ICS 03.100.99
CCS 00.01

团 体 标 准

T/JAS 11—2023

检验检测机构 检验业务信息化安全管理规范

Inspection body and laboratory--Inspection Business Informatization Security Management Specification

（征求意见稿）

2023-**-**发布 2023-**-**实施

吉林省标准化协会 发布

前　言

本文件按照GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起。

本文件由吉林省标准化协会提出并归口。

本文件起草单位：吉林省标准化协会。

本文件主要起草人：高明智、薛 雪、刘化冰、张琳琳、张晶书、康文欣、贾 俊、宫国强、吕 航、郑丹丹、杨 帆、李赫然、丛月梅、谷 乐、臧英男、周明明。

本文件于2023年**月**日首次发布。

检验检测机构 检验业务信息化安全管理规范

1 范围

本文件规定了检验检测机构实验室信息管理系统安全管理的术语和定义、基本要求、机房安全管理、设备安全管理、网络安全管理、计算机软件安全管理、计算机数据安全管理和实验室信息管理系统（Lims）安全管理等内容。

本文件适用于检验检测机构检验业务信息安全管理工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

RB/T 028 实验室信息管理系统管理规范

RB/T 214 检验检测机构资质认定能力评价 检验检测机构通用要求

3 术语和定义

RB/T 028、RB/T 214界定的以及下列术语和定义适用于本文件。

3.1

检验检测机构 Inspection body and laboratory

依法成立，依据相关标准或者技术规范，利用仪器设备、环境设施等技术条件和专业技能，对产品或者法律法规规定的特定对象进行检验检测的专业技术组织。

3.2

信息化安全 Information security

信息化安全是指对信息系统的硬件、软件以及数据信息实施安全防护，保证在意外事故或恶意攻击情况下系统不会遭到破坏，敏感数据信息不会被篡改和泄漏，保证信息的机密性、完整性、可用性和可控性，并保证系统能够正常运行，信息服务功能不中断。

3.3

实验室信息管理系统 Laboratory information management system；LIMS

由计算机及其相关配套设备、设施(含网络)和软件构成,以实现实验室获得的数据和信息(包括计算机及非计算机系统保存的)管理,具有根据实验室管理规则对数据和信息进行采集、记录、报告、存储传输、检索、统计、分析等处理功能。

4 基本要求

4.1 检验检测机构应按照相关法规和标准要求建立检验业务信息化安全管理制度，加强数据和信息在采集、记录、存储、传输、统计等环节的安全管理，采取有效的技术和管理措施，保护核心数据和业务信息；明确设备使用、维护、定期核查等要求，避免数据和信息的泄露、数据丢失或被篡改等安全风险。

4.2 检验检测机构应配置满足实验室活动的数据采集器、数据存储介质、服务器、网络、软件、机房等保障系统安全运行必备的设备和设施。

4.3 检验检测机构应配备检验业务信息化专职管理人员，负责日常运行维护、监控及故障问题处理、意外事件处理、安全防护的管理等工作。

5 机房安全管理

5.1 检验检测机构应指定专人负责机房日常运行维护管理。严禁非机房管理人员进入机房，特殊情况需经上级领导批准，并填写《机房出入人员登记表》（可参考附录 A）后方可进入。机房管理员工作岗位变动时，应向接任的负责人办理书面移交手续。

5.2 机房网络管理员负责机房硬件和软件管理，负责维护保养机房中计算机及辅助设备确保正常运转。定期检查 UPS 设备，在外部供电意外中断和恢复时，能够保证网络设备安全运行。妥善保管机房专用设备的保修、维修、使用说明书等资料以及软件、驱动、备用件、消耗材料等。

5.3 机房应整洁有序，温度、湿度和通风状况等要满足机房内设备正常运转需要。机房管理员应定期检查火警监测系统是否工作正常，灭火设施是否有效。机房内不得存放易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品。

5.4 严谨使用机房计算机操作与工作无关的事情，做好计算机病毒查杀。

6 设备安全管理

6.1 计算机设备

6.1.1 实验室计算机设备的操作应该规范进行，未经授权同意，个人不得擅自将私有或外来的零件、配件、设备，加入到本单位的办公计算机设备或网络中。非本单位的计算机在未经批准的情况下，一律不得进入本单位网络。新电脑或设备需接入本单位网络时应检查机器，杀毒后方可入网，未经批准不得修改 IP 地址。

6.1.2 进入本实验室局域网内的计算机，未经批准不得擅自安装未经认可的软件；严禁安装游戏、娱乐及违反法律法规，危害安全的软件。

6.1.3 计算机中如有涉及本单位的关键信息应采取保密措施，操作密码要定期更改，如发现失、泄密现象应及时上报。任何人未经保管人同意，不得使用他人的电脑。使用人在离开前应退出系统或关机，确保计算机信息的安全。

6.1.4 计算机应按照杀毒软件，工作用 U 盘、移动硬盘在使用前，必须进行病毒扫描确保无病毒。

6.2 检验设备

6.2.1 检验设备需要连接网络的，需采用内网或加密方式，防止无关人员访问实验室检验设备，保证设备数据安全。

6.2.2 检验设备需安装杀毒软件，并定期对软件进行升级和更新，以防范病毒入侵和传播。

6.2.3 检验设备的软件、数据等信息禁止非法拷贝，以防止信息泄漏和丢失。使用的移动存储介质需要经过授权并杀毒后才能使用，防止病毒的传播和数据丢失。

6.2.4 检验设备中的重要数据需要定期备份，以防止数据丢失和灾难性损坏。同时对备份数据要进行安全加密，以防止数据泄漏和非法访问。

6.3 网络设备和设施

网络设备和设施应指派专人负责运行维护，使用人员不应私自变更位置或拆卸维修。

7 网络安全管理

严禁通过互联网应用程序（如：邮件、网站、软件、APP等其他相关方式）发布、复制、查阅和传播违反宪法和法律、行政法规的信息。需要在网站或相关平台发布本单位相关信息时，应按照本单位审批制度执行。

8 计算机软件安全管理

8.1 检验检测机构计算机软件首次使用应进行技术性验收和安全性确认，并做好验收记录（可参考附录 B）；软件的调整或二次开发也应进行验收和确认。

8.2 检验检测人员采用计算机软件进行计算和数据转换时，应定期检查，发现异常应及时查清原因并予以纠正。

8.3 计算机软件登录密码应定期更换，不应存在弱密码、默认密码或未设置密码的情况。

9 计算机数据安全管理

9.1 本规范所指的计算机数据，是指由计算机（服务器）及其相关的配套设备、网络进行采集、加工存储、传输和检测等处理得到的信息。

9.2 实验室应指定专人负责重要电子文件和数据（如相关检测/校准数据、记录，文档表格等）定期备份，避免数据丢失；对传递应予保密的数据，应通过符合保密要求的方式进行。

10 实验室信息管理系统（Lims）安全管理

10.1 实验室应设置 Lims 系统管理员，负责实验室信息管理系统的安装、调试、检查等工作，并经批准后在系统中给相关使用人员设置和变更系统使用权限。系统管理员应根据维护情况及时填写相关记录（可参考附录 C）

10.2 不得使用他人账号登录系统操作。若有人员变动，如离职、调岗、调离等情况应及时通知系统管理员，经批准后在系统中对相应的账户进行调整。

10.3　实验室信息管理系统不应随意向他人展示。外来人员参观系统运行情况，须经主管领导批准，由系统管理员现场演示，并做好数据保密工作。

10.4　系统使用人员应按照系统管理员的要求，安装符合本实验室信息管理系统对应版本的软件程序，不得随意安装其它版本。

附　录　A
（资料性附录）
机房出入人员登记表

机房出人人员登记表见 A.1

表A.1　机房出人人员登记表

姓名	进入机房时间	离开机房时间	事由	同行人员	备注

附　录　B
（资料性附录）
软件验收记录表

软件验收记录见表B.1

表B.1　软件验收记录表

软件名称		版本	
生厂商名称		联系人、电话	
验收情况			
验收结果及处里意见			
备注			

验收部门：　　验收人：　　验收时间

附 录 C
（资料性附录）
实验室信息管理系统维护记录表

实验室信息管理系统维护记录见表C.1

表C.1 实验室信息管理系统维护记录表

序号	维护日期	维护内容	操作人	备注

参 考 文 献

[1] GB 50174 数据中心设计规范
[2] GB/T 20269 信息安全技术 信息系统安全管理要求
[3] GB/T 25069 信息安全技术 术语
[4] GB/T 31496 信息技术 安全技术 信息安全管理体系 指南
[5] GB/T 39204 信息安全技术 关键信息基础设施安全保护要求