

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

中标华信（北京）认证中心有限公司认证规则公开方式或可获取的途径：本中心认证规则信息依法依申请公开，如需获取经备案的认证项目认证规则全文请发函至本中心邮箱 cshcc@cshcc.cn 或拨打电话 010-88255986 联系本机构技术信息部获取。

中标华信（北京）认证中心有限公司认证依据用标准或技术规范名称公开方式或可获取的途径：本中心按国家认监委要求备案及公示认证依据的封面和目录等关键信息，获取全文请购买和使用正版标准文件。

【认证规则、认证依据及认证证书公示信息及相关附件】

认证类别	认证领域	认证规则名称	认证规则编号	认证规则版本信息	状态标识	认证规则发布单位	认证规则发布/实施/修订日期	认证规则来源信息	认证依据用标准或技术规范名称	认证依据用标准或技术规范编号	认证依据用标准或技术规范发布单位	认证依据用标准或技术规范发布/实施日期	认证依据用标准或技术规范公开方式或可获取的途径	认证证书名称	认证证书与认证标志发布/所有权单位	认证证书样式
管理体系	其他管理体系	公有云中保护个人可识别信息管理体系认证规则	CSHCC-RZGZ-PC	B0	新建	中标华信（北京）认证中心有限公司	20251215	自行制定	信息技术-安全技术-作为 PII 处理者的公有云中保护个人可识别信息（PII）的操作规范	ISO/IEC 27018:2019	国际标准化组织；国际电工委员会	20190115	见附页	公有云中保护个人可识别信息管理体系认证证书	中标华信（北京）认证中心有限公司	见附页
									公有云中保护个人可识别信息管理体系认证技术规范	CTS CSHCC014-2025	中标华信（北京）认证中心有限公司	20260101				

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息



公有云中保护个人可识别信息
管理体系认证规则

文件编号：CSHCC-RZGZ-PC

文件版本：B0

编 制：李岩、金鹏

审 核：伍倩惠

批 准：刘伯钊

2025-12-15 发布

2026-01-01 实施

中标华信（北京）认证中心有限公司 发布

CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则

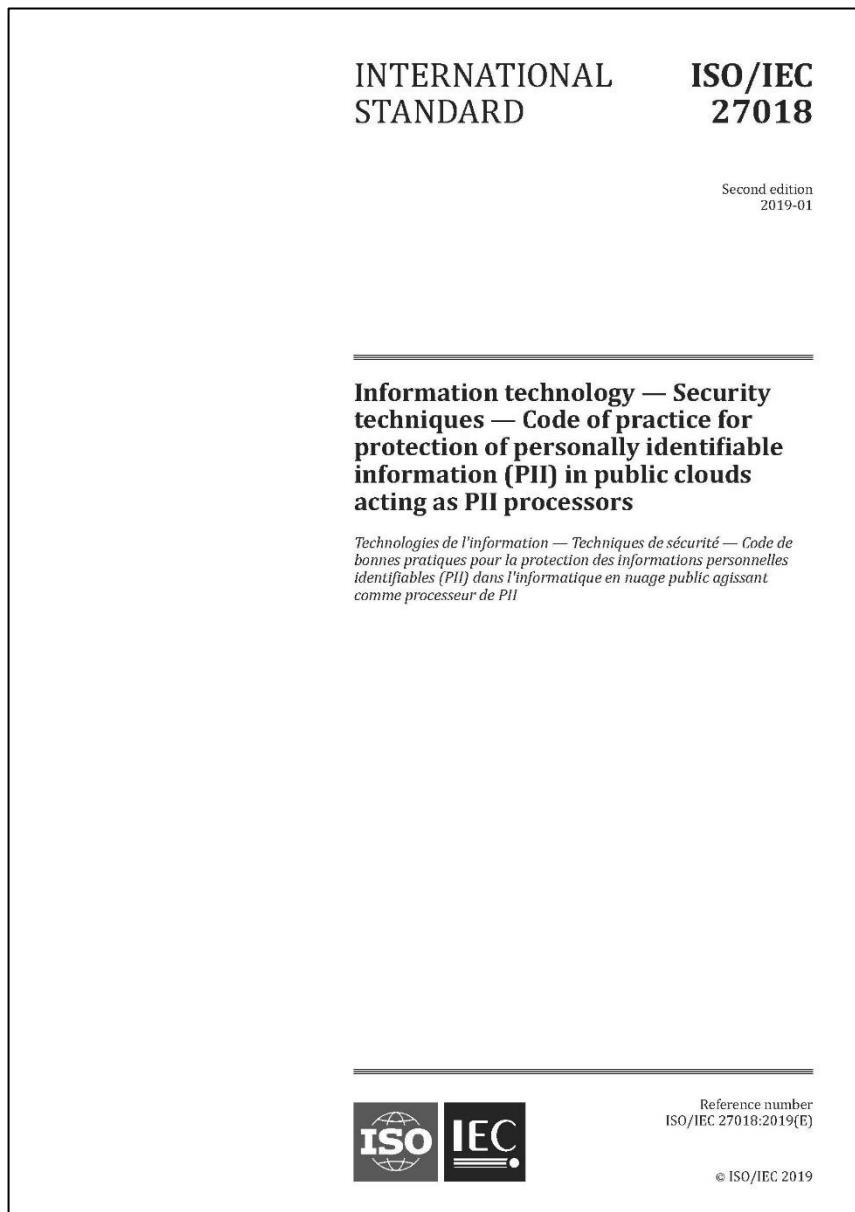
目 录

1. 适用范围.....	3
2. 对认证人员的基本要求.....	3
3. 初次认证程序.....	3
4. 监督审核程序.....	10
5. 再认证程序.....	11
6. 认证书状态管理.....	11
7. 认证书及认证标志要求.....	13
8. 与其他管理体系的结合审核.....	14
9. 其他.....	14
附录 A. 审核时间要求.....	15
附录 B. 修订记录.....	17

中标华信（北京）认证中心有限公司

2 / 17

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息



ISO/IEC 27018:2019(E)	
	Page
Contents	
Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	3
4.1 Structure of this document	3
4.2 Control categories	4
5 Information security policies	4
5.1 Management direction for information security	4
5.1.1 Policies for information security	4
5.1.2 Review of the policies for information security	5
6 Organization of information security	5
6.1 Internal organization	5
6.1.1 Information security roles and responsibilities	5
6.1.2 Segregation of duties	5
6.1.3 Contact with authorities	5
6.1.4 Contact with special interest groups	5
6.1.5 Information security in project management	5
6.2 Mobile devices and teleworking	5
7 Human resource security	5
7.1 Prior to employment	5
7.2 During employment	5
7.2.1 Management responsibilities	6
7.2.2 Information security awareness, education and training	6
7.2.3 Disciplinary process	6
7.3 Termination and change of employment	6
8 Asset management	6
9 Access control	6
9.1 Business requirements of access control	6
9.2 User access management	6
9.2.1 User registration and de-registration	7
9.2.2 User access provisioning	7
9.2.3 Management of privileged access rights	7
9.2.4 Management of secret authentication information of users	7
9.2.5 Review of user access rights	7
9.2.6 Removal or adjustment of access rights	7
9.3 User responsibilities	7
9.3.1 Use of secret authentication information	7
9.4 System and application access control	7
9.4.1 Information access restriction	7
9.4.2 Secure log-on procedures	8
9.4.3 Password management system	8
9.4.4 Use of privileged utility programs	8
9.4.5 Access control to program source code	8
10 Cryptography	8
10.1 Cryptographic controls	8
10.1.1 Policy on the use of cryptographic controls	8
10.1.2 Key management	8

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

ISO/IEC 27018:2019(E)

11	Physical and environmental security	8
11.1	Secure areas	8
11.2	Equipment	9
11.2.1	Equipment siting and protection	9
11.2.2	Supporting utilities	9
11.2.3	Cabling security	9
11.2.4	Equipment maintenance	9
11.2.5	Removal of assets	9
11.2.6	Security of equipment and assets off-premises	9
11.2.7	Secure disposal or re-use of equipment	9
11.2.8	Unattended user equipment	9
11.2.9	Clear desk and clear screen policy	9
12	Operations security	9
12.1	Operational procedures and responsibilities	9
12.1.1	Documented operating procedures	10
12.1.2	Change management	10
12.1.3	Capacity management	10
12.1.4	Separation of development, testing and operational environments	10
12.2	Protection from malware	10
12.3	Backup	10
12.3.1	Information backup	10
12.4	Logging and monitoring	11
12.4.1	Event logging	11
12.4.2	Protection of log information	11
12.4.3	Administrator and operator logs	11
12.4.4	Clock synchronization	12
12.5	Control of operational software	12
12.6	Technical vulnerability management	12
12.7	Information systems audit considerations	12
13	Communications security	12
13.1	Network security management	12
13.2	Information transfer	12
13.2.1	Information transfer policies and procedures	12
13.2.2	Agreements on information transfer	12
13.2.3	Electronic messaging	12
13.2.4	Confidentiality or non-disclosure agreements	12
14	System acquisition, development and maintenance	13
15	Supplier relationships	13
16	Information security incident management	13
16.1	Management of information security incidents and improvements	13
16.1.1	Responsibilities and procedures	13
16.1.2	Reporting information security events	13
16.1.3	Reporting information security weaknesses	13
16.1.4	Assessment of and decision on information security events	13
16.1.5	Response to information security incidents	14
16.1.6	Learning from information security incidents	14
16.1.7	Collection of evidence	14
17	Information security aspects of business continuity management	14
18	Compliance	14
18.1	Compliance with legal and contractual requirements	14
18.2	Information security reviews	14
18.2.1	Independent review of information security	14
18.2.2	Compliance with security policies and standards	14
18.2.3	Technical compliance review	14

ISO/IEC 27018:2019(E)

Annex A (normative) Public cloud PII processor extended control set for PII protection	15
Bibliography	23

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

中标华信认证中心 内部使用翻译稿
ISO/IEC27018:2019 信息技术 安全技术 作为PII处理者的公有云中保护个人可识别信息（PII）的操作规范

国际 ISO / IEC
标准 27018

第二版
2019-01

信息技术—安全技术—作为PII处理者的公有云中
保护个人可识别信息（PII）的操作规范

信息技术—安全技术—公有云中保护个人信息的良好做法保护个人
可识别信息（PII）



参考编号
ISO/IEC 27018:2019(E)

© ISO/IEC 2019

ISO/IEC 27018:2019(E)

中标华信认证中心（www.cshcc.cn） 内部使用翻译稿-20210317

中标华信认证中心 内部使用翻译稿
ISO/IEC27018:2019 信息技术 安全技术 作为PII处理者的公有云中保护个人可识别信息（PII）的操作规范

目录 页码

前言	vi
引言	vii
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 概述	2
4.1 标准结构	2
4.2 控制类别	4
5 信息安全策略	4
5.1 信息安全管理指导	4
5.1.1 信息安全策略	4
5.1.2 信息安全策略的评审	4
6 信息安全组织	5
6.1 内部组织	5
6.1.1 信息安全的角色和责任	5
6.1.2 职责分离	5
6.1.3 与职能机构的联系	5
6.1.4 与特定相关方的联系	5
6.1.5 项目管理中的信息安全	5
6.2 移动设备和远程工作	5
7 人力资源安全	5
7.1 任用前	5
7.2 任用中	5
7.2.1 管理责任	5
7.2.2 信息安全意识、教育和培训	5
7.2.3 违规处理过程	6
7.3 任用的终止和变更	6
8 资产管理	6
9 访问控制	6
9.1 访问控制的业务要求	6
9.2 用户访问管理	6
9.2.1 用户注册和注销	6
9.2.2 用户访问供给	6
9.2.3 特许访问权管理	7
9.2.4 用户的秘密鉴别信息管理	7
9.2.5 用户访问权的评审	7
9.2.6 访问权的移除或调整	7
9.3 用户责任	7
9.3.1 秘密鉴别信息的使用	7
9.4 系统和应用访问控制	7
9.4.1 信息访问限制	7
9.4.2 安全登录规程	7

中标华信认证中心（www.cshcc.cn） 内部使用翻译稿-20210317

ii

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

中标华信认证中心 内部使用翻译稿	
ISO/IEC27018:2019 信息技术 安全技术 作为PII处理者的公有云个人保护个人可识别信息(PII)的操作规范	
9.4.3 口令管理规定	7
9.4.4 特权实用程序的使用	7
9.4.5 程序源代码的访问控制	7
10 密码	8
10.1 密码控制	8
10.1.1 密码控制的使用策略	8
10.1.2 密钥管理	8
11 物理和环境安全	8
11.1 安全区域	8
11.2 设备	8
11.2.1 设备安置和保护	8
11.2.2 支持性设施	8
11.2.3 布缆安全	8
11.2.4 设备维护	8
11.2.5 资产的移动	8
11.2.6 组织场所外的设备与资产安全	8
11.2.7 设备的安全处置或再利用	9
11.2.8 无人值守的用户设备	9
11.2.9 清理桌面和屏幕策略	9
12 运行安全	9
12.1 运行规程和责任	9
12.1.1 文件化的操作规程	9
12.1.2 变更管理	9
12.1.3 容量管理	9
12.1.4 开发、测试和运行环境的分离	9
12.2 恶意软件防范	9
12.3 备份	9
12.3.1 信息备份	9
12.4 日志和监视	10
12.4.1 事态日志	10
12.4.2 日志信息的保护	10
12.4.3 管理员和操作员日志	11
12.4.4 时钟同步	11
12.5 运行软件控制	11
12.6 技术方面的脆弱性管理	11
12.7 信息系统审计的考虑	11
13 通信安全	11
13.1 网络安全管理	11
13.2 信息传输	11
13.2.1 信息传输策略和规程	11
13.2.2 信息传输协议	11
13.2.3 电子消息发送	11
13.2.4 保密或不泄露协议	12
14 系统获取、开发和维护	12

中标华信认证中心（www.cshcc.cn） 内部使用翻译稿-20210317

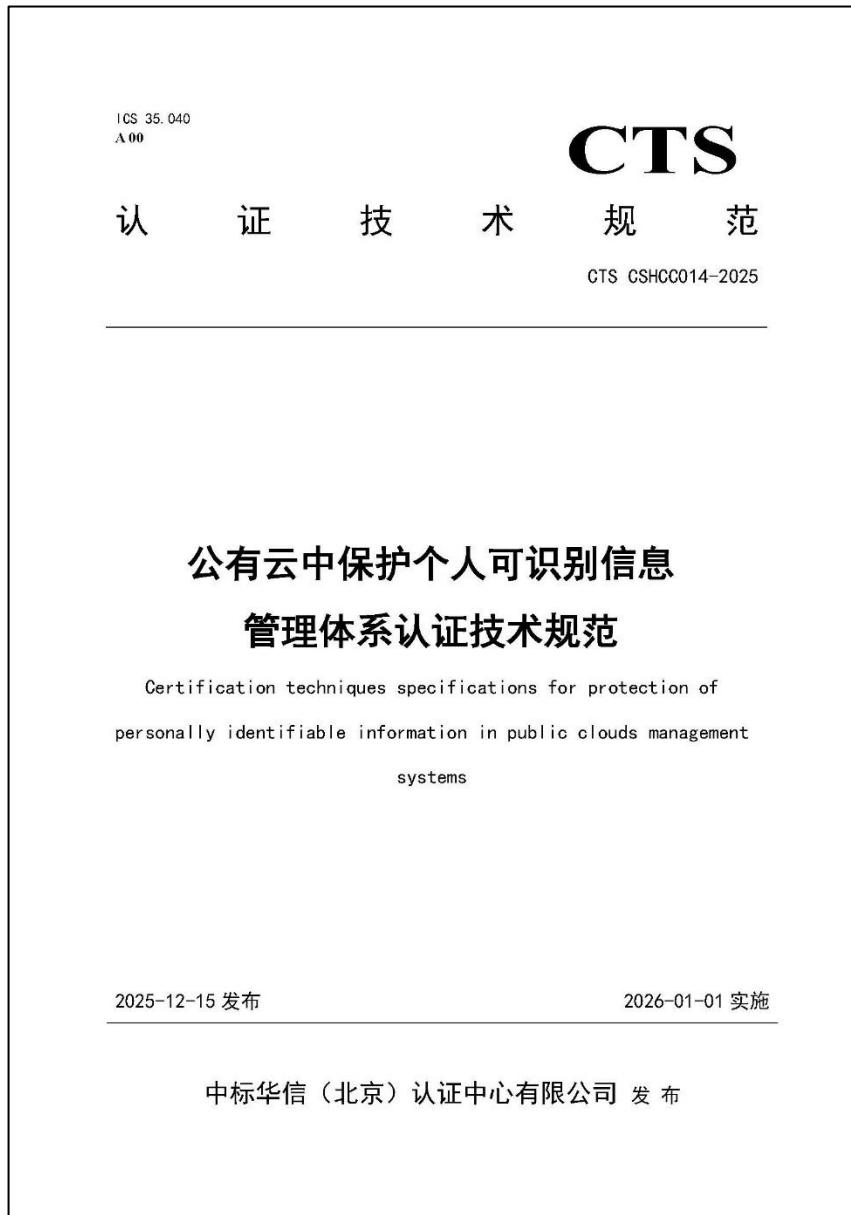
II

中标华信认证中心 内部使用翻译稿	
ISO/IEC27018:2019 信息技术 安全技术 作为PII处理者的公有云个人保护个人可识别信息(PII)的操作规范	
15 供应商关系	12
16 信息安全管理	12
16.1 信息安全事件的管理和改进	12
16.1.1 责任和规程	12
16.1.2 报告信息安全事态	12
16.1.3 报告信息安全弱点	12
16.1.4 信息安全事态的评估和决策	12
16.1.5 信息安全事件的响应	13
16.1.6 从信息安全事件中学习	13
16.1.7 证据的收集	13
17 业务连续性管理的信息安全方面	13
18 符合性	13
18.1 符合法律和合同要求	13
18.2 信息安全评审	13
18.2.1 信息系统的独立评审	13
18.2.2 符合安全策略和标准	13
18.2.3 技术符合性评审	13
附件 A (规范性) 用于PII保护的公有云中PII处理器扩展控制集	14
参考文献	21

中标华信认证中心（www.cshcc.cn） 内部使用翻译稿-20210317

IV

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息



CTS CSHCC014-2025
目 录
1 范围 6
2 规范性引用文件 6
3 术语和定义 6
4 组织环境 6
4.1 理解组织及其环境 6
4.2 理解相关方的需求和期望 6
4.3 确定管理体系范围 6
4.4 公有云中保护个人可识别信息管理体系 7
5 领导作用 7
5.1 领导作用和承诺 7
5.2 方针 7
5.3 组织角色、责任和权限 8
6 策划 8
6.1 应对风险和机遇的措施 8
6.1.1 总则 8
6.1.2 公有云中保护个人可识别信息风险评估 8
6.1.3 公有云中保护个人可识别信息风险处置 9
6.2 公有云中保护个人可识别信息目标及其策划的实现 10
6.3 变更的策划 10
7 支持 10
7.1 意识 10
7.2 资源 10
7.3 能力 11
7.4 沟通 11
7.5 文件化信息 11
7.5.1 总则 11
7.5.2 创建和更新 11
7.5.3 文件化信息的控制 12
8 运行 12
8.1 运行策划和控制 12
8.2 概述 12
8.2.1 内容结构 13
8.2.2 控制类别 14
8.3 信息安全策略 14
8.3.1 信息安全指导 14

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

CTS CSHCC014-2025

8.4 信息安全组织.....	15
8.4.1 内部组织.....	15
8.4.2 移动设备和远程工作.....	15
8.5 人力资源安全.....	15
8.5.1 任用前.....	15
8.5.2 任用中.....	15
8.5.3 任用的终止和变更.....	16
8.6 资产管理.....	16
8.7 访问控制.....	16
8.7.1 访问控制的业务需求.....	16
8.7.2 用户访问管理.....	16
8.7.3 用户责任.....	17
8.7.4 系统和应用访问控制.....	17
8.8 密码.....	18
8.8.1 密码控制.....	18
8.9 物理和环境安全.....	18
8.9.1 安全区域.....	18
8.9.2 设备.....	18
8.10 运行安全.....	19
8.10.1 运行程序和责任.....	19
8.10.2 防范恶意软件.....	20
8.10.3 备份.....	20
8.10.4 日志和监控.....	21
8.10.5 运行软件控制.....	21
8.10.6 技术方面的脆弱性管理.....	21
8.10.7 信息系统审计的考虑.....	22
8.11 通信安全.....	22
8.11.1 网络安全管理.....	22
8.11.2 信息传输.....	22
8.12 系统获取、开发和维护.....	22
8.13 供应商关系.....	22
8.14 信息安全事件管理.....	22
8.14.1 信息安全事件的管理和改进.....	22
8.15 业务连续性管理的信息安全方面.....	23
8.16 符合性.....	23
8.16.1 符合法律和合同要求.....	24
8.16.2 信息安全评审.....	24
9 绩效评价.....	24
9.1 监视、测量、分析和评价.....	24

CTS CSHCC014-2025

9.2 内部审核.....	25
9.2.1 总则.....	25
9.2.2 内部审核方案.....	25
9.3 管理评审.....	25
9.3.1 总则.....	25
9.3.2 管理评审输入.....	25
9.3.3 管理评审结果.....	26
10 改进.....	26
10.1 持续改进.....	26
10.2 不符合和纠正措施.....	26

中标华信(北京)认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

