ICS 35.240.99
B 20

LS

中华人民共和国粮食行业标准

LS/T 1807—2017

粮食信息安全技术规范

Security specification for grain information system

2017-03-10 发布　　2017-06-01 实施

国　家　粮　食　局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家粮食局提出。

本标准由全国粮油标准化技术委员会(SAC/TC 270)归口。

本标准起草单位:航天信息股份有限公司、湖北省粮食局、北京天融信科技股份有限公司。

本标准主要起草人:李其均、宋玉玲、罗秀春、施展、王千喜、周贵来。

粮食信息安全技术规范

1 范围

本标准规定了粮食信息安全保护对象、粮食信息安全技术及安全管理的基本要求。部署在电子政务外网的相关安全建设由电子政务外网保障，部署在电子政务内网的相关安全建设由电子政务内网保障。本标准重点阐述的是各级粮食行政管理部门、粮食企业及其他涉粮机构在企业内部网、互联网交互时的安全要求。

本标准适用于粮食信息化项目的规划、设计、建设、运维和评估。

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。

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全域 security domain

同一环境内有相同的安全保护需求、相互信任、并具有相同的安全访问控制和边界控制策略的网络或系统。

3.2

粮食云计算平台 grain cloud computing platform

云计算基础设施和其上运行的粮食信息化软件的集合。

3.3

粮食物联网 grain internet of things

通过专用传感器对储粮环境和粮食的数量、质量进行在线监测的传感器网络系统。

4 缩略语

下列缩略语适用于本文件。

VPN：虚拟专用网络(Virtual Private Network)

PKI/CA：公钥基础设施/认证中心(Public Key Infrastructure/Certificate Authority)

4A：统一安全管理的身份认证、授权、审计和账号(Authentication，Account，Authorization，

Audit)

5 信息安全保护对象

主要包括粮食信息网络、信息系统、粮食信息及其物理环境、支撑性基础设施与安全设备设施等。

5.1 信息网络

被保护网络对象包括粮食业务管理范围内的各个信息网络，分别运行于电子政务内网、电子政务外网、企业内部网、互联网四个不同的网络中。

5.2 信息系统

被保护业务对象是粮食信息系统中运行的各类粮食业务应用系统，粮食信息系统按业务应用类型分为粮食企业业务管理应用系统和粮食行政管理应用系统；按照架构分为国家级粮食管理平台（简称“国家级平台”）、省级粮食管理平台（简称“省级平台”）、企业粮食管理平台。粮食企业业务管理应用系统运行在企业内网、互联网；粮食行政管理应用系统，分别运行在电子政务内网、电子政务外网和互联网。

5.3 粮食信息

被保护的信息对象是各类粮食业务信息，可分为公开信息和非公开信息，非公开信息中包含各类敏感信息。不同的信息类别，应设定不同的安全保护等级措施。

对于公开信息，主要是防篡改、防丢失；对于敏感信息，除防篡改、防丢失外，还需增加防止未经授权的披露、滥用和销毁。

5.3.1 公开信息

包括但不限于：

粮食生产、粮食加工、粮油市场、粮食消费、储粮环境、社会经济等信息。

5.3.2 粮食敏感信息

包括但不限于：

a) 应该公开，但正式发布前不宜泄漏的信息，如招投标、规划、统计、预算等过程信息；
b) 粮食行政执法过程中生成的不宜公开的记录文件；
c) 粮食企业的地理位置信息；
d) 粮食企业的商业秘密；
e) 粮食行政管理部门的人事规划和工作章程，人员能力评价等信息；
f) 售粮人银行卡、身份证、结算资金等信息；
g) 粮食库存量、质量、轮换计划、粮食应急预案等信息。

6 总体要求

从安全管理、安全技术、粮食专业领域安全技术三个方面提出粮食信息系统的安全要求，其架构如图1所示。

粮食行政管理部门、粮食企业和其他涉粮机构应按照国家信息安全主管部门的要求对粮食信息系统进行定级，并根据定级情况达到相应的安全要求。粮食企业业务管理应用系统应符合GB/T 22240

国家信息安全保护等级二级或二级以上标准，跨省或覆盖全省的粮食行政管理应用系统，应符合安全保护等级三级标准。

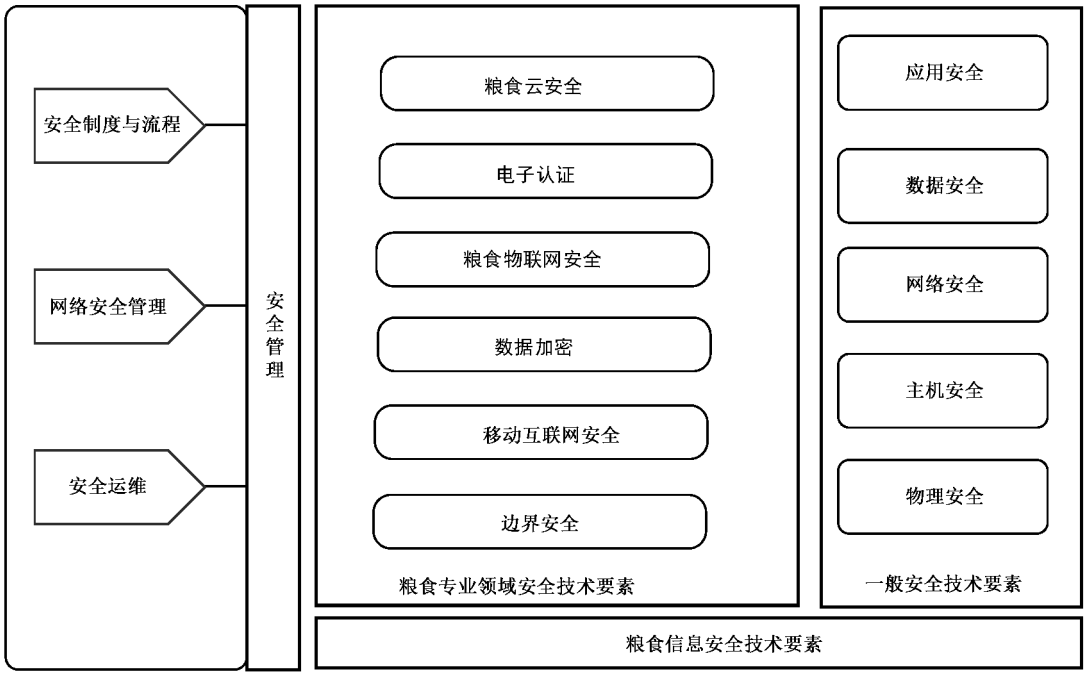

图 1　粮食信息安全框架

7　安全管理

安全管理的制度、机构、人员、系统建设、运维服务等，应符合 GB/T 22239、GB/T 22240 的要求。

8　安全技术

粮食信息系统的安全技术应符合 GB/T 22239、GB/T 22240 的通用要求外，还应满足以下技术要求。

8.1　物理安全

8.1.1　办公场地改造的机房

针对收纳库、中心库等粮食企业从办公场地改建的机房，至少应具备：

a）　机房和办公场地应具有防风、防雨的设计；

b）　空调水管安装不得穿过机房房顶或活动地板下；

c）　应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

d）　应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

e）　机房建筑应设置避雷装置；

f）　供电电源应具有良好接地；

g）　应具有防盗窃、防破坏的监控报警装置和安全管理措施；

h）　机房应设置灭火器材；

i）　电源线和通信缆应隔离铺设，避免互相干扰；

j) 收储企业的备用电力供应，至少应满足收购业务在断电情况下的正常运行；
k) 应保持机房和办公场地的干净卫生，计算机设备灰尘较多时，应采取负压清理方式，灰尘较少时，可采用普通清理方式；
l) 配线架、服务器机架应有显著的标识；
m) 独立机房可配置电子门禁系统，控制、鉴别和记录进入的人员。

8.1.2 仓房外的强电、弱电机柜

包括但不限于：
a) 应有良好的防雨设计；
b) 应具有漏电、过载、短路保护装置；
c) 应对机柜内的线缆、开关或其他控制单元有显著的标识，通过标识，可追溯相关图纸、检修记录、责任人等。

8.2 网络安全

8.2.1 库区网络布线

包括但不限于：
a) 粮库内网网络的综合布线宜采用光纤环网等可靠的网络链路；
b) 应在每个仓房门口设置一个信息节点；
c) 信息节点应安装在仓房外的防水防尘的弱电箱内。

8.2.2 结构安全

包括但不限于：
a) 与省级管理平台连接的企业，应有固定的 IP 地址；
b) 应绘制与当前运行情况相符的网络拓扑结构图；
c) 应保证接入网络和核心网络的带宽满足业务高峰期需要，如远程视频监管的需要；
d) 应根据业务类别、重要性和所涉及信息程度等因素，划分不同子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
e) 重要网段不得直接连接外部信息系统，重要网段与其他网段之间应采取可靠的技术隔离手段。

8.2.3 访问控制

包括但不限于：
a) 应利用网闸、VPN、防火墙等技术确定外部边界，实现安全可靠的外部网络互联；
b) 应利用身份认证技术实现分层管理，将内部安全域的信息分等级划分，禁止低安全域的用户/业务非授权访问高安全域用户/业务；
c) 应具备网络性能保护机制，防止对网络资源的滥用，确保网络资源的合理使用；
d) 应具备网络接入认证的能力，确保只有授权的终端才能接入网络。

8.2.4 安全审计

应对网络系统中的网络设备运行状况、网络流量、用户行为进行审计。

8.2.5 入侵防范

应在网络边界防范端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、网络蠕虫等攻击

行为。

8.3 主机安全

应符合 GB/T 22240 的要求。

8.4 数据安全

包括但不限于：

a) 粮食企业的业务数据应至少保存一个储粮周期且不少于 5 年；相关政策有要求的，还应满足相关政策文件要求；
b) 存储空间不足时，应逐步删除视频数据，保留业务数据；
c) 应具有本地的数据备份，在粮食轮换期应增加备份次数，备份介质应场地外存放；
d) 应加强备份介质的安全管理。

8.5 应用安全

包括但不限于：

a) 粮食信息系统应实现基于粮食行业 PKI/CA 数字证书体系的用户身份认证，并要求实现 4A 的应用系统安全体系，确保本地应用系统的信息安全；
b) 应根据人员的岗位职责，授予不同账户为完成各自承担任务所需的最小权限，并在他们之间形成相互制约的关系；
c) 应及时删除或禁用多余账号、测试账号、过期账号，避免共享账号、过期账号的使用。

9 粮食专业领域安全技术

9.1 粮食物联网安全

粮食物联网的设计和实施，除了应遵循一般的物理安全、主机安全、网络安全、数据安全和应用安全的技术要求外，其安全性还应具有：

a) 感知节点应通过接口，通过身份认证和授权访问，确认其身份真实性和正确性，以及访问控制的准确性后，才能接入到网络中；
b) 大型粮库、粮油加工企业或物流中心，可采用工业防火墙、网闸等设备对粮食业务管理网络和工业控制网络进行逻辑隔离；
c) 对于出入库数据录入数据的变更，不能以超级用户或其他高权限用户直接操作数据库修改，系统应提供完整的变更流程，记录数据录入、审核、变更的全过程信息，并形成数据变更报表；
d) 应当遵循客观性原则，不得修改、伪造粮食物联网的原始采集数据；
e) 粮食物联网系统应保留操作日志、访问日志，通过审计人员账户、访问时间、操作内容等日志信息，追踪定位非授权访问行为；
f) 系统日志应能记录设备的现场手动操作，与远程操作日志结合，形成完整的设备操作日志；
g) 粮食信息化技术支撑单位远程或本地进行系统升级时，应制定变更计划，明确变更时间、变更内容、变更验证、变更责任人等事项，应对原有版本和当前版本软件、数据备份到物理介质，并留有相关记录。

9.2 粮食云安全

9.2.1 云计算平台的使用范围

包括但不限于：

a) 对于涉密的粮食信息系统，信息的处理、保存、传输、利用应按照国家保密法规执行，不得使用政务云或其他公有云服务平台[GB/T 31167—2014 中的优先级确定]；
b) 涉及粮食信息敏感信息程度较多的信息系统或关键业务系统，可采用社区云或私有云计算平台，也可按照传统方式自建系统运行；
c) 交通偏远、网络通信条件差的基层收纳点，采用云计算平台，应确保网络中断后，还有备用的技术手段和措施，完成各环节的信息采集和业务处理，不影响粮食收购业务。

9.2.2 云计算的安全责任认定

粮食信息化平台迁入云计算平台后，其安全责任并未转移，仍需承担云计算平台上的数据和业务的最终安全责任[GB/T 31167—2014 中的云计算服务安全管理基本要求]。

9.2.3 云服务商的选择

包括但不限于：
a) 对于拟迁入云计算平台的系统，应对其信息和业务进行分析，按照信息的敏感程度和业务的重要程度选择相应安全能力水平的云服务商；
b) 粮食云计算客户应通过合同明确云服务商的责任和义务，强调客户对数据和业务系统运行状态的知情权；应要求云计算平台提供必要的监管接口和日志查询功能，建立有效的审查、检查机制，实现对云计算服务的有效监管。

9.2.4 云计算平台客户端的安全要求

粮食云客户应管控自身的客户端系统，应：
a) 不得向云计算平台和相关系统传送恶意程序，垃圾数据，以及其他可能影响云计算正常运行的代码；
b) 不得对云计算平台进行网络攻击、窃取或篡改数据资料；
c) 不得通过云平台从事违背国家信息安全的非法活动。

9.2.5 云平台的安全威胁

包括但不限于：
a) 粮食云服务环境下，需具备应对处理传统信息安全威胁的技术手段和措施，包括主机安全威胁、网络安全威胁、以及应用安全威胁；
b) 应处理虚拟化带来的新的安全威胁，包括虚拟化平台、虚拟机与虚拟机的网络管理、租户与租户之间的安全隔离；
c) 云计算模式下，云计算的设施层(物理环境)、硬件层(物理设备)、资源抽象层和控制层都处于云服务商的完全控制之下，所有安全设施由云服务商承担，对其安全性要求，应按照 GB/T 31168—2014 执行。应用软件层、软件平台层的安全保障措施，和传统信息安全保障措施相同。

9.3 移动互联网安全

移动互联网应用带来的安全风险，应从移动终端安全、移动应用安全、敏感信息防泄漏等方面防范。

9.3.1 移动终端安全

应对涉粮的移动终端进行全生命周期管理，其安全性要求如下：
a) 对移动终端的系统功能进行限制；

b) 建立领用登记、归还制度；
c) 涉粮应用在检测到运行环境处于越狱或 ROOT 等非安全环境时，应及时提出安全警示，必要时可以终止运行；
d) 应支持远程终端控制，如果移动终端发生丢失被盗，可远程进行设备密码更改、设备锁机、警告信息发送、数据擦除等操作，保护设备和数据安全；
e) 应定位、跟踪移动终端，提供受管设备的集中式管理和多维度统计信息的可视化展现；
f) 应防范自带设备风险，防止自带设备不合规造成信息泄露，通过移动设备结论码、电话号码等，确保系统内只有授权的终端。

9.3.2 移动应用安全

包括但不限于：
a) 应通过黑白名单限制移动应用程序下载及访问，提供安全相关封装工具和 SDK，确保已有应用及新开发应用均能运行在安全的容器环境中，应避免使用有漏洞的开源第三方应用组件及代码，严格限制第三方组件自身数据收集功能；
b) 用户身份鉴别或密码设定、找回，应进行二次鉴权，避免用户身份被冒领，如系统注册信息校验、短信验证码、指纹等；
c) 不宜通过第三方账户进行认证；
d) 不宜用移动终端采集或处理涉及售粮人银行卡号、金额、支付以及库存量等信息；
e) 应提供应用安全扫描和加固，若发现未指定的非涉粮应用可立刻禁止访问，并发送警告信息；
f) 不应访问移动终端中非业务必需的文件和数据；
g) 不开启与服务无关的功能；
h) 未向用户明示并经用户同意，不得擅自收集粮食业务信息、智能仓储管理数据等；
i) 对于科研需要的数据，应当遵循合法、正当、必要原则，明示收集使用信息的目的、方式和范围，并经用户同意；
j) 与粮库照明、通风等与控制系统有关的移动应用，以及仓储管理等移动应用，在用户权限控制的基础上，应增加地理围栏限制，限制对粮食自动控制系统的数据资源、网络资源、设备的访问；
k) 输入敏感信息时，应使用经过第三方专业机构检测的安全软键盘，确保敏感信息不被移动终端的其他应用程序窃取；
l) 应通过签名标识移动终端应用程序的来源和发布者，保证用户所下载的移动应用来源于粮食技术支撑单位。

9.3.3 终端敏感信息防泄漏

包括但不限于：
a) 对于协同办公、仓储业务管理、库存监管、行政执法类的移动应用，应加强对敏感文档的内容泄露防护，包括文档内容加密及安全传送；
b) 设备离开指定的地理区域后限制文档访问；
c) 限制文档保存、复制、编辑、打印等操作；
d) 限制第三方应用浏览文档内容；通过实时同步及安全共享提高协作效率；
e) 对后台任务列表中的预览界面应采取模糊或其他防护措施；
f) 敏感信息的存储应进行加密或不可逆变换，密码算法应采用官方发布 SDK 中自带算法库，如使用第三方算法库，应对其安全性进行验证，密码算法应符合国家密码管理局的相关要求；
g) 有条件的情况下，可采取数字签名技术。

9.4 电子认证

9.4.1 基本要求

包括但不限于：

a) 粮食信息系统应采用电子认证服务，以实现各个业务系统中的身份认证、完整性、保密性，抗抵赖等安全要求；

b) 粮食行政管理部门应该以省为最小单位，选择粮食 CA 或者其他具有《电子认证服务许可证》的电子认证服务机构提供电子认证服务；

c) 为粮食信息系统提供电子认证服务的提供商需接入国家根 CA，与之构成完整可信证书链。

9.4.2 电子认证的应用范围

包括但不限于：

a) 库存监管系统；

b) 地磅码单的电子签章系统；

c) 各项统计系统；

d) 各级储备粮管理系统。

9.4.3 电子认证服务要求

包括但不限于：

a) 电子认证服务机构应结合粮食信息系统外部用户和内部用户的实际需求，提供证书申请、证书发放、证书更新、证书吊销、证书解锁、密钥恢复和证书查询等证书业务服务和相关技术支持服务；

b) 电子认证服务机构在粮食信息系统开展服务时，应制定针对粮食 CA 管理平台的数据同步接口，实现数字证书和黑名单的同步上传。

9.4.4 证书格式和载体要求

电子认证服务机构发放的数字证书格式、证书介质应符合 GB/T 20518 相关要求。

9.5 数据加密

应对粮食敏感信息进行加密，实现信息离网后不可解读，确保粮食敏感信息在获取、传输、处理和应用过程中安全。

9.5.1 存储和传输过程加密

包括但不限于：

a) 数据源中含有敏感信息的原始文件，应进行文件级加密，加密完成后传输给数据系统；

b) 客户识别信息入库时，对涉及的敏感字段应进行字段级的加密处理，密码算法应符合国家密码管理局的相关规定；

c) 客户识别信息在数据系统内应独立加密存储，不另存副本，任何数据加工都应在数据系统内完成。对敏感信息的任何数据操作应留有日志记录；

d) 敏感信息的网络传输，应采用电子认证技术，防范传输过程中的截获、篡改。

9.5.2 粮食敏感信息模糊化

包括但不限于：

a) 对确实需要客户识别数据的需求，如售粮人银行卡号、身份证号等信息，除支付环节或对账环节外，其他场景的使用应进行客户识别信息模糊化；
b) 模糊化处理建议对部分数字用字母 X 替代。

9.6 边界安全

粮食信息网络安全应遵循 GB/T 22239、GB/T 22240 的要求进行建设，应全面覆盖相应级别的网络安全的控制项要求。

9.6.1 内部局域网与互联网的边界安全

包括但不限于：
a) 应部署逻辑隔离措施，主要是防火墙隔离；
b) 粮食行政管理部门与粮食企业之间的数据访问应通过虚拟专用网络（VPN）；对于漫游用户，或远程技术支持，均应通过采用 VPN 技术访问相应的内部网络；
c) 省级平台与粮食企业之间的 VPN 设备，应采用相同的安全协议，并经过连通性测试；
d) 有条件的情况下，建议采用基于国密算法的 VPN 设备；
e) 粮食信息可以设置用户网络准入控制，网络准入控制方式宜采用中心集中认证方式；禁止访问与其不相关的应用和业务服务；
f) 允许局域网用户访问互联网相关服务器的对外开放服务；
g) 应通过 CA 认证体系，实现基于角色的访问控制。

9.6.2 企业业务管理网络和工业控制网络的边界安全

包括但不限于：
a) 业务管理网络与工业控制网络的数据交换，大型企业可以通过网闸实现，一般企业应采用防火墙进行逻辑隔离；用于内部安全访问控制的防火墙可以和互联网边界的防火墙共用；
b) 对于控制粮库出入库作业、通风、用电等工业控制系统，应严格禁止面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务，确保系统只能在粮库内部局域网范围内使用；
c) 前端的隔离网闸应对 Modbus、S7、Ethernet/IP、OPC 等主流工业协议进行深度分析和过滤的防护设备，阻断不符合协议标准结构的数据包、不符合业务要求的数据内容；
d) 其关键业务数据，如工艺参数、配置文件、控制指令、运行采集的数据、日志等，应定期备份。

9.6.3 电子政务外网和互联网的边界安全

应符合电子政务外网的相关规定要求。

9.6.4 电子政务内网的边界安全

包括但不限于：
a) 电子政务内网为涉密网络，必须与公共信息网络实行物理隔离；
b) 电子政务内网与其他网络的数据交换，参考国家电子内网的相关标准和规定；
c) 对于要进行电子政务内网与电子政务外网数据交换的个别需求，可以在有数据交换的涉密网络边界部署物理隔离产品实现数据交换，相关隔离产品应按照“一事一议”的原则，向相关部门申请，批准后方能使用。

参 考 文 献

[1] GB 17859—1999 计算机信息系统安全保护等级划分准则

[2] GB/T 18336—2001/ISO/IEC 15408—1999 信息技术安全性评估准则

[3] GB/T 19715.1—2005/ISO/IEC TR 13335-1:1996 信息技术 信息技术安全管理指南 第1部分:信息技术安全概念和模型

[4] GB/T 19715.2—2005/ISO/IEC TR 13335-2:1997 信息技术 信息技术安全管理指南 第2部分:管理和规划信息技术安全

[5] GB/T 19716—2005/ISO/IEC 17799:2000 信息安全管理实用规则

[6] GB/T 20271—2006 信息安全技术信息系统通用安全技术要求

[7] GB/T 20272—2006 信息安全技术操作系统安全技术要求

[8] GB/T 20273—2006 信息安全技术数据库管理系统安全技术要求

[9] GB/T 20282—2006 信息安全技术信息系统安全工程管理要求

[10] GB/T 20269—2006 信息安全技术信息系统安全管理要求

[11] GB/T 20270—2006 信息安全技术网络基础安全技术要求

[12] DB 42/T 462 湖北省电子政务外网安全体系建设规范

[13] ISO/IEC 27001 信息技术 安全技术 信息安全管理体系

[14] 信息安全技术 终端计算机系统安全等级技术要求

[15] 信息安全技术 操作系统安全技术要求

[16] 信息产业部 等级保护的指导意见 TC 260-N0015 信息系统安全技术要求

[17] 工业和信息化部 工业控制系统信息安全防护指南(工信部信软〔2016〕338号)

[18] 中央办公厅 国务院办公厅 国家电子文件管理“十三五”规划(厅字〔2016〕37号)

[19] 上海市信息安全测评认证中心 移动互联网应用软件安全通用技术规范(试行)

[20] 国家粮食局关于规范粮食行业信息化建设的意见(国粮财〔2016〕74号)

[21] 公通字[2007]43号信息安全等级保护管理办法

中华人民共和国粮食
行业标准
粮食信息安全技术规范
LS/T 1807—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017年6月第一版
*
书号:155066·2-31703

LS/T 1807-2017