.3 管理人员

4.3.1 管理人员的录用

a） 应设立专门的部门或人员负责人员的录用工作；
b） 应明确人员录用时对人员的条件要求，对被录用人的身份、背景和专业资格进行审查，对技术人员的技术技能进行考核；
c） 录用后应签署相应的针对个人信息的保密协议。
d） 应建立管理文档，说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；
e） 应记录录用人身份、背景和专业资格等，记录审查内容和审查结果等；
f） 应记录录用人录用时的技能考核文档或记录，记录考核内容和考核结果等；；
g） 应签订保密协议，其中包括保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。

4.3.2 管理人员的离岗

a） 人员离岗时应办理调离手续，签署调离后个人信息保密义务的承诺书；
b） 应对即将离岗人员具有控制方法，及时终止离岗人员的所有访问权限，取回其身份认证的配件，诸如身份证件、钥匙、徽章以及机构提供的软硬件设备；
c） 应形成对离岗人员的安全处理记录（如交还身份证件、设备等的登记记录）；
d） 应具有按照离职程序办理调离手续的记录。

4.3.3 管理人员的考核

a) 应设立专人负责定期对接触个人信息数据工作的工作人员进行全面、严格的安全审查、意识考核和技能考核；
b) 应按照考核周期形成考核文档，考核人员应包括各个岗位的人员。

4.3.4 管理人员的教育培训

a) 应制定培训计划并按计划对各岗位员工进行基本的安全意识教育培训和岗位技能培训；
b) 应对违反违背制定的安全策略和规定的人员进行惩戒；
c) 应定期考查安全管理员、系统管理员和网络管理员其对工作相关的信息安全基础知识、安全责任和惩戒措施等的理解程度；
d) 应制定安全教育和培训计划文档，明确培训方式、培训对象、培训内容、培训时间和地点等，培训内容包含信息安全基础知识、岗位操作规程等；
e) 应形成安全教育和培训记录，记录包含培训人员、培训内容、培训结果等。

4.3.5 外部人员访问

a) 应建立关于物理环境的外部人员访问的安全措施：
   1) 制定外部人员允许访问的设备、区域和信息的规定；
   2) 外部人员访问前需要提出书面申请；
   3) 外部人员访问被批准后应有专人全程陪同或监督；
   4) 外部人员访问情况应登记备案。
b) 应建立关于网络通道的外部人员访问的安全措施：
   1) 外部人员访问时应进行身份认证；
   2) 应根据外部访问人员的身份划分不同的访问权限和访问内容；
   3) 应对外部访问人员的访问时间进行限制；
   4) 对外部访问人员对个人信息的操作进行记录。

5 技术措施

5.1 基本要求

应按照GB/T 22239—2008 7.1第三级的物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复要求进行安全保护，并满足以下要求：

5.1.1 网络和通信安全

5.1.1.1 网络架构

a) 应为个人信息处理系统所处网络划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
a) 个人信息处理系统和存储个人信息的设备应作为重点区域部署，并设有边界防护措施。

5.1.1.2 通信传输

a) 应采用校验技术或密码技术保证通信过程中个人信息的完整性；
b) 应采用密码技术保证通信过程中个人信息字段或整个报文的保密性。

5.1.1.3 边界防护

应确保跨越边界的访问和个人信息流通过边界设备提供的受控接口进行通信。

5.1.1.4 访问控制

应在个人信息处理系统边界根据访问控制策略设置访问控制规则。

5.1.1.5 入侵防范

应在个人信息处理系统边界部署入侵防护设备，检测、防止或限制从外部、内部发起的网络攻击行为。

5.1.1.6 恶意代码和垃圾邮件防范

应在个人信息处理系统的网络边界处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

5.1.1.7 安全审计

a) 应在个人信息处理系统的网络边界、重要网络节点进行安全审计，审计应覆盖到每个用户，应对重要的用户行为和重要安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份并避免受到未预期的删除、修改或覆盖等；
d) 审计记录的留存时间应符合法律法规的要求；
e) 应能够对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

5.1.2 设备和计算

5.1.2.1 身份鉴别

a) 应对登陆个人信息处理系统的用户进行身份标识和鉴别；
b) 应确保身份鉴别标识不易被冒用；
c) 身份鉴别信息应定期更换并有一定的复杂度；
d) 个人信息处理系统和存储个人信息的设备应启用登陆失败处理功能，采取诸如结束会话、限制非法登录次数和自动退出等措施；
e) 个人信息处理系统和存储个人信息的设备进行远程管理时，应采取措施防止身份鉴别信息在网络传输过程中被窃听；
f) 个人信息处理系统和存储个人信息的设备应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

5.1.2.2 访问控制

a) 应对登陆个人信息处理系统和存储个人信息的设备的用户分配账户和权限；
a) 个人信息处理系统和存储个人信息的设备应重命名或删除默认账户，修改默认账户的默认口令；
b) 个人信息处理系统和存储个人信息的设备应及时删除或停用多余的、过期的账户，避免共享账户的存在；
c) 个人信息处理系统和存储个人信息的设备应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；
d) 个人信息处理系统和存储个人信息的设备应由授权主体配置访问控制策略，访问控制策略应规定主体对客体的访问规则；

e) 个人信息处理系统和存储个人信息的设备的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
f) 个人信息处理系统和存储个人信息的设备应对个人信息设置安全标记，并控制主体对有安全标记资源的访问。

5.1.2.3 安全审计

a) 个人信息处理和存储设备应启用安全审计功能，并且审计覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，进行定期备份并避免受到未预期的删除、修改或覆盖等；
d) 审计记录的留存时间应符合法律法规的要求；
e) 应对审计进程进行保护，防止未经授权的中断。

5.1.2.4 入侵防范

a) 个人信息处理和存储设备应遵循最小安装的原则，只安装需要的组件和应用程序；
b) 个人信息处理和存储设备应关闭不需要的系统服务、默认共享和高危端口；
c) 个人信息处理和存储设备应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
d) 个人信息处理和存储设备应能够发现存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
e) 个人信息处理和存储设备应能够检测到对重要节点的入侵行为，并在发生严重入侵事件时提供报警；

5.1.2.5 恶意代码防范和程序可信执行

应采取免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

5.1.2.6 资源控制

a) 应限制单个用户或进程对个人信息处理和存储设备系统资源的最大使用限度；
b) 应提供重要节点设备的硬件冗余，保证系统的可用性；
c) 应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；
d) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

5.1.3 应用和数据

5.1.3.1 身份鉴别

a) 个人信息处理应用应对登陆的用户进行身份标识和鉴别，该身份标识应具有唯一性，鉴别信息应具有复杂度并要求定期更换；
b) 个人信息处理应用应提供并启用登陆失败处理功能，并在多次登陆后采取必要的保护措施；
c) 个人信息处理应用应强制用户首次登陆时修改初始口令；
d) 用户身份鉴别信息丢失或失效时，应采取技术措施保证鉴别信息重置过程的安全；
e) 应采取口令、密码技术、生物技术等两种或两种以上的组合鉴别技术对用户进行身份鉴别，且其中一种鉴别技术使用密码技术来实现；

5.1.3.2 访问控制

a) 个人信息处理应用应提供访问控制功能，并对登陆的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 应授予不同账户为完成各自承担任务所需的最小权限，在它们之间形成相互制约的关系；
e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
f) 访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；
g) 个人信息应设置安全标记，控制主体对有安全标记资源的访问；

5.1.3.3 安全审计

a) 个人信息处理应用应提供安全审计功能，审计应覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，并避免受到未预期的删除、修改或覆盖等；
d) 审计记录的留存时间应符合法律法规的要求；
e) 应对审计进程进行保护，防止未经授权的中断。

5.1.3.4 软件容错

a) 应提供个人信息的有效性校验功能，保证通过人机接口输入或通过通信接口输入的内容符合个人信息处理应用设定要求；
b) 应能够发现个人信息处理应用软件组件可能存在的已知漏洞，并能够在充分测试评估后及时修补漏洞；
c) 应能够在故障发生时，继续提供一部分功能，并能够实施必要的措施。

5.1.3.5 资源控制

a) 在通信双方中的一方在一段时间内未做任何响应时，另一方应能够自动结束会话；
b) 应对个人信息处理系统的最大并发会话连接数进行限制；
c) 应能够对单个用户的多重并发会话进行限制。

5.1.3.6 数据完整性

a) 应采取校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据和个人信息；
b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据和个人信息；

5.1.3.7 数据保密性

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据和个人信息；
b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据和个人信息；

5.1.3.8 数据备份恢复

a) 应提供个人信息的本地数据备份与恢复功能；
b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

5.1.3.9 剩余信息保护

a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b) 应保证存有个人信息的存储空间被释放或重新分配前得到完全清除。

5.2 增强要求

5.2.1 云计算安全增强要求

a) 应使用校验技术或密码技术保证虚拟机迁移过程中，个人信息的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
b) 应使用密码技术保证虚拟机迁移过程中，个人信息的保密性，防止在迁移过程中的个人信息泄露；

5.2.2 物联网安全扩展增强要求

物联网感知节点设备采集信息回传应采用密码技术保证通信过程中个人信息的保密性。

6 业务流程

6.1 收集

个人信息的收集行为应满足以下要求：
a) 个人信息收集前，应向被收集的个人信息主体公示本机构收集的目的、范围、方法和手段、处理方式等信息；
b) 个人信息收集应获得个人信息主体的同意和授权；
c) 个人信息收集应执行收集前签署的约定和协议，不应有超范围收集的现象；
d) 应确保收集个人信息过程的安全性：
   1）收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全性；
   2）收集个人信息时，信息在传输过程中应进行加密等保护处理；
   3）收集个人信息的系统应落实网络安全等级保护要求；
   4）收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。

6.2 保存

个人信息的保存行为应满足以下要求：
a) 收集到的个人信息应采取相应的安全加密存储等安全措施进行处理；
b) 应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限；
c) 应对保存的个人信息在超出设置的时限后予以删除；
d) 保存信息的主要设备，应对个人信息数据提供备份和恢复功能，确保数据备份的频率和时间间隔，并使用不少于以下一种备份手段：
   1) 具有本地数据备份功能；
   2) 将备份介质进行场外存放；
   3) 具有异地数据备份功能。

6.3 应用

个人信息的应用应满足以下要求：

a) 对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息；
注：经过匿名化或脱敏的方式处理的个人信息数据可用于历史、统计或科学目的，可以超出与信息主体签署的相关使用协议和约定，但应提供适当的保护措施进行保护。

b) 个人信息主体应拥有控制本人信息的权限，包括：
   1) 允许对本人信息的访问；
   2) 允许对本人信息的修改，包括纠正不准确和不完整的数据；

c) 应对个人信息的接触者设置相应的访问控制措施，包括：
   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时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。

d) 应对必须要通过界面展示的个人信息进行去标识化的处理。

6.4 删除

a) 个人信息相关存储设备，应在个人信息超过保存时限之后进行删除；
b) 个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复；
c) 对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除；
d) 废弃存储设备，应在进行删除后再进行处理。

6.5 第三方委托处理

a) 在对个人信息委托处理时，不应超出该信息主体授权同意的范围；
b) 在对个人信息的相关处理进行委托时，应对受托方的数据安全能力进行评估；
c) 对个人信息进行委托处理时，应签订相关协议要求受托方符合本规范；
d) 应向受托方进行对个人信息数据的使用和访问的授权；
e) 受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。

6.6 共享和转让

如存在个人信息共享和转让行为时，应满足以下要求：

a) 共享和转让行为应经过合法性、必要性评估；
b) 在对个人信息进行共享和转让时应进行安全影响评估，应对受让方的数据安全能力进行评估，并按照评估结果采取有效的保护个人信息主体的措施；
c) 在共享、转让前应向个人信息主体告知转让该信息的目的、数据接收方的类型等信息；
d) 在共享、转让前应得到个人信息主体的授权同意；
e) 应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记；
f) 在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，例如访问、更正、删除、注销等。

6.7 公开披露

个人信息原则上不得公开披露。如存在该行为，应满足以下要求：

a) 公开披露行为应经过合法性、必要性评估；
b) 应对该行为进行安全影响评估，并按照评估结果采取有效的保护个人信息主体的措施；
c) 在披露前应向个人信息主体告知披露的目的、类型等；
d) 在公开披露前应得到个人信息主体的明示同意；
e) 应记录公开披露的信息内容，将公开披露情况中包括公开披露的日期、数据量、目的和数据接收方的基本情况在内的信息进行记录。

6.8 应急处置

a) 应建立健全网络安全风险评估和应急工作机制；
b) 应制定网络安全事件应急预案；
c) 应定期组织相关个人信息事件安全事件演练；
d) 应制定相关制度信息，在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制；
e) 应对进行个人信息处理的相关内部人员进行应急响应培训和应急演练；
f) 应了解知晓应急处置策略和规程；
g) 应记录信息安全事件信息，在应急事件发生后对事件内容进行记录，包括发现事件的人员、事件、涉及的个人信息和人数、发生事件的系统名称等；
h) 应对事件造成的影响进行评估，并采取必要的措施对事态进行控制；
i) 应将事件的情况告知受影响的个人信息主体。