

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-PIIPMS 个人身份信息保护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	标志样式
管理体系	其他管理体系	个人身份信息保护管理体系认证规则	CSHCC-RZGZ-PIIPMS	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 个人身份信息保护实施规范	ISO/IEC 29151:2017	国际标准化组织；国际电工委员会	20170818	见附页	个人身份信息保护管理体系认证证书	中标华信（北京）认证中心有限公司	见附页	不适用
									个人身份信息保护管理体系认证技术规范	CTS CSHCC013-2025	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-PIIPMS 个人身份信息保护管理体系认证规则及相关公示信息



## 个人身份信息保护管理体系认证规则

文件编号：CSHCC-RZGZ-PIIP

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-PIIP

个人身份信息保护管理体系认证规则

### 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. 认证证书状态管理 .....	11
7. 认证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-PIIPMS 个人身份信息保护管理体系认证规则及相关公示信息

INTERNATIONAL  
STANDARD

ISO/IEC  
29151

First edition  
2017-08

Information technology — Security  
techniques — Code of practice for  
personally identifiable information  
protection

*Techniques de l'information — Techniques de sécurité — Code de  
bonne pratique pour la protection des données à caractère personnel*



Reference number  
ISO/IEC 29151:2017(E)

© ISO/IEC 2017

ISO/IEC 29151:2017(E)

CONTENTS

	Page
1 Scope .....	1
2 Normative references .....	1
3 Definitions and abbreviated terms .....	1
3.1 Definitions .....	1
3.2 Abbreviated terms .....	1
4 Overview .....	2
4.1 Objective for the protection of PII .....	2
4.2 Requirement for the protection of PII .....	2
4.3 Controls .....	2
4.4 Selecting controls .....	2
4.5 Developing organization specific guidelines .....	3
4.6 Life cycle considerations .....	3
4.7 Structure of this Specification .....	3
5 Information security policies .....	4
5.1 Management directions for information security .....	4
6 Organization of information security .....	4
6.1 Internal organization .....	4
6.2 Mobile devices and teleworking .....	5
7 Human resource security .....	6
7.1 Prior to employment .....	6
7.2 During employment .....	6
7.3 Termination and change of employment .....	6
8 Asset management .....	7
8.1 Responsibility for assets .....	7
8.2 Information classification .....	7
8.3 Media handling .....	8
9 Access control .....	9
9.1 Business requirement of access control .....	9
9.2 User access management .....	9
9.3 User responsibilities .....	10
9.4 System and application access control .....	10
10 Cryptography .....	11
10.1 Cryptographic controls .....	11
11 Physical and environmental security .....	11
11.1 Secure areas .....	11
11.2 Equipment .....	12
12 Operations security .....	12
12.1 Operational procedures and responsibilities .....	12
12.2 Protection from malware .....	13
12.3 Backup .....	13
12.4 Logging and monitoring .....	13
12.5 Control of operational software .....	14
12.6 Technical vulnerability management .....	14
12.7 Information systems audit considerations .....	14
13 Communications security .....	15
13.1 Network security management .....	15
13.2 Information transfer .....	15
14 System acquisition, development and maintenance .....	15
14.1 Security requirements of information systems .....	15
14.2 Security in development and support processes .....	16

Rec. ITU-T X.1058 (03/2017) iii

ISO/IEC 29151:2017(E)

	Page
14.3 Test data .....	16
15 Supplier relationships .....	17
15.1 Information security in supplier relationships .....	17
15.2 Supplier service delivery management .....	18
16 Information security incident management .....	18
16.1 Management of information security incidents and improvements .....	18
17 Information security aspects of business continuity management .....	19
17.1 Information security continuity .....	19
17.2 Redundancies .....	19
18 Compliance .....	20
18.1 Compliance with legal and contractual requirements .....	20
18.2 Information security reviews .....	21
Annex A — Extended control set for PII protection (This annex forms an integral part of this Recommendation   International Standard) .....	22
A.1 General .....	22
A.2 General policies for the use and protection of PII .....	22
A.3 Consent and choice .....	22
A.4 Purpose legitimacy and specification .....	24
A.5 Collection limitation .....	26
A.6 Data minimization .....	26
A.7 Use, retention and disclosure limitation .....	27
A.8 Accuracy and quality .....	30
A.9 Openness, transparency and notice .....	31
A.10 PII principal participation and access .....	32
A.11 Accountability .....	34
A.12 Information security .....	37
A.13 Privacy compliance .....	37
Bibliography .....	39

iv Rec. ITU-T X.1058 (03/2017)

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-PIIPMS 个人身份信息保护管理体系认证规则及相关公示信息

第一版  
2017-08

国际标准

ISO/IEC  
29151

信息技术 - 安全技术 -  
个人身份信息保护实施规范  
信息技术-安全技术-个人信息保护和存储



参考编号 ISO/IEC  
29151:2017(E)

©ISO/IEC 2017

ISO/IEC 29151:2017(E)

目录

1	范围	14
2	规范性参考文献	14
3	定义和缩写	14
3.1	定义	14
3.2	缩写	14
4	概述	14
4.1	保护 PII 的目标	14
4.2	要求保护 PII	15
4.3	控制	15
4.4	选择控制	15
4.5	制定针对具体组织的指导方针	15
4.6	生命周期注意事项	16
4.7	本规范的结构	16
5	信息安全策略	16
5.1	信息安全指南	16
6	信息安全组织	16
6.1	内部组织	17
6.2	移动设备和远程办公	18
7	人力资源安全	18
7.1	聘用前	18
7.2	任职期间	18
7.3	雇佣关系的终止和变更	19
8	资产管理	19
8.1	资产的责任	19
8.2	信息分类	20
8.3	介质处理	20
9	访问控制	21
9.1	访问控制的业务需求	21
9.2	用户访问管理	21
9.3	用户责任	22
9.4	系统和应用程序的访问控制	22
10	加密技术	23
10.1	加密控制	23
11	物理和环境安全	23
11.1	安全区域	23
11.2	设备	23
12	运行安全	24
12.1	运行程序和责任	24
12.2	防止恶意软件	25
12.3	备份	25
12.4	日志和监控	25
12.5	运行软件的控制	26
12.6	技术调查管理	26
12.7	信息系统审计注意事项	26
13	通信安全	26
13.1	网络安全管理	26
13.2	信息传输	26
14	系统采购、开发和维护	27

iii

ISO/IEC 29151:2017(E)

14.1	信息系统的安全需求	27
14.2	开发和支持过程中的安全性	27
14.3	测试数据	28
15	供应商关系	28
15.1	供应商关系中的信息安全	28
15.2	供应商服务交付管理	29
16	信息安全事件管理	29
16.1	信息安全事件的管理和改进	29
17	业务连续性管理的信息安全方面	30
17.1	信息安全的连续性	30
17.2	冗余	30
18	合规性	31
18.1	遵守法律和合同要求	31
18.2	信息安全评估	31
<b>用于保护 PII 的扩展控制集</b>		<b>33</b>
(本附件是本标准   国际标准的组成部分)。		<b>33</b>

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-PIIPMS 个人身份信息保护管理体系认证规则及相关公示信息

ICS 35.040  
A 00

CTS

认 证 技 术 规 范

CTS CSHCC013-2025

个人身份信息保护管理体系  
认证技术规范

Certification techniques specifications for Personally  
identifiable information protection management systems

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

CTS CSHCC013-2025

目 录

1 范围 .....	6
2 规范性引用文件 .....	6
3 术语、定义和缩略语 .....	6
4 组织环境 .....	7
4.1 理解组织及其环境 .....	7
4.2 理解相关方的需求和期望 .....	7
4.3 确定管理体系范围 .....	7
4.4 个人身份信息保护管理体系 .....	7
5 领导作用 .....	7
5.1 领导作用和承诺 .....	7
5.2 方针 .....	8
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 个人身份信息保护风险评估 .....	9
6.1.3 个人身份信息保护风险处置 .....	9
6.2 个人身份信息保护目标及其策划的实现 .....	10
6.3 变更的策划 .....	10
7 支持 .....	10
7.1 资源 .....	10
7.2 能力 .....	11
7.3 意识 .....	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 .....	12
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 保护 PII 的目标 .....	13
8.2.2 要求保护 PII .....	13
8.2.3 控制 .....	13
8.2.4 选择控制 .....	13
8.2.5 制定适合组织的指导方针 .....	14
8.2.6 生命周期注意事项 .....	14
8.2.7 内容的结构 .....	14
8.3 信息安全策略 .....	15
8.3.1 信息安全管理指南 .....	15

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-PIIPMS 个人身份信息保护管理体系认证规则及相关公示信息

CTS CSHCC013-2025

8.4 信息安全组织.....	15
8.4.1 内部组织.....	15
8.4.2 移动设备和远程办公.....	17
8.5 人力资源安全.....	18
8.5.1 聘用前.....	18
8.5.2 任职期间.....	18
8.5.3 雇佣关系的终止和变更.....	19
8.6 资产管理.....	19
8.6.1 资产的责任.....	19
8.6.2 信息分类.....	20
8.6.3 介质处理.....	21
8.7 访问控制.....	22
8.7.1 访问控制的业务需求.....	22
8.7.2 用户访问管理.....	22
8.7.3 用户责任.....	23
8.7.4 系统和应用程序的访问控制.....	23
8.8 加密技术.....	24
8.8.1 加密控制.....	24
8.9 物理和环境安全.....	24
8.9.1 安全区域.....	24
8.9.2 设备.....	25
8.10 运行安全.....	26
8.10.1 运行程序和责任.....	26
8.10.2 防范恶意软件.....	27
8.10.3 备份.....	27
8.10.4 日志和监控.....	27
8.10.5 运行软件的控制.....	28
8.10.6 技术漏洞管理.....	28
8.10.7 信息系统审计注意事项.....	28
8.11 通信安全.....	29
8.11.1 网络安全管理.....	29
8.11.2 信息传输.....	29
8.12 系统采购、开发和 维护.....	30
8.12.1 信息系统的安全需求.....	30
8.12.2 开发和支持过程中的安全性.....	30
8.12.3 测试数据.....	31
8.13 供应商关系.....	31
8.13.1 供应商关系中的信息安全.....	31
8.13.2 供应商服务交付管理.....	32
8.14 信息安全事件管理.....	32
8.14.1 信息安全事件的管理和改进.....	33
8.15 业务连续性管理的 信息安全方面.....	34
8.15.1 信息安全的连续性.....	34
8.15.2 冗余.....	34

CTS CSHCC013-2025

8.16 合规性.....	35
8.16.1 遵守法律和合同要求.....	35
8.16.2 信息安全评审.....	36
9 绩效评价.....	36
9.1 监视、测量、分析和评价.....	36
9.2 内部审核.....	37
9.2.1 总则.....	37
9.2.2 内部审核方案.....	37
9.3 管理评审.....	37
9.3.1 总则.....	37
9.3.2 管理评审输入.....	37
9.3.3 管理评审结果.....	38
10 改进.....	38
10.1 持续改进.....	38
10.2 不符合和纠正措施.....	38



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-PIIPMS 个人身份信息保护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  
CSHCC.CN

## 个人身份信息保护管理体系认证证书

证书编号: XXXXXXXXXXXXXXXX

**兹证明**

**XXXXXXXXXX 有限公司**

统一社会信用代码: XXXXXXXXXXXXXXXX

注册地址: XXXXXXXXXXXXXXXX

办公地址: XXXXXXXXXXXXXXXX

生产地址: XXXXXXXXXXXXXXXX

**个人身份信息保护管理体系符合标准:**

ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实施规范》  
CTS CSHCC013-2025《个人身份信息保护管理体系认证技术规范》

通过认证的范围:

与 XXXXXXXX 相关的个人身份信息保护管理活动

本证书在国家规定的各行政许可、资质许可有效期内使用有效，  
在接受监督审核并经审核合格后，与证书下方二维码一并使用有效。

发证日期: XXXX-XX-XX      初次发证: XXXX-XX-XX  
有效期至: XXXX-XX-XX      换证日期: XXXX-XX-XX

签发: 

中标华信(北京)认证中心  
有限公司



 中心地址: 北京市石景山区石景山路3号玉泉大厦5层    中心电话: 010-88255986    中心邮编: 100049  
注: 证书详细信息可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn)  
及本机构网站 (www.cshcc.cn) 或扫描左侧二维码查询



中标华信(北京)认证中心  
CSHCC.CN

## Authentication Certificate of Personally Identifiable Information Protection Management Systems

Registration No. XXXXXXXXXXXXXXXX

**This is to certify that**

**XXXXXXXXXX LTD.**

Unified Social Credit Code: XXXXXXXXXXXXXXXX

Registered Address: XXXXXXXXXXXXXXXX

Office Address: XXXXXXXXXXXXXXXX

Production Address: XXXXXXXXXXXXXXXX

Personally Identifiable Information Protection Management Systems satisfy:

ISO/IEC 29151:2017 Information technology-Security techniques-  
Code of practice for personally identifiable information protection  
CTS CSHCC013-2025 Certification techniques specifications for  
Personally Identifiable Information Protection Management Systems

**The certificate is valid for the following scope:**

Personal identity information protection and management activities related to XXXXXXXX

This certificate is valid for use within the validity period of various administrative and  
qualification licenses stipulated by the state. It is valid when used together with the QR code below the certificate  
after undergoing supervision audit and passing the review.

Date of Issue: XXXX-XX-XX      Date of Initial Certification: XXXX-XX-XX  
Date of Expiry: XXXX-XX-XX      Date of Change: XXXX-XX-XX



China Standard Huaxin(Beijing)  
Certification Center Co.,Ltd.



 Address of Certification Authority: 5 Floor,YuQuan Building,No.3 Shijingshan Road,Shijingshan District,Beijing    Tel: 010-88255986    P.C.: 100049  
Note: The detailed information is available on the Certification and Accreditation Administration of the People's Republic of China official website  
(www.cnca.gov.cn) the authority's website(www.cshcc.cn) and the Quick Response Code on the left.