

信息安全技术
信息系统个人信息保护技术与管理规范

Information security technology — Information system personal information
protection management and technical specification

草稿

XXXX—XX—XX 发布

XXXX—XX—XX 实施

河北省技术质量监督局

发布

目 次

目 次..... 2

前 言..... 2

引 言..... 3

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 个人信息处理过程安全保证要求..... 2

4.1 概述..... 2

4.2 收集阶段..... 2

4.2.1 告知和警示..... 2

4.2.2 信息显示限制..... 2

4.2.3 防截获..... 2

4.2.4 防篡改..... 2

4.3 加工阶段..... 3

4.3.1 加工处理..... 3

4.3.2 存储数据的完整性..... 3

4.3.3 存储数据的保密性..... 3

4.4 转移阶段..... 3

4.4.1 转移数据的完整性..... 3

4.4.2 转移数据的保密性..... 3

4.5 删除阶段..... 4

4.5.1 信息删除..... 4

4.5.2 监督执行..... 4

5 个人信息保护安全基本要求..... 5

5.1 技术要求..... 5

5.1.1 物理安全..... 5

5.1.1.1 环境安全..... 5

5.1.1.2 存储介质安全..... 5

5.1.2 网络及主机安全..... 5

5.1.3 终端安全..... 5

5.1.4 权限管理..... 6

5.1.5 数据安全..... 6

5.1.6 访问控制.....6

5.1.7 审计管理.....6

5.1.8 备份恢复.....7

5.2 管理要求.....7

5.2.1 策略与制度.....7

5.2.2 机构与人员.....7

5.2.3 环境与资源.....8

5.2.4 操作与维护.....8

5.2.5 个人信息处理.....9

5.2.6 风险控制.....10

参 考 文 献.....7

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由河北省工业和信息化厅提出并归口。

本标准主要起草单位：河北省信息安全测评中心、中国软件评测中心、河北金信网络技术开发服务有限公司、河北行政学院。

本标准主要起草人：张凤臣、陶卫江、闫利平、马仲光、黄亮、孟宪辉、刘艳、唐刚、张友平、马正英、马一超、朱信铭、王涛、周峰、任旭东、付江、张桐。

引 言

随着信息技术的广泛应用和互联网的不断普及，个人信息在社会、经济活动中的地位日益凸显，滥用个人信息的现象随之出现，给社会秩序和个人切身利益带来了危害。随着网络安全法的颁布实施，其对个人信息保护的提出了更高的要求，规定了收集、使用个人信息规则。为了规范信息系统使用中的个人信息保护行为，促进个人信息的合理使用和有效保护，引导我国个人信息保护工作健康有序发展，依据《中华人民共和国网络安全法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号），制定本标准。

个人信息保护标准体系包括基础类、技术类、管理类和应用类标准。基础类标准用于明确个人信息保护的概念和原则，技术类标准用于从技术角度对信息系统个人信息保护的实施和测评工作进行规范要求，管理类标准是对信息系统个人信息保护管理体系建设的规范指引，应用类标准根据行业业务特性，为各关键行业贯彻执行提供支撑。GB/Z 28828-2012属于基础类标准，对个人信息保护的术语和基本概念进行定义，提出了个人信息保护的八项基本原则及信息系统个人信息处理的行为指导，后续配套技术、管理、应用类标准将参照GB/Z 28828-2012给出的指导原则逐步形成。

本标准包括个人信息保护标准体系中的技术类标准和管理类标准。其中技术类标准提出和规定了个人信息保护安全功能和处理过程中各个阶段的安全保证要求；管理类标准，适用于从管理方面指导涉及个人信息保护的信息系统安全建设、检查、监督，或信息系统使用单位自查等。

信息安全技术

信息系统个人信息保护技术与管理规范

1 范围

本标准技术类标准规定了处理个人信息的信息系统的安全功能要求和个人信息处理过程中各个阶段收集、加工、转移、删除的安全保证要求。本标准管理类标准规定了个人信息保护策略与制度、机构与人员、环境与资源、操作与维护、个人信息处理和风险控制六个方面的管理要求。

技术类标准适用于指导除政府机关等行使公共管理职责的机构以外的各类组织和机构，参照GB/Z 28828-2012给出的指导原则进行信息系统个人信息处理的具体设计和实现，对按照个人信息保护要求进行的信息系统安全测试和评估可参照使用。管理类标准适用于指导除政府机关等行使公共管理职责的机构以外的各类组织和机构，参照GB/Z 28828-2012给出的指导原则进行信息系统个人信息保护的管理指导和评估。

2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 2887-2011 计算机场地通用规范

GB/T 9361-2011 计算机场地安全要求

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/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

3 术语和定义

GB/Z 28828-2012中界定的术语和定义适用于本标准。

1、用户画像 user profiling

通过收集、综合、分析个人信息，获得某特定自然人个人特征，如对其职业、经济、健康、教育、个人喜好、信用、行为、位置等方面做出分析、预测，并形成标签化的用户特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

2、个人信息影响评估 Personal Information Impact Assessment

针对个人信息处理活动，检验其合规程度，判断其对个人信息主体合法权益造成损害的风险，以及评估为保护个人信息主体的各项措施的分析过程。

3、删除 delete

去除个人信息，使其在日常业务场景中不可被检索、访问。

4、披露 public disclosure

向社会或特定受众发布信息的行为。

5、转让 transfer

个人信息控制权由一个控制者向另一个控制者转移的过程。

6、共享 sharing

个人信息控制者向其他控制者提供数据、且双方分别拥有对数据的独立控制权的过程。

7、匿名化 anonymization

对个人信息进行技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原。

8、去标识化 De-identification

对个人信息进行技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体。

注：去标识化仍建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

9、个人信息最小元素集 Minimum collection of personal information

个人信息最小元素集是指实现产品或服务核心业务功能和满足法律法规要求所必需使用的个人信息集合。如实现即时通信功能所必需的个人信息为账号和通信记录；实现导航功能所必需的个人信息为位置信息。

4 个人信息处理过程安全保证要求

4.1 概述

本标准按收集、加工、转移和删除4个阶段对信息系统个人信息处理过程提出以下安全保证要求。

4.2 收集阶段

4.2.1 告知和警示

本项目包括但不限于：

应在进行个人信息收集前，应确认数据来源的合法性，如果是通过交易得来的数据，明确交易对象和过程的合法性。采用个人信息主体易知悉的方式，通过技术手段明确告知、警示和承诺相关事项，具体内容应满足 5.2.5 a)的要求。

4.2.2 信息显示限制

本项目包括但不限于：

- a) 收集个人信息的客户端应隐蔽个人输入的口令之类的信息，使其不以明文形式显示。
- b) 显示个人敏感信息或个人一般信息中与个人敏感信息相关联的信息时，涉及的个人敏感信息应不超过 3 种，对超范围信息显示应进行权限控制。
- c) 在公共环境下，显示个人敏感信息时要隐藏部分字段或内容。

4.2.3 防截获

本项目包括但不限于：

信息系统应能使用户输入的数据不被其他设备或程序非授权获取。

4.2.4 防篡改

本项目包括但不限于：

信息系统应能防止用户输入的数据被其他设备或程序篡改。

4.3 加工阶段

4.3.1 加工处理

本项目包括但不限于：

- a) 应制定个人信息加工程序，并严格按照程序进行个人信息处理。
- b) 应采用必要手段，对违反程序进行个人信息的加工行为进行禁止。
- c) 严格控制对个人信息进行加工的用户，避免多用户进行同一操作行为。
- d) 当预期的目的达到后，应锁定个人信息，禁止对个人信息的进一步加工。

4.3.2 存储数据的完整性

本项目包括但不限于：

应对存储的个人信息相关的数据进行完整性检测与恢复，确保个人信息处于完整、可用状态。

4.3.3 存储数据的保密性

本项目包括但不限于：

- a) 应对存储的个人信息数据进行保密性保护，确保具有访问权限的合法用户才能对其进行访问。
- b) 不应在客户端上存储个人敏感信息及其密文。
- c) 个人敏感信息及其密文在使用后应立即清除。
- d) 应对客户端存储的个人一般信息进行加密处理。
- e) 不应将个人敏感信息中的个人鉴别信息以任何形式发到客户端。鉴别信息的比对只能在服务器中进行。
- f) 信息系统或云计算系统中存储个人敏感信息，必要时应采用加密的方式存储。并通过有效的技术措施保证存储过程中个人敏感信息不会被任何与预期处理目的无关的个人、组织和机构获取。
- g) 对用户密码进行加密存储。

4.4 转移阶段

4.4.1 转移数据的完整性

本项目包括但不限于：

- a) 应对传输中的个人信息数据进行完整性保护，例如：进行完整性检测，以及必要的完整性恢复等，确保个人信息数据在传输过程中不会发生被篡改、删除、插入等情况。

4.4.2 转移数据的保密性

本项目包括但不限于：

- a) 不应使个人信息转移的范围超出在个人信息收集阶段已告知的处理个人信息的范围。
- b) 应在通信过程中对传输个人敏感信息的报文或会话进行加密。
- c) 个人敏感信息中的个人身份信息在发送至客户端之前，应屏蔽个人身份信息中不可猜测的一部分，被屏蔽部分应使用统一的符号替代。
- d) 应采取数据加密或协议加密措施（如：MD5、DES、RSA、ECC 等加密算法，https 等传输协议），保证转移过程中，个人敏感信息不会被预期个人信息获得者之外的任何个人、组织和机构获取。
- e) 对个人信息存储边界进行明确。

4.5 删除阶段

4.5.1 信息删除

本项目包括但不限于：

- a) 对于需要删除的个人信息，应采取信息完全清除或删除工具等有效措施，及时妥善删除或销毁。
- b) 在达到收集阶段告知的个人信息使用目的后，应立即删除或销毁相关信息；如需继续处理个人信息，应消除其中能够识别具体个人的内容；如需继续处理个人敏感信息，应获得个人信息主体的明示同意。
- c) 在到达收集阶段告知的个人信息留存期限时，应立即删除或销毁相关信息。对留存期限有明确规定的，应严格按照相关规定执行。
- d) 应采取必要的措施，防止删除或销毁的个人信息数据泄露。
- e) 应在将用户个人敏感信息所在的存储空间（无论在硬盘上还是在内存中）释放或再分配给其他用户前完全清除其中的个人信息。

4.5.2 监督执行

本项目包括但不限于：

- a) 应根据“双人控制”原则，在监督人员在场的情况下，删除或销毁个人敏感信息。
- b) 对于不同类别的个人信息进行删除或销毁，应分别建立删除或销毁登记记录。删除或销毁记录至少应包括：使用人、用途、删除或销毁方式与时间、删除或销毁人及其签字、监督人及其签字等内容。

5 个人信息保护安全基本要求

5.1 技术要求

5.1.1 物理安全

5.1.1.1 环境安全

本项目包括但不限于：

- a) 机房在场地选择、防火、内部装修、供配电、空气调节、安全等方面应符合 GB/T 9361-2011 中 B 级以上的要求。
- b) 应为机房安装电子门禁系统，控制、鉴别和记录进入机房的人员。
- c) 应在物理隔离区域进出通道或机房内部等重要工作区域安装录像监控设备，监控录像保留期限应满足 5.2.3 g) 的要求。

5.1.1.2 存储介质安全

本项目包括但不限于：

- a) 应对存放个人信息数据的各类介质，例如：纸介质、磁介质、半导体介质和光介质等，采取相应的技术保护措施，防止其被盗、被毁或受损。
- b) 应对系统内使用的移动存储介质采用技术手段进行管理，防止非系统内的移动存储介质在系统内使用。
- c) 应对不再使用或二次使用存储个人敏感信息的介质采用技术手段进行清除或销毁。

5.1.2 网络及主机安全

本项目包括但不限于：

- a) 应明确信息系统的边界，并按照一定的需求划分安全管理区域，部署必要的安全设备（如：防火墙、入侵检测、主机审计、防病毒、防篡改及完整性保护系统等），实施安全防护策略。
- b) 应设置主机本地安全策略，并开启相应的安全审计功能。包括：
 - 1) 密码策略，开启密码复杂度要求，并设置密码长度、最长使用周期和最短使用周期等；
 - 2) 账户锁定策略，设置账户锁定时间、账户锁定阈值等；
 - 3) 审核策略和安全选项，对事件的成功和失败操作均进行审核，合理设置安全选项中的策略。
- c) 应采用技术手段对处理个人信息的主机进行防护，以限制使用主机的串/并口、USB 口、蓝牙、无线网卡等。
- d) 应采用技术手段限制信息系统内的主机非授权接入其他信息系统中，限制非系统内主机接入到信息系统中。

5.1.3 终端安全

本项目包括但不限于：

- a) 应采用技术手段对采集、处理、存储个人信息的计算机终端进行防护，并对使用计算机终端的串/并口、USB 口、蓝牙、无线网卡等进行管控，防止未经授权的信息泄露。
- b) 应设置终端本地安全策略，并开启相应的安全审计功能。包括：
 - 1) 密码策略，开启密码复杂度要求，并设置密码长度、最长使用周期和最短使用周期等；
 - 2) 账户锁定策略，设置账户锁定时间、账户锁定阈值等；
 - 3) 审核策略和安全选项，对事件的成功和失败操作均要审核，合理设置安全选项中的策略。

- c) 应采用技术手段限制采集、处理、存储个人信息的计算机终端非授权接入其他信息系统中。
- d) 应按照 4.1 的要求对采集、处理、存储个人信息的单机系统进行物理安全防护。
- e) 应采取必要的技术和管理手段限制外出携带采集、处理、存储个人信息的计算机终端。

5.1.4 权限管理

本项目包括但不限于：

- a) 在个人信息系统中，应根据权限分配名单进行权限分配，并定期审核。
- b) 应根据“双人控制”原则，对个人敏感信息的访问权限应根据用户分类清单进行分配。必要时应根据“双人控制”原则，查询、使用和处理与个人敏感信息相关联的个人一般信息时，应进行严格的访问权限分配。

5.1.5 数据安全

本项目包括但不限于：

- a) 在信息系统中，应对存储、处理个人信息的数据库进行安全设计。包括：
 - 1) 应为个人敏感信息和个人一般信息设计不同的数据库，且在个人敏感信息和个人一般信息之间采取一定的加密算法进行关联对应；
 - 2) 对数据库的使用操作进行安全审计，审计结果的存储满足管理制度中的基本要求；
 - 3) 应加强数据库系统的加固，对个人敏感信息以及个人一般信息中与个人敏感信息相关联的信息的输入输出进行管控，防止非授权输入输出。
- b) 应用于云计算系统上的个人信息处理系统的安全性应满足以下要求：
 - 1) 应对个人信息数据在云计算系统的存放边界进行详细的确认；
 - 2) 应对云计算系统的安全防护措施进行测试；
 - 3) 应采用技术手段对退出云计算系统的个人信息数据进行完整删除。

5.1.6 访问控制

本项目包括但不限于：

- a) 应采取相应的访问控制策略对不同类型个人信息相关数据的访问进行控制。包括：
 - 1) 按照权限划分的要求，一般权限人员可以访问到不多于 3 类的个人敏感信息以及个人一般信息中与个人敏感信息相关联的信息；特殊权限人员可以访问更多的个人敏感信息；
 - 2) 对个人信息的模糊查询进行管控，对模糊查询结果的复制、输出、利用等行为需经授权。
- b) 应采取相应的访问控制策略对不同类型用户的访问进行控制。包括：
 - 1) 应限定个人信息主体在信息收集阶段对其个人信息进行更正和修改，并在更正和修改前对用户身份进行鉴别；
 - 2) 采用符合管理制度要求的技术手段（如：口令、数字证书、生物特征等）验证访问个人信息的人员身份，采用口令验证的要对口令长度、复杂度进行限定；
 - 3) 对信息系统用户、接入信息系统的设备进行标识与鉴别，对标识与鉴别信息进行管理、维护，确保其不被非授权地访问、修改或删除，对接入信息系统的设备进行维护管理时应通过口令认证其管理权限。
- c) 采用数字签名等技术手段保证用户操作行为的不可否认性。

5.1.7 审计管理

本项目包括但不限于：

- a) 应通过开启主机设备、数据库、网络设备、安全设备、终端设备等的日志功能，对个人信息处理的相关过程进行记录。记录内容包括：操作人、操作日期和时间、操作内容与类型、成功与

- 否等。应根据需要确定审计存储空间，当存储空间将满时进行告警。
- b) 应对审计记录设定一定的留存期，留存期应满足 5.2.4 h) 9) 的要求。
 - c) 采用自动机制，对存在安全隐患的不安全或者异常行为进行告警。

5.1.8 备份恢复

本项目包括但不限于：

- a) 应具有必要的备份恢复功能，对存储的个人信息数据进行备份和必要时的恢复处理，同时保证备份、恢复信息的完整性、可靠性和准确性。
- b) 信息系统应具有策略设置功能，在服务器和虚拟服务器上存储个人信息时，可以根据对个人信
息进行处理的方式，制定相应的保护策略，包括：权限分配、访问控制、密钥管理、存储期限、
覆盖方式、备份恢复等。

5.2 管理要求

5.2.1 策略与制度

本项目包括但不限于：

- a) 应建立明确的个人信息保护管理目标、内容和范围。
- b) 应制定明确的个人信息保护策略，个人信息保护工作计划，做出个人信息保护声明。
- c) 应根据国家法律、法规、规章等有关要求，结合实际制定个人信息保护管理规章制度。包括：
 - 1) 对文件、记录、合同等文档进行备案管理；
 - 2) 在个人信息保护管理过程中记录与个人信息相关的活动和行为（如：制度建立、宣传、教
育、培训、安全管理、过程改进等）的目的、时间、范围、对象、方式方法、效果、反馈
等信息；
 - 3) 对信息系统个人信息保护系统的设计与开发建立相关的规范和流程；
 - 4) 定期检查个人信息安全策略、制度的适宜性，并对其进行持续的改进和完善；
 - 5) 为个人信息主体提供投诉或申诉渠道；
 - 6) 制定合理、有效的个人信息侵害补救措施（包括纠正错误、消除影响、恢复名誉、适当赔
偿等）。

5.2.2 机构与人员

本项目包括但不限于：

- a) 应建立个人信息保护管理责任制，明确个人信息保护管理机构和人员的职责。个人信息管理者
的职责应包括：
 - 1) 制订、维护、宣传和落实个人信息保护策略、制度与程序；
 - 2) 开展个人信息保护日常管理、监督检查、风险控制和技术指导；
 - 3) 分析处理个人信息保护相关事件等。
- b) 应根据“业务需要”和“最少够用”原则，对信息系统访问权限进行分配，控制对个人信息的
访问和使用，确保任何人都只能在其履行职责时间范围内访问其开展业务所必需的个人信息，
防止未经授权擅自对个人信息进行查看、披露、篡改或破坏。个人信息获得者的职责应包括：
 - 1) 按照个人信息主体的意愿、委托合同和个人信息保护管理制度，在授权范围内进行个人信
息的处理；
 - 2) 当个人信息处理过程中发生个人信息安全事件时，应按照管理制度要求向个人信息管理者
报告，并在其指导或授权下采取补救措施。

- c) 应制定相关规章制度，对涉及个人信息的第三方人员（包括：测评机构、设备供应商、电信运营商、外来参观人员等）提出基本要求。包括：
 - 1) 按照来访对象和工作性质，制定相关管理制度；
 - 2) 按照相关管理制度及第三方人员涉及的个人信息内容，必要时与其签订保密协议；
 - 3) 规定第三方人员进入机房时的活动范围并经审批，第三方人员进入机房时有管理人员陪同；
 - 4) 限定第三方人员访问个人信息的范围。
- d) 提供个人信息的个人信息主体应获知相关事项并取得相关权利。包括：
 - 1) 个人信息的处理目的、手段、内容和披露范围；
 - 2) 进行投诉或申诉的渠道；
 - 3) 访问、修改、删除自己个人信息的权力；
 - 4) 个人信息安全事件发生时获得事件通告的权力；
 - 5) 个人信息主体权益受到侵害时追究法律责任的权力。
- e) 应对涉及个人信息的从业人员进行岗前、在岗和离岗管理。包括：
 - 1) 对从业人员进行背景了解和调查，签署保密协议或在劳动合同中设置相应的保密条款；
 - 2) 对从业人员就个人信息安全相关法律、法规、标准和管理制度等进行培训和宣贯，确保相关人员了解各自的个人信息保护职责以及违反职责可能导致的后果；
 - 3) 从业人员离岗时，按照管理制度终止其对个人信息的访问权限。

5.2.3 环境与资源

本项目包括但不限于：

- a) 应在安全的工作环境（包括：物理环境、网络环境、计算机环境 and 应用环境）中进行个人信息各阶段的处理。
- b) 应对个人信息处理相关的工作环境进行管理，防止个人信息被泄露、损毁、丢失或未经授权使用。
- c) 应对存储或处理个人信息的相关设备和各类介质，例如：纸介质、磁介质、半导体介质和光介质等，进行严格管理，移入或移出保护区域应经申请和审批。
- d) 应对机房分区域进行管理。包括：
 - 1) 按照管理要求在机房内设置不同区域，区域之间设置物理隔离装置或隔离标识；
 - 2) 在重要区域前设置交付或安装等过渡区域等。
- e) 应对存放个人信息数据的各类介质进行专人管理，对移动存储介质统一购买、统一发放，并定期进行核查。
- f) 移动存储介质的存放应符合 GB/T 2887-2011 中“媒体存放条件”对存放环境的要求。
- g) 应对人员、设备进出情况或相关活动进行监控和记录，监控录像资料至少保留 90d。
- h) 应对个人信息系统的软硬件资源和信息资源制定管理要求。

5.2.4 操作与维护

本项目包括但不限于：

- a) 应建立个人信息保护安全管理操作流程，规范对个人信息的操作与维护。
- b) 应对信息系统用户进行分类管理，建立用户分类清单，按照审查和批准的用户分类清单建立用户和分配权限。
- c) 应对信息系统个人信息处理过程中收集、存储、转移、删除各阶段提出具体工作要求，明确各岗位在个人信息保护管理方面的工作内容。
- d) 应对个人信息各阶段的处理进行授权管理和访问控制，严格控制对个人信息的访问、处理权限。

- e) 应对个人信息各阶段的处理活动进行监控、跟踪和审计，建立相关的日志、记录，及时发现和处理个人信息保护相关的安全事件。
- f) 必要时，应对个人敏感信息的处理执行双人控制原则。
- g) 未经授权，不允许对个人一般信息和个人敏感信息相关联的个人的查询结果进行复制、使用和处理。
- h) 应对个人信息系统的维护进行管理。包括：
 - 1) 采集、处理、存储个人信息的计算机终端应使用非系统管理员用户作为日常办公用户，禁止其他高权限或特殊权限的用户进行日常办公，删除或禁用系统中的特殊用户、多余用户。
 - 2) 应建立用户口令保护制度，对主机、网络设备、安全设备、计算机终端、应用系统用户口令的长度、复杂度、修改周期进行规定，禁止空口令、弱口令用户登录。
 - 3) 应定期进行木马、病毒等恶意代码查杀，并及时对安全防护系统进行更新升级；
 - 4) 应定期对采集、处理、存储个人信息的主机和终端进行安全漏洞扫描和安全配置检查，及时评估和修补已经发布的安全漏洞。
 - 5) 应及时升级病毒库，安装操作系统、数据库系统及中间件系统补丁。
 - 6) 用户登录服务器连续失败达到 5 次，应冻结用户账号，在一定的时间延迟后，经系统管理员对用户身份进行验证并通过验证后，才能再恢复其用户状态；用户登录系统后，无任何操作时间达到 30min，应要求用户重新登录并验证其身份。
 - 7) 应由系统管理员实施用户账户的添加、修改或删除；对连续 90d 未使用的账号予以权限冻结；冻结后 30d 仍未使用的，予以注销。
 - 8) 应对用户口令长度、组成、修改周期进行限制（禁止空口令、弱口令用户登录；一般用户口令应由大小写字母、数字及特殊字符中两者以上，长度不小于 8 位；口令修改周期一般不长于 30d）；对口令进行加密保护，在系统中口令不应以任何明文的形式出现；重置用户口令前应对用户身份进行核实。
 - 9) 应对审计记录设定一定的留存期，并至少留存 90d。在留存期内，应保持审计记录的连续性。
 - 10) 应通过内部审计人员或第三方审计人员，定期对个人信息处理过程进行审计并形成审计报告。

5.2.5 个人信息处理

本项目包括但不限于：

- a) 收集阶段。应将个人信息收集的目的、范围、方法和手段、处理方式等明确告知或警示个人信息主体，只收集能够达到已告知目的的最少信息，并征得个人信息主体同意。
 - (一) 应告知或警示的相关事项包括：
 - 1) 收集个人信息的目的；
 - 2) 收集个人信息的法律、法规依据；
 - 3) 收集个人信息的方式、手段、内容；
 - 4) 保护个人信息的措施；
 - 5) 个人信息收集方与个人信息主体签订的合同或协议；
 - 6) 个人信息管理者、个人信息获得者的名称、地址、联系方式等；
 - 7) 个人信息主体有权选择是否允许对其个人信息进行处理；
 - 8) 个人信息主体有权访问自己的个人信息；
 - 9) 个人信息主体提供个人信息后可能存在的风险，以及不提供个人信息可能出现的后果；
 - 10) 处理个人信息的范围，包括：披露或向其他组织和机构提供其个人信息的范围；

- 11) 个人信息主体的投诉渠道和应急机制;
- 12) 个人信息主体个人信息侵害可能导致的实质损害及解决办法。

(二) 个人信息收集方应承诺以下相关事项:

- 1) 采用专业术语清楚表达收集目的, 对处理个人敏感信息的需求进行充分说明;
 - 2) 收集目的符合相关法律、法规;
 - 3) 不收集与收集目的不相关的个人信息;
 - 4) 建立个人信息收集程序, 保障个人信息的质量和准确性;
 - 5) 对个人信息的处理操作仅取决于收集目的所决定的处理过程, 不对个人信息进行其他不相关的处理;
 - 6) 从非个人信息主体所收集的个人信息是可靠的;
 - 7) 收集的个人信息是准确的、最新的, 是与收集目的相关的、充分的;
 - 8) 收集个人信息前或将个人信息用于其他目的时, 向个人信息主体说明并获取同意;
 - 9) 个人信息处理程序发生变更时通知个人信息主体;
 - 10) 在收集个人信息, 或试图将其转移或委托于其他组织或机构时, 应确保个人信息主体能够确认同意或不同意对其个人信息执行相应操作;
 - 11) 系统持续进行个人信息收集时, 应允许个人信息主体配置、调整、关闭个人信息收集功能或删除其内容;
 - 12) 仅采用已告知的技术手段收集个人信息, 不采取隐藏的技术手段收集个人信息。
- b) 加工阶段。应建立个人信息存储清单, 定期备份存储的个人信息, 对备份数据按照原数据的要求进行管理, 保证存储、备份、恢复个人信息的保密性、完整性和准确性。
 - c) 转移阶段。应基于明确、合法的目的, 采用已告知的手段, 征得个人信息主体事先同意的情况下, 在已告知的范围内进行。在转移的过程中应保证个人信息保密性、完整性和准确性, 防止个人信息在传输过程中被其他人未经授权获取。
 - d) 删除阶段。应制定严格的个人信息删除或销毁制度, 确保纸介质、磁介质、半导体介质和光介质等存储到期或已经使用完毕的个人信息得到及时、有效、完全清除或销毁。通过双人控制及记录等措施, 防止个人信息在删除或销毁过程中被泄露。

5.2.6 风险控制

本项目包括但不限于:

- a) 应将个人信息保护管理纳入组织中相应机构的工作和管理, 在统一、规范的信息安全风险管理框架中实施个人信息保护管理。
- b) 应建立个人信息保护日常管理监督机制, 定期检查个人信息保护策略、制度的落实情况, 并及时进行相关整改, 确保个人信息保护的各項要求落实到位。
- c) 应建立个人信息保护检查评估机制和工作流程, 及时发现和评估个人信息保护工作中存在的漏洞及风险。
- d) 应建立信息系统投入运行前的功能审核机制, 保证信息系统无个人信息数据主动外泄的隐藏功能。
- e) 应建立第三方评估机构定期对信息系统进行安全测评的机制, 发现问题及时整改, 以提高系统的安全性和个人信息防护水平。
- f) 采用云计算部署信息系统的, 应依据 GB/T 31168-2014 和 GB/T 31167-2014, 部署前考核云计算服务商的能力水平, 部署后与云计算服务商签订保密协议, 使其保证不对信息系统的个人信息进行转存、读取、分析和外泄, 并定期对信息系统进行安全检查。
- g) 应对云计算系统上个人信息处理系统的安全性进行风险评估。

- h) 应建立个人信息保护应急响应机制，形成应急预案，并定期演练，以有效应对个人信息保护安全事件。
- i) 应定期开展个人信息保护管理相关的内部或外部审计，并根据审计结果持续改善相关策略、制度和流程。
- j) 应建立个人信息保护安全事件报告和通报机制，提高组织个人信息保护的安全预防和预警能力。

参 考 文 献

[1] 全国人民代表大会常务委员会关于加强网络信息保护的決定，2012

[2] 《中华人民共和国网络安全法》

[3] 国务院關於大力推进信息化发展和切实保障信息安全的若干意见（国发〔2012〕23号），2012

[4] 电信和互联网用户个人信息保护規定（工业和信息化部令第24号），2013

[5] 欧盟电子通讯领域个人数据处理及个人隐私保护指令2002/58/EC，2002

[6] OECD 关于保护隐私和个人数据跨国流通的建议，2013

[7] 中华人民共和国刑法修正案（七），2009

[8] 中华人民共和国计算机信息系统安全保护条例（国务院令第147号），1994

[9] 中华人民共和国计算机信息网络国际联网管理暂行规定（国务院令第195号），1996

[10] 中华人民共和国计算机信息网络国际联网管理暂行规定实施办法（国信〔1998〕003号），1998

[11] NIST SP 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

[12] ISO/IEC FDIS 29100 Information technology – Security techniques – Privacy framework, 2011
