

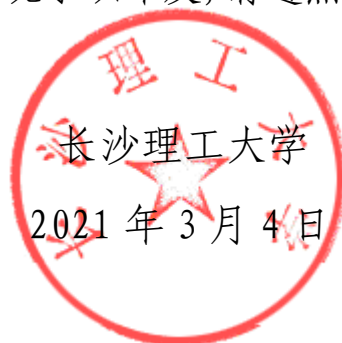
长沙理工大学文件

长理工大综〔2021〕9号

关于印发修订后的《长沙理工大学信息系统建设与管理细则》的通知

校属各单位:

修订后的《长沙理工大学信息系统建设与管理细则》已经学校2021年3月4日第3次校务会研究同意，现予以印发，请遵照执行。



长沙理工大学信息系统建设与管理细则

第一章 总 则

第一条 为深入贯彻落实党中央“加快推进教育现代化、建设教育强国”的新要求，决胜建成“百强”大学目标，打造适应学校事业发展要求、契合广大师生期待、匹配学校综合实力和省内地位的校园信息化保障体系，更好服务人才培养和学校改革发展各项事业，为学校内涵式发展、治理体系和治理能力现代化提供有力保障，充分体现统筹规划、统一标准、统一平台、统一身份认证、共享数据与资源的校园信息化建设原则，加强信息系统开发过程的管理和控制，提高信息系统开发的质量和水平，促进现有信息系统整合，实现信息交换与共享，特制定本细则。

第二条 参照标准。长沙理工大学信息系统建设与管理细则主要参照教育部颁发的《中华人民共和国教育行业标准 JY/T1001-2012》及国家和地方颁布的相关标准与管理细则。

第三条 主管机构。长沙理工大学信息化建设管理与现代教育中心（以下简称信息化中心）负责学校信息系统的整体规划、公共平台建设与管理、项目立项及审批、项目建设监管、组织项目验收，公共平台安全和日常维护，为校内各信息系统提供运行所需硬件、软件和数据资源。

第四条 适用范围。本细则适用于所有新建和现有信息系统；规定信息系统与数字化校园基础平台的数据集成、身份认证

集成及门户界面集成的技术要求；细则的主要使用者为信息系统规划人员、设计人员、开发人员和各部门系统管理员。

第五条 术语及定义

（一）长沙理工大学信息系统：学校的教学、科研、管理和服务等各类公用信息系统；

（二）数字化校园的 3 类基础平台，包括共享数据平台、统一身份认证平台、信息门户平台。共享数据平台是收集、处理、存放学校的各类共享数据，并为全校提供信息共享服务的平台。统一身份认证平台是实现网上应用系统的用户、角色和组织机构统一化管理的平台，实现各种应用系统间跨域的单点登录和单点退出和统一的身份认证功能，解决不同的信息系统用户名和口令不统一问题。信息门户平台是校内所有网络应用服务系统的统一访问点，汇集校内各种资源、应用、信息，把分散于各个信息系统的不同功能和服务有效地组织起来，为各类用户提供 1 个统一的信息服务入口；

（三）信息系统集成：指信息系统间采用统一的标准、规范和编码，实现各信息系统信息共享，进而可实现相关用户系统间的交互。信息系统集成以标准化为基础，分为数据集成、身份认证集成、门户界面集成；

（四）新建系统：指新建或者改建的信息系统；

（五）现有信息系统：指已经正常使用过的信息系统；

（六）关系型数据库：建立在关系模型基础上的数据库，借助于集合代数等数学概念和方法来处理数据库中的数据。现实世

界中的各种实体以及实体之间的各种联系均用关系模型来表示。
主流关系型数据库如：Oracle，DB2，微软的 SQL Server 等；

（七）B/S 架构：B/S 结构（Browser/Server，浏览器/服务器模式），是 WEB 兴起后的一种网络结构模式，WEB 浏览器是客户端最主要的应用软件；

（八）在线应用服务：Web Service，是由信息系统发布、完成其特定需求，其他信息系统能够通过 Internet 来访问并使用这项在线服务；

（九）可扩展标记语言：XML (Extensible Markup Language, XML)，用于标记电子文件使其具有结构性的标记语言，可以用来标记数据、定义数据类型，是一种允许用户对自己的标记语言进行定义的源语言。XML 非常适合 Web 传输，提供统一的方法来描述和交换独立于应用程序或供应商的结构化数据；

（十）应用程序编程接口：API (Application Programming Interface)，是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节；

（十一）ODI 工具：ODI (Oracle Data Integrator)，是 Oracle 公司的一个 ETL 数据集成工具，可以方便的实现将多种数据源中的数据迁移、转换到不同种类的目标中；

（十二）数据清洗：是把不符合信息编码标准要求的数据替换成信息编码标准规定的内容；

（十三）数据抽取：指共享数据平台从信息系统的后台数据

库中获取共享数据;

(十四) 数据下发: 指信息系统从共享数据平台获取需要的数据;

(十五) 数据生产者: 称为权威数据源, 指该信息产生的源头, 负责该信息的更新维护;

(十六) 单点登录 (SSO): SSO (Single Sign On), 是目前比较流行的业务整合解决方案之一。SSO 的定义是在多个信息系统中, 用户只需要登录 1 次就可以访问所有相互信任的系统。

第二章 项目的立项、验收与终止

第六条 立项申请。学校信息系统项目建设校属单位应准确详实地填写《长沙理工大学信息化建设项目申请表》, 由本单位通过协同办公系统向信息化中心提出申请。

第七条 立项审批。信息化中心收到建设单位提交的项目申请表后, 组织评审专家组进行评审。评审通过的项目, 报学校批准立项。学校准予立项的项目, 由信息化中心进行登记和备案。信息化系统建设单位如需学校提供有关服务器资源, 立项后通过协同办公系统提交《长沙理工大学服务器申请表》。

第八条 项目验收。新建信息系统至少上线运行 1 个月, 达到建设目标, 建设单位向信息化中心提交《长沙理工大学信息系统验收申请表》和《长沙理工大学信息系统测试报告书》后, 信息化中心组织专家对项目进行验收。

第九条 项目终止

（一）单位如需终止信息系统的服务，应由本单位从学校协同办公系统中发起终止流程申请，办理有关信息系统的终止事宜；

（二）信息系统在运行过程中，如违背本细则或违反国家有关计算机网络信息管理的各种法律、法规，信息化中心有权终止其服务。

第三章 总体框架及技术规范

第十条 信息系统建设总体框架

根据学校信息化建设规划，构建以共享数据平台、统一身份认证平台、信息门户平台为核心的数字化校园基础平台。建立硬件网络、操作系统，制订信息系统运行环境、架构、技术、安全等方面的规范，以规范信息系统设计、开发及建设过程，实现学校范围内的资源整合、信息共享。通过将新建及现有信息系统与数字化校园基础平台进行集成，实现本系统与数字化校园基础平台之间的数据交换，通过单点登录，实现集成的信息门户服务，方便师生工作、学习与生活。

第十一条 系统建设技术规范

（一）服务器管理

为规范管理、保证运行安全，新建信息系统使用的服务器应统一部署到学校数据中心机房，集中统一管理，不得使用普通 PC 机代替服务器。

（二）操作系统及访问

信息系统的服务端（WEB 服务器、应用服务器、数据库服务器）须安装运行在主流 Windows 或者 Linux、Unix 等操作系统上。

服务器操作系统的口令应只掌握在管理员手中，密码必须保证一定强度并定期更改。信息系统建设阶段，为便于调试，可对系统建设厂商开放管理用户口令，建设完成后应立即更改。所有服务器应按要求安装杀毒软件，并定时升级病毒库，及时升级操作系统补丁。

所有服务器不得安装、运行与信息系统无关的软件、伺服程序等；不得上传危害系统及网络安全的恶意代码和病毒，如因管理不当给学校硬件网络及信息服务带来危害，相关管理员应承担相应责任。

（三）系统部署

在条件允许的情况下，信息系统应通过双机热备、负载均衡等方式来提高信息系统服务的可靠性。在条件允许的情况下，信息系统部署应遵循服务器专机专用的原则，把数据库、应用服务、WEB 服务分别部署在不同的服务器或虚拟机上。

（四）数据库使用

信息系统应使用主流关系型数据库。数据库系统管理员账号只能由数据库管理员掌握，密码应保证一定强度并定期更改。信息系统使用的数据库账号不应分配数据库管理员权限。

信息系统在进行数据集成时若创建用于集成的数据库用户，应按照数据库管理要求设定用户权限，保障数据安全。

（五）系统架构

信息系统应采用 B/S 三层架构，即 WEB 服务器、应用服务器、数据库服务器，以方便用户使用并提高系统安全性。

（六）网络访问

信息系统提供 WEB 服务只能默认通过 80 端口。在实际使用中如需开放其他端口，须通过协同办公系统向信息化中心提出申请，并说明开放的端口及用途。

（七）接口要求

信息系统应根据学校管理需要提供如系统管理、查询、关键业务等功能的 Web Service 接口。信息系统间的数据交换支持标准 XML 格式数据。

（八）信息编码标准

新建信息系统所使用的信息编码应严格遵循“长沙理工大学信息编码标准”的要求，并按照学校信息编码管理与基础数据共享管理规定执行。

现有信息系统使用的信息编码如不符合本细则“长沙理工大学信息编码标准”，原则上应逐步通过数据清洗的方法将原有编码替换成学校信息标准编码；如因技术或其他原因无法进行数据清洗，则需通过建立应用系统和学校信息标准编码间的对照表来实现学校信息标准编码的应用。

数据生产者应及时准确地维护好相关信息，通过后续的数据集成同步到数字化校园共享数据平台，供其他信息系统使用。所产生数据中涉及到的信息编码，应与“长沙理工大学信息编码标

准”保持一致。规范中的信息编码不能满足信息系统业务需要时，应遵照学校信息编码管理与基础数据共享管理规定进行维护。

数据使用者应向信息化中心（网信办）提出使用数据申请，通过数据集成定时从数字化校园共享数据平台获取需要使用的信息，在使用过程中不得修改数据，如发现数据不正确或者不能符合使用要求，应联系信息化中心（网信办）协商解决。

信息系统若使用的信息编码未包含在“长沙理工大学信息编码标准”中，应按照学校信息编码管理与基础数据共享管理规定，经信息化中心批准后，对信息编码进行补充。

（九）权限管理

信息系统的权限管理应采用角色、权限组的权限管理方式，通过配置用户角色赋予用户相应的权限进行管理。

（十）系统备份

信息系统应定期进行运行程序备份和数据备份。

（十一）系统安全

代码安全：信息系统开发过程中应充分测试，不能因程序代码的问题形成信息系统安全漏洞。

数据传输安全：在信息系统间进行数据传输时，不得以明文传输用户名、口令等敏感信息，需要进行加密处理。

追溯机制：应建立系统用户访问及操作日志。

（十二）隐私保护

信息系统应充分保护个人信息，除因业务需要面向管理人员

开放的统计查询功能外，不得公开涉及用户个人隐私的信息。个人隐私包括生活情况、生理心理情况、资产情况、通讯信息、社会关系等。

（十三）扩展性

信息系统须具有良好的扩展性。要求模块间应相对独立、接口清晰，内部的业务流程升级和改造与其他模块无关，能根据信息系统的类型提供必要的二次开发 API 以及详细的使用说明和开发示例。

（十四）技术支持及售后

信息系统开发厂商应提供完善的技术支持和售后服务响应机制，及时应对使用过程中的突发问题或适应学校业务发展带来的需求变动，信息系统开发厂商须在合同中承诺在学校需要的时候提供集成支持。

（十五）移动应用建设技术规范

1. 移动应用总体技术要求

随着移动智能终端的迅速发展，学校对移动应用的建设需求也越来越迫切。在通用的信息系统技术规范的基础上，移动应用平台及开发需满足以下要求：

（1）统一平台：在学校层面构建统一安全的移动应用平台，各类移动应用都基于该移动应用平台来建设；

（2）统一接入：各运营商、学校各部门统一接入到移动应用平台，采用统一的业务接口标准，可以支持包括 CDMA1X/EV-DO、

GSM/GPRS/WCDMA/TD-SCDMA、WLAN 等多种无线接入技术；

(3) 统一安全架构：移动应用平台提供统一的安全架构，实现业务和数据信息的真实性、机密性和完整性、可核查性、可控性、可用性，必须保障移动应用的安全；

(4) 统一认证：用户接入由移动应用平台进行统一的用户管理、开通注册、认证和授权；

(5) 统一终端选择：移动应用平台采用统一的终端选择原则。

2. 接口规范

移动应用和移动应用平台应该是松耦合结构，平台通过开放的功能集成接口为应用提供集成的多功能支撑和管理数据支撑，移动应用通过平台提供的标准接口进行管理、展现。

移动应用平台提供的 Web Service 接口应该具备灵活配置的能力，应能够支持文件接口、API 接口等多种接口方式，与源数据的对接应该安全、高效并且可扩展。

3. 可靠性与性能要求

移动应用平台应具有良好的容错机制，当平台某一模块发生错误时不影响整个业务运行；采用成熟的技术和设备，关键部分有冗余、备份措施；关键设备应采用热备份和负载均衡等方式保证应用正常运行；系统峰值负荷不超过 70%；核心设备不能有单点故障。

客户端 WAP、Web 页面并行处理应至少支持 300 用户在线进行并行操作，300 用户并发情况下系统响应时间应小于 5 秒；CPU 忙时利用率平均应不超过 70%；从数据库备份到存储设备和从存储设备恢复到数据库的时间应不超过 4 小时。

4. 安全要求

移动应用平台要提供相应的安全性保障，实现业务和数据信息的真实性、保密性、完整性、可核查性、可控性、可用性。移动应用平台应具备以下安全功能：接入的 CA 身份认证，链路安全，平台边界防护，移动应用系统安全、终端安全防护等。

5. 终端支持要求

移动应用平台应广泛支持主流移动智能终端，包括 iOS、Android 系统的富客户端应用程序，也应支持 Windows Phone、Symbian、Palm Web OS 等系统以 WEB 浏览的方式来获取平台的服务。

可接收移动智能终端的版本检查请求，根据移动智能终端类型检测最新版本，实现客户端软件自动升级。

移动应用平台应支持内嵌功能，例如内嵌既有的 iOS、Android 应用，有利于各类应用的融合，可以使移动智能终端的应用更为丰富。

6. 移动应用开发要求

移动应用平台应开放服务端开发常用的组件工具类包、客户端开发包等，并提供详细的开发手册。移动应用开发者可直接使用，避免重新进行底层开发，降低开发难度同时保证稳定高效。

移动应用平台架构设计上应做好数据库操作代码的封装，在满足业务功能需要的前提下优先考虑将数据库操作的相关代码封装成存储过程、函数等可重用的数据对象。移动应用程序代码中使用数据库连接时，应及时关闭数据库连接。为了提高应用访问速度可采用生成静态页面等技术，具体情况应根据移动应用的实际情况而定。

第十二条 信息系统集成技术层次

信息系统集成共包括 4 个层次，分别是数据集成、业务集成、身份认证集成、门户应用集成。

（一）数据集成

数据集成依据各个信息系统管理的范围，结合数据的基本特点对数据进行组织；定义统一的标准格式，采用适用的交换技术实现数据的交换和共享。

（二）业务集成

业务集成实现业务逻辑在多个信息系统之间的流转，即统一业务逻辑。

（三）身份认证集成

身份认证集成主要为各信息系统提供集中的身份认证服务。用户可使用一个身份账号访问所有信息系统，实现单点登录，通过指定相应的认证技术规范，提供丰富的信息系统认证接口，最终实现所有信息系统用户认证的集中统一管理。

（四）门户应用集成

门户应用集成实现现有的业务系统、数据资源的整合，实现信息的合理聚集；通过实现统一的用户和统一的访问入口来访问门户平台中整合的相关信息资源。

第四章 信息系统集成规范

第十三条 数据集成

信息系统在进行数据集成时若创建用于集成的数据库用户，应按照数据库管理要求设定用户权限，保障数据安全。

（一）数据抽取

1. 数据抽取方式

（1）集成工具通过具有可读权限的数据库用户访问数据库表、视图读取数据进行抽取；

（2）信息系统提供 Web Service 接口以获取标准 XML 数据进行抽取。采用集成工具（ODI）直接访问数据库表、视图进行数据抽取的方式。

2. 实施步骤

（1）确定数据抽取可行性及抽取方式；

（2）信息系统所属部门配合数字化校园项目组搜集本系统可共享的数据的需求；

（3）在信息系统数据库中创建用于集成的账号，配置好相应的权限，并按照需求创建表或视图，让该集成账号可以访问；

（4）数字化校园共享数据平台通过 ODI 工具访问信息系统数据库进行数据集成抽取操作；

（5）数据抽取测试。

3. 信息系统开发厂商的任务

（1）配合讨论确认数据集成方案；

（2）配合进行数据集成实施，创建数据库账号，创建表或视图，提供数据结构等；

（3）数据集成测试。

（二）数据下发

1. 数据下发方式

（1）信息系统直接访问方式：在共享数据平台的数据库创建查询账号，并生成信息系统需要的数据视图，信息系统通过访问该查询账号获取数据；

（2）写临时表方式：共享数据平台通过 ODI 工具把信息系统需要的数据写入到信息系统数据库临时表中。信息系统需要创建有操作权限的账号，并创建保存需要获取的数据的临时表。信息系统从临时表中获取数据，处理后维护进信息系统正式数据中。

2. 实施步骤

（1）确定数据下发可行性及下发方式；

（2）信息系统所属部门配合数字化校园项目组搜集本系统需要从共享数据平台获取的数据的需求；

（3）如采用信息系统直接访问的下发方式，则共享数据平台创建供信息系统访问的查询账号，并生成信息系统需要的数据的视图；如采用写临时表的下发方式，则信息系统须在数据库中创建用于集成的账号，配置好相应的权限，并按照需求创建临时表。数字化校园共享数据平台通过 ODI 工具访问信息系统数据库，把信息系统需要的数据写到相应的临时表中；

（4）信息系统通过开发系统功能或其他方式处理从共享数据平台或临时表中获取到的数据，并同步到信息系统正式数据中；

(5) 数据下发测试。

3. 信息系统开发厂商任务

(1) 配合讨论确认数据集成方案；

(2) 进行数据集成实施。创建需要的数据库账号，创建临时表，进行必要的数据处理功能开发等；

(3) 数据集成测试。

第十四条 身份认证集成

(一) 信息系统进行身份认证集成的前提条件

1. 信息系统采用 B/S 架构；

2. 配置域名访问信息系统，域名后缀为 *.lzu.edu.cn；

3. 数字化校园平台中的教职工、学生唯一身份识别码为校园卡卡号，并以邮箱账号作为别名。新建系统须以校园卡卡号作为登录账号；现有信息系统需要维护系统中用户信息与校园卡卡号的对应，并能以校园卡卡号登录系统；

4. 提供集成开发支持。

(二) 身份认证集成方式

数字化校园统一身份认证平台提供多种认证接口，包括 C、JAVA、COM 组件、PHP 等接口，还提供扩展的 Web Agent 代理认证接口。

信息系统可根据本信息系统所适用的开发语言、运行环境等参照选择接口类型，确定身份认证系统集成的方式。如以上接口都不能满足，则需要向信息化中心（网信办）报告，批准后可采取其他集成方式。信息化中心（网信办）根据确认的集成方式提

供信息系统集成所需的接口及示例。信息系统参照接口示例，根据学校集成要求或沟通确认的集成方案，修改系统的认证模块代码，实现统一身份认证集成。

（三）集成实施步骤

1. 信息系统所属部门与信息化中心（网信办）沟通确认集成方式及要求；

2. 信息系统所属部门从信息化中心（网信办）获取接口及示例，对信息系统进行开发修改；

3. 通过数据同步或者维护账号对应关系等方法，保证信息系统中用户账号与数字化校园平台中用户账号一致；

4. 集成测试。

（四）信息系统开发厂商任务

1. 配合讨论确认身份认证集成方式；

2. 进行身份认证集成开发实施工作；

3. 身份认证集成测试。

不符合身份认证集成前提条件，或无法按照本细则要求进行身份认证集成的信息系统，需与信息化中心另行协商集成方案。

第十五条 门户应用集成

（一）集成方式

信息系统应参照“身份认证集成”部分的说明实现认证集成。信息系统提供实现认证集成后的页面 URL，通过信息门户中的集成模块配置到信息门户中展现。

如果学校需要在信息门户中展现信息系统的某个单独的功

能页面，则该功能页面 URL 也须实现身份认证集成。

（二）实施步骤

1. 沟通确认信息系统需要在信息门户中展现的内容；
2. 信息系统开发厂商实现身份认证集成；
3. 信息系统开发厂商提供实现身份认证集成的访问页面 URL（或者单独功能页面的 URL），由管理员配置到信息门户中展现。

（三）信息系统开发厂商任务

1. 配合沟通信息系统在信息门户中的集成方式和展现内容；
2. 提供集成所需的页面 URL，进行必要的开发修改工作；
3. 集成测试。

第五章 安全管理

第十六条 应用安全

信息系统必须制定针对用户的访问安全策略，具备防止恶意探测、暴力破解、抵御普通 DDOS 攻击的能力；

信息系统必须进行程序资源（程序功能、菜单、WEB 下的 URL 资源）访问的安全控制，仅为用户提供和其权限相符的程序资源；

信息系统的业务流和数据流的设计必须严谨，不能存在纰漏；

信息系统必须严格依据用户权限来决定其数据域的范围；

信息系统必须具备完善的日志系统；

信息系统的部署不能影响系统平台的安全，不能影响自身的安全，不能影响其他信息系统的安全；

应用中涉及的重要业务数据应加密后存放至数据库；
涉及到信息系统本身关键性数据的操作，应进行二次鉴权。

第十七条 数据库安全

数据库必须有严格的存取权限控制措施；

在数据库的使用过程中必须通过备份、恢复等技术手段来保护数据库的完整性；

应对输入数据进行逻辑检验，数据库更新时应保证数据的准确性；

必须建立可靠的日志制度。对数据完整性要求较高的场合要建立双副本日志以保证意外时的数据恢复；

必须建立定期转存制度，并根据交易量的大小决定转存频度。

第十八条 传输安全

重要数据（如认证信息等）严禁以明文方式进行传输，必须采用 128 位及以上强度进行加密传输。

第六章 测试与部署

第十九条 测试

测试分 3 部分：总体测试、功能测试、联调测试。

（一）总体测试

总体测试是指按照本细则条款对系统进行的全面测试，检查系统是否严格按照细则要求进行建设。由信息化中心组织专家、开发人员测试组，按照《长沙理工大学信息系统测试报告书》的

要求对系统进行逐项测试。

（二）功能测试

功能测试是指按照项目建设方与项目开发方约定的业务功能需求和系统性能需求对系统的业务功能和系统运行性能进行全面测试。建设单位组织相关业务人员和系统开发人员组成功能测试组，按照项目约定内容，对系统进行功能的全面测试，协助信息化中心完成系统的性能测试。

（三）联调测试

联调测试是指某信息系统与其他信息系统之间进行的各种相关业务的功能测试。信息化中心组织本项目建设单位和参与联调测试相关单位的人员组成联调测试组，对各相关系统之间的业务联动功能进行测试。

第二十条 部署及运行系统通过全面测试后，由建设单位在信息化中心的配合下进行系统试运行前的部署，进入试运行阶段，试运行时间为1~6个月。系统试运行阶段结束后，转入正式运行阶段。

第七章 系统管理与维护

第二十一条 运行环境的管理与维护信息化中心负责信息系统部署的机房环境、网络环境、软件运行环境以及服务器硬件环境的管理和维护。

信息化中心保障机房电力供应、温度恒定以及环境整洁；保障公共数据信息中心信息系统接入网络、平台软件以及服务器硬件正常运行；

信息化中心需定期修正信息系统平台软件的补丁，操作完毕后填写系统管理员信息系统平台升级操作日志；

信息化中心负责公共数据库的备份。

第二十二条 建设和使用单位职责

信息系统建设单位负责信息系统及所在服务器的管理与后续维护；

信息系统的使用单位至少配备 1 名信息系统管理员并报信息化中心登记备案，信息系统管理员在业务上接受信息化中心的指导；

信息系统管理员须每天检查信息系统及所在服务器的运行状况，并填写系统运行日志；

信息系统管理员负责每天定时对本单位各信息系统内部数据的备份工作；

信息系统如需升级，使用单位必须向信息化中心提交升级申请，经信息化中心审核批准后系统升级方可进行；

信息系统使用单位必须制定信息系统的应急处理方案，方案必须明确所要采取的具体步骤以及每个步骤的内容并确定应急方案执行人；

应急方案执行人在故障排除后需填写详细的故障维护日志。

第八章 文档规范

第二十三条 文档编制

信息系统在其软件生存周期各阶段都必须产生相应的文档；
信息系统软件在生存周期各阶段产生的文档都必须遵照国家标准编写；

文档的编制人员必须注意适应自己特定读者的水平、特点和要求；

信息系统可依据其系统的规模大小来确定文档编制的规模。

第二十四条 文档管理

信息系统使用单位都必须指派专职人员来负责文档编制的监督和已编制文档的整理，并上报信息化中心备案；

信息系统使用单位必须在项目验收时向信息化中心办递交项目所有文档的电子文档（DOC 或 PDF 格式），其中《软件需求说明书》《操作手册》《项目开发总结报告》《测试分析报告》必须同时递交纸质文档。

第九章 附 则

第二十五条 本细则由信息化中心负责解释。

第二十六条 本细则自公布之日起施行，原《长沙理工大学信息系统建设与管理规范》（长理工大综〔2016〕59号）同时废止。

附件：1. 长沙理工大学信息化建设项目申请表
2. 长沙理工大学服务器申请表

3. 长沙理工大学服务器申请规定
4. 长沙理工大学信息系统验收申请表
5. 长沙理工大学信息系统测试报告

附件 1

长沙理工大学 信息化建设项目申请表

项目名称: _____

申请单位: _____

负责人: _____

联系电话: _____

电子邮件: _____

长沙理工大学

年 月 日

项目名称			
经费来源		预算（万元）	
部署地点		预计采购时间	
建设项目说明			
<p>（请在此处对建设项目系统进行详细说明,包括建设目的、预计解决的问题、功能点描述等。如需进行招投标,请附上招标书的技术参数要求部分的文档）</p>			

申请方单位负责人意见

签字：
年 月 日

信息化建设管理与现代教育中心负责人意见

签字：
年 月 日

附件 2

长沙理工大学服务器申请表

单位名称				
联系地址				
部门类别	<input type="checkbox"/> 党政管理机构(含群团组织) <input type="checkbox"/> 教学院 <input type="checkbox"/> 教辅及其他机构 <input type="checkbox"/> 其他----			
行政负责人	姓名		手机	
	电话		QQ	
系统管理员	姓名		手机	
	电话		QQ	
系统需求	CPU		内存	
	硬盘		预装系统	
软件清单				
开通端口				
用途	<input type="checkbox"/> Web 主页(域名)----- <input type="checkbox"/> 其他-----			
费用预算	虚拟机成本			
	年度维护成本			
使用时限	年 月 日至 年 月 日			
相关规定	本单位承诺遵守《长沙理工大学信息化建设管理与现代教育中心虚拟机托管规定》及长沙理工大学校园网及信息系统的相关管理规定。是否授权由信息化建设管理与现代教育中心代为重启服务器。 <input type="checkbox"/> 是 <input type="checkbox"/> 否			
申请事由				
申请单位签字(盖章):		批准单位签字:		
年 月 日		年 月 日		

长沙理工大学服务器申请规定

一、服务的对象和范围

长沙理工大学各院、系、所、中心，各部、处，各单位。

二、虚拟机托管服务条款

（一）托管部门须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》等相关国家法律和长沙理工大学校规校纪，以及信息化中心的管理规定。

（二）托管服务器原则上只允许对外开放以 www 为主的互联网基本信息服务，如需提供其他服务，需要申请时特别说明，经信息化中心审批后，方可提供。

（三）托管部门自行解决服务器上所有软件版权（许可/使用权）问题以及由此造成的法律纠纷，并负责服务器上数据的完整性和保密性，做好数据备份工作。

（四）为了规范校园网络管理，保障托管服务器的正常运行，最快时间的故障排除和应用服务的恢复，服务器使用部门须填写《长沙理工大学服务器申请表》。

（五）信息化中心有权对虚拟机使用进行必要的监控，以保证学校网络线路的正常运行。

（六）信息化中心保留因服务器使用部门违反服务条款，或因

服务器中毒、被黑客侵入等情况出现时终止服务器运行的权利。

（七）每台虚拟机最长使用期限 3 年，逾期需重新申请和预算成本。3 年使用期限内需每年申请年检，参照信息化中心资源年检制度。

（八）申请审批后，在 10 个工作日内由信息化中心提供虚拟机或物理服务器交付用户使用。

（九）信息化中心保留对本规定的最终解释权。

三、服务内容

（一）信息化中心提供良好的机房环境，完备的机房设施。

（二）信息化中心负责设备物理位置的摆放、IP 地址的分配、网段划分、网络流量监控和校园网的正常运行，保证设备物理安全、网络畅通。

四、争议解决与不可抗力

（一）由于不可抗力因素引起供电和通信不稳定而造成的网络故障以及软硬件问题，信息化中心不承担责任。

（二）由于 ISP（InternetServicesProvider）的原因造成的网络故障，将由信息化中心负责与运营商联系，及时排除故障。

附件 4

长沙理工大学_____项目验收申请表

项目名称			
合同编号		实施单位	
部署地点		项目启动日期	
项目说明			

验收条件说明	
1、安装、调试、运行情况	
2、测试报告书	
3、其他情况说明书	
4、存在的问题和解决计划书	
申请单位负责人意见	
签字盖章： 年 月 日	

附件 5

长沙理工大学信息系统测试报告

信息系统测试报告书主要是依据《长沙理工大学信息系统建设与管理细则》对拟上线信息系统进行测试，测试内容包括用户界面、功能性、安全性和压力测试。

一、测试安排

应用系统名称:

申请测试单位名称:

系统维护负责人:

测试人员:

测试员姓名	联系方式	职责

测试进度:

测试活动	计划开始日期	计划结束日期	实际开始日期	结束日期

二、测试项目

(一) 用户界面

1. 布局通过标准：界面布局整齐，风格一致。

测试记录：应包括测试时间、测试的具体内容、发现的问题等。

2. 菜单通过标准：子菜单不超过 3 级。

测试记录：用类似第 1 个测试记录的方式书写第 2 个及其后的测试记录。

3. 对用户动作的反馈通过标准：对用户动作提供及时、正确、可读的操作提示。

测试记录：

4. 数据录入通过标准：具备以键盘方式独立完成数据录入的功能。

测试记录：

5. Web 浏览器兼容性

通过标准：可在 IE、Firefox、Chrome 的当前最新版本上使用，并能保证呈现同等的效果，包括界面的效果，功能的可用性等。

测试记录：

(二) 功能性

根据系统建设功能、技术要求，逐项进行满足性测试。并如实填写下表：

序号	测试功能点	测试样例	测试结果

(三) 安全性

日志系统通过标准：日志系统能够记录用户的操作和系统运行状况。测试记录：用类似第 1 个测试记录的方式书写第 2 个及其后的测试记录。

数据保护

通过标准：重要数据加密后存放至数据库。

测试记录：

(四) 压力测试

连接或模拟连接最大实际(实际允许)数量的访问测试记录：应包括测试时间，使用的测试软件，测试的具体内容，测试时服务器开销(内存使用、CPU 占用、网络流量等)，发现的问题。

三、整改建议

针对以上项的测试记录，提出以下改进建议：

四、测试结论

____年__月__日，____系统进行全部__项测试，其中项合格，____项需整改，测试结果为：(通过/未通过)。

测试组负责人签名：

信息化中心负责人签名/盖章：

长沙理工大学党政办公室

2021 年 4 月 2 日印发
