

# 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-PIMS 隐私信息管理体系认证规则及相关公示信息

### 【前言】

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](mailto: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详见附件】

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	隐私信息管理体系认证规则	CSHCC-RZGZ-PIMS	A3	修订	中标华信（北京）认证中心有限公司	20260501	自行制定	安全技术-扩展 ISO/IEC 27001 和 ISO/IEC 27002 的隐私信息管理要求和指南	ISO/IEC 27701:2019	国际标准化组织；国际电工委员会	20190805	见附页	隐私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	不适用

# 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-PIMS 隐私信息管理体系认证规则及相关公示信息



### 隐私信息管理体系认证规则

文件编号: CSHCC RZGZ PIMS  
文件版本: A3  
编制: 金鹏、时小敏  
复核: 江雪  
审核: 伍倩惠  
批准: 刘伯钊

2021-01-27 首次发布    2026-04-20 修订    2026-05-01 实施  
中标华信（北京）认证中心有限公司 发布

CSHCC-RZGZ-PIMS

隐私信息管理体系认证规则

### 目录

1 适用范围	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 提前较长时间通知的审核	14
5.10 不符合项及其验证	15

中标华信（北京）认证中心有限公司

2 / 27


CSHCC-RZGZ-PIMS

隐私信息管理体系认证规则

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 总则	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	23
11.1 认证标准换版	23
11.2 内部审核	23
11.3 PIMS 技术服务	23
11.4 认证数据安全	23
12 附则	23
附录 A PIMS 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

3 / 27

INTERNATIONAL STANDARD		ISO/IEC 27701	ISO/IEC 27701:2019(E)
		First edition 2019-08	
<b>Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines</b>			
<i>Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices</i>			
		Reference number ISO/IEC 27701:2019(E)	
		© ISO/IEC 2019	
Provided by IIS Markt under license with ANZI			
			<b>Contents</b>
			Page
			<b>Foreword</b> .....vi
			<b>Introduction</b> .....vii
			<b>1 Scope</b> .....1
			<b>2 Normative references</b> .....1
			<b>3 Terms, definitions and abbreviations</b> .....1
			<b>4 General</b> .....2
			4.1 Structure of this document.....2
			4.2 Application of ISO/IEC 27001:2013 requirements.....2
			4.3 Application of ISO/IEC 27002:2013 guidelines.....3
			4.4 Customer.....4
			<b>5 PIMS-specific requirements related to ISO/IEC 27001</b> .....4
			5.1 General.....4
			5.2 Context of the organization.....4
			5.2.1 Understanding the organization and its context.....4
			5.2.2 Understanding the needs and expectations of interested parties.....5
			5.2.3 Determining the scope of the information security management system.....5
			5.2.4 Information security management system.....5
			5.3 Leadership.....5
			5.3.1 Leadership and commitment.....5
			5.3.2 Policy.....5
			5.3.3 Organizational roles, responsibilities and authorities.....5
			5.4 Planning.....6
			5.4.1 Actions to address risks and opportunities.....6
			5.4.2 Information security objectives and planning to achieve them.....7
			5.5 Support.....7
			5.5.1 Resources.....7
			5.5.2 Competence.....7
			5.5.3 Awareness.....7
			5.5.4 Communication.....7
			5.5.5 Documented information.....7
			5.6 Operation.....7
			5.6.1 Operational planning and control.....7
			5.6.2 Information security risk assessment.....7
			5.6.3 Information security risk treatment.....7
			5.7 Performance evaluation.....8
			5.7.1 Monitoring, measurement, analysis and evaluation.....8
			5.7.2 Internal audit.....8
			5.7.3 Management review.....8
			5.8 Improvement.....8
			5.8.1 Nonconformity and corrective action.....8
			5.8.2 Continual improvement.....8
			<b>6 PIMS-specific guidance related to ISO/IEC 27002</b> .....8
			6.1 General.....8
			6.2 Information security policies.....8
			6.2.1 Management direction for information security.....8
			6.3 Organization of information security.....9
			6.3.1 Internal organization.....9
			6.3.2 Mobile devices and teleworking.....10
			6.4 Human resource security.....10
			6.4.1 Prior to employment.....10
			6.4.2 During employment.....10
			6.4.3 Termination and change of employment.....11
			© ISO/IEC 2019 - All rights reserved
			iii
			Provided by IIS Markt under license with ANZI

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-PIMS 隐私信息管理体系认证规则及相关公示信息

ISO/IEC 27701:2019(E)

6.5	Asset management	11
6.5.1	Responsibility for assets	11
6.5.2	Information classification	11
6.5.3	Media handling	12
6.6	Access control	13
6.6.1	Business requirements of access control	13
6.6.2	User access management	13
6.6.3	User responsibilities	14
6.6.4	System and application access control	14
6.7	Cryptography	15
6.7.1	Cryptographic controls	15
6.8	Physical and environmental security	15
6.8.1	Secure areas	15
6.8.2	Equipment	16
6.9	Operations security	17
6.9.1	Operational procedures and responsibilities	17
6.9.2	Protection from malware	18
6.9.3	Backup	18
6.9.4	Logging and monitoring	18
6.9.5	Control of operational software	19
6.9.6	Technical vulnerability management	20
6.9.7	Information systems audit considerations	20
6.10	Communications security	20
6.10.1	Network security management	20
6.10.2	Information transfer	20
6.11	Systems acquisition, development and maintenance	21
6.11.1	Security requirements of information systems	21
6.11.2	Security in development and support processes	21
6.11.3	Test data	23
6.12	Supplier relationships	23
6.12.1	Information security in supplier relationships	23
6.12.2	Supplier service delivery management	24
6.13	Information security incident management	24
6.13.1	Management of information security incidents and improvements	24
6.14	Information security aspects of business continuity management	27
6.14.1	Information security continuity	27
6.14.2	Redundancies	27
6.15	Compliance	27
6.15.1	Compliance with legal and contractual requirements	27
6.15.2	Information security reviews	28
7	<b>Additional ISO/IEC 27002 guidance for PII controllers</b>	29
7.1	General	29
7.2	Conditions for collection and processing	29
7.2.1	Identify and document purpose	29
7.2.2	Identify lawful basis	29
7.2.3	Determine when and how consent is to be obtained	30
7.2.4	Obtain and record consent	30
7.2.5	Privacy impact assessment	31
7.2.6	Contracts with PII processors	31
7.2.7	Joint PII controller	32
7.2.8	Records related to processing PII	32
7.3	Obligations to PII principals	33
7.3.1	Determining and fulfilling obligations to PII principals	33
7.3.2	Determining information for PII principals	33
7.3.3	Providing information to PII principals	34
7.3.4	Providing mechanism to modify or withdraw consent	34
7.3.5	Providing mechanism to object to PII processing	35
7.3.6	Access, correction and/or erasure	35

iv  
Provided by IHS Markit under license with ANSI

© ISO/IEC 2019 - All rights reserved

ISO/IEC 27701:2019(E)

7.3.7	PII controllers' obligations to inform third parties	36
7.3.8	Providing copy of PII processed	36
7.3.9	Handling requests	37
7.3.10	Automated decision making	37
7.4	Privacy by design and privacy by default	38
7.4.1	Limit collection	38
7.4.2	Limit processing	38
7.4.3	Accuracy and quality	38
7.4.4	PII minimization objectives	39
7.4.5	PII de-identification and deletion at the end of processing	39
7.4.6	Temporary files	39
7.4.7	Retention	40
7.4.8	Disposal	40
7.4.9	PII transmission controls	40
7.5	PII sharing, transfer, and disclosure	41
7.5.1	Identify basis for PII transfer between jurisdictions	41
7.5.2	Countries and international organizations to which PII can be transferred	41
7.5.3	Records of transfer of PII	41
7.5.4	Records of PII disclosure to third parties	42
8	<b>Additional ISO/IEC 27002 guidance for PII processors</b>	42
8.1	General	42
8.2	Conditions for collection and processing	42
8.2.1	Customer agreement	42
8.2.2	Organization's purposes	43
8.2.3	Marketing and advertising use	43
8.2.4	Infringing instruction	43
8.2.5	Customer obligations	43
8.2.6	Records related to processing PII	44
8.3	Obligations to PII principals	44
8.3.1	Obligations to PII principals	44
8.4	Privacy by design and privacy by default	44
8.4.1	Temporary files	44
8.4.2	Return, transfer or disposal of PII	45
8.4.3	PII transmission controls	45
8.5	PII sharing, transfer, and disclosure	46
8.5.1	Basis for PII transfer between jurisdictions	46
8.5.2	Countries and international organizations to which PII can be transferred	46
8.5.3	Records of PII disclosure to third parties	47
8.5.4	Notification of PII disclosure requests	47
8.5.5	Legally binding PII disclosures	47
8.5.6	Disclosure of subcontractors used to process PII	47
8.5.7	Engagement of a subcontractor to process PII	48
8.5.8	Change of subcontractor to process PII	48
	<b>Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)</b>	49
	<b>Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors)</b>	53
	<b>Annex C (informative) Mapping to ISO/IEC 29100</b>	56
	<b>Annex D (informative) Mapping to the General Data Protection Regulation</b>	58
	<b>Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151</b>	61
	<b>Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002</b>	64
	<b>Bibliography</b>	66

© ISO/IEC 2019 - All rights reserved

v

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-PIMS 隐私信息管理体系认证规则及相关公示信息

国际  
标准

ISO/IEC  
27701

安全技术 – 扩展  
ISO/IEC27001 和  
ISO/IEC27002 的  
隐私信息管理 要求和指南



Reference number  
ISO/IEC 27700:2023(E)

© ISO/IEC 2023

目录

前言	4
引言	5
0.1 总则	5
0.2 与其他管理体系标准的兼容性	5
1 范围	5
2 规范性引用文件	6
3 术语、定义和缩略语	6
3.1 联合 PII 控制者	6
3.2 隐私信息管理体系 PIMS	6
4 总则	6
4.1 本文档的结构	6
4.2 ISO/IEC 27001:2013 要求的应用	7
4.3 ISO/IEC 27002:2013 的指南应用	8
4.4 顾客	8
5 与 ISO/IEC 27001 相关的具体要求	9
5.1 总则	9
5.2 组织环境	9
5.3 领导	10
5.4 计划	10
5.5 支持	11
5.6 运行	12
5.7 绩效评价	12
5.8 改进	12
6 与 ISO/IEC 27002 相关的 PIMS 具体指南	12
6.1 总则	12
6.2 信息安全策略	13
6.3 信息安全组织	13
6.4 人力资源安全	14
6.5 资产管理	15
6.6 访问控制	17
6.7 密码	18
6.8 物理和环境安全	19
6.9 运行安全	20
6.10 通信安全	22
6.11 系统获取、开发和维护	23
6.12 供应商关系	25
6.13 信息安全事件管理	26
6.14 业务连续性管理的信息安全方面	28
6.15 符合性	29
7 PII 控制者附加的 ISO/IEC27002 指南	30

7.1 总则	30
7.2 收集和处理的条件	30
7.3 对 PII 主体的义务	34
7.3.10 自动化决策	37
7.4 设计隐私和默认隐私	38
7.5 PII 分享、转移与披露	40
8 PII 处理者附加的 ISO/IEC 27002 指南	42
8.1 总则	42
8.2 收集和处理的条件	42
8.3 对 PII 主体的义务	44
8.4 涉及隐私和默认隐私	44
8.5 PII 分享、转移与披露	45
附录 A	48
附录 B	51
附录 C	54
附录 D	59
附录 E	64
参考文献	71

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-PIMS 隐私信息管理体系认证规则及相关公示信息

