

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-PIIP 个人信息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	个人信息保护管理体系认证规则	CSHCC-RZGZ-PIIP	B1	修订	中标华信（北京）认证中心有限公司	20260601	自行制定	信息技术 安全技术 个人信息保护实施规范	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
									网络安全技术 信息安全管理体系 要求	GB/T 22080—2025/ISO/IEC27001:2022	国家市场监督管理总局；国家标准化管理委员会	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-PIIP 个人信息信息保护管理体系认证规则及相关公示信息



个人信息信息保护管理体系认证规则

文件编号：CSHCC RZGZ PIIP
文件版本：B1
编制：金鹏、李一辉
复核：江雪
审核：伍倩惠
批准：刘伯钊

2025-12-15 首次发布 2026-04-20 修订 2026-06-01 实施
中标华信（北京）认证中心有限公司 发布

目录

1 通用范围.....	4
2 认证依据.....	4
3 对认证机构的基本要求.....	4
4 对认证人员的基本要求.....	5
5 认证程序.....	6
5.1 认证申请.....	6
5.2 申请评审.....	7
5.3 认证合同及相关责任.....	8
5.4 审核方案和审核策划.....	9
5.4.1 审核方案.....	9
5.4.2 审核时间.....	9
5.4.3 多场所抽样方案.....	10
5.4.4 组建审核组.....	10
5.4.5 审核计划.....	11
5.5 实施审核.....	11
5.6 初次认证审核.....	12
5.6.1 总则.....	12
5.6.2 第一阶段审核.....	12
5.6.3 第二阶段审核.....	13
5.7 监督审核.....	13
5.8 再认证审核.....	14
5.9 特殊审核.....	14
5.9.1 扩大认证范围.....	14
5.9.2 变更前较长时间通知的审核.....	14
5.10 不符合项及其验证.....	15
5.11 审核报告.....	15

5.12 认证决定.....	16
6 认证证书和认证标志.....	17
6.1 解释.....	17
6.2 认证证书.....	18
6.3 认证标志.....	19
7 认证证书的暂停、撤销和注销.....	19
7.1 总则.....	19
7.2 认证证书的暂停.....	19
7.3 认证证书的撤销.....	20
7.4 认证证书的注销.....	20
8 申诉（投诉）处理.....	20
9 信息公开与报告.....	21
10 认证记录.....	21
11 其他.....	22
11.1 认证标准类别.....	22
11.2 内部审核.....	23
11.3 PMPMS 技术服务.....	23
11.4 认证数据安全.....	23
12 附则.....	23
附录 A 个人信息信息保护管理体系审核时间要求.....	25
附录 B 证书编号规则.....	26
修订记录.....	27

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-PIIP 个人信息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

Technologies 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

	<i>Page</i>
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)

	<i>Page</i>
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-PIIP 个人信息信息保护管理体系认证规则及相关公示信息



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	信息安全管理指南	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	技术漏洞管理	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	测试标准	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	信息安全审计	31
用于保护 PII 的扩展控制集		33
(本附件是本标准 国际标准的组成部分)。		33

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-PIIP 个人信息信息保护管理体系认证规则及相关公示信息

ICS 35.030
CCS L 80



中华人民共和国国家标准

GB/T 22080—2025/ISO/IEC 27001:2022
代替 GB/T 22080—2016

网络安全技术 信息安全管理体系 要求

Cybersecurity technology—Information security management systems—
Requirements

(ISO/IEC 27001:2022, Information security, cybersecurity and privacy
protection—Information security management systems—Requirements, IDT)

2025-06-30 发布 2026-01-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

GB/T 22080—2025/ISO/IEC 27001:2022

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 组织环境	1
4.1 理解组织及其环境	1
4.2 理解相关方的需求和期望	1
4.3 确定信息安全管理体系范围	2
4.4 信息安全管理体系	2
5 领导	2
5.1 领导和承诺	2
5.2 方针	2
5.3 组织的角色、责任和权限	2
6 规划	3
6.1 应对风险和机会的措施	3
6.2 信息安全目标及其实现规划	4
6.3 针对变更的规划	4
7 支持	4
7.1 资源	4
7.2 能力	4
7.3 意识	5
7.4 沟通	5
7.5 文件化信息	5
8 运行	6
8.1 运行策划和控制	6
8.2 信息安全风险评估	6
8.3 信息安全风险处置	6
9 绩效评价	6
9.1 监视、测量、分析和评价	6
9.2 内部审计	6
9.3 管理评审	7
10 改进	7

GB/T 22080—2025/ISO/IEC 27001:2022

10.1 持续改进	7
10.2 不符合与纠正措施	7
附录 A (规范性) 信息安全控制参考	9
参考文献	16

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-PIIP 个人信息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

个人信息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

个人信息信息保护管理体系符合标准:
GB/T 22080-2025/ISO/IEC 27001:2022
《网络安全技术 信息安全管理体系 要求》
ISO/IEC 29151:2017
《信息技术 安全技术 个人信息信息保护实施规范》

通过认证的范围:
与 XXXXXXXXXX 相关的个人信息信息保护管理活动
(适用性声明版本:XXXX)

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: *刘仰利*

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
XXXXXXXXXXXX LTD.
Unified Social Credit Code: XXXXXXXXXXXXXXXX
Registered Address: XXXXXXXXXXXXXXXX
Office Address: XXXXXXXXXXXXXXXX
Production Address: XXXXXXXXXXXXXXXX

Personally Identifiable Information Protection Management Systems satisfy:
GB/T 22080-2025/ISO/IEC 27001:2022 Cybersecurity technology—
Information security management systems—Requirements
ISO/IEC 29151:2017 Information technology—Security techniques—
Code of practice for personally identifiable information protection

The certificate is valid for the following scope:
Personal identifiable information protection and management activities related to XXXXXXXX
(Statement of Applicability: XXXX)

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

Prof Han Lin
General Manager

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.