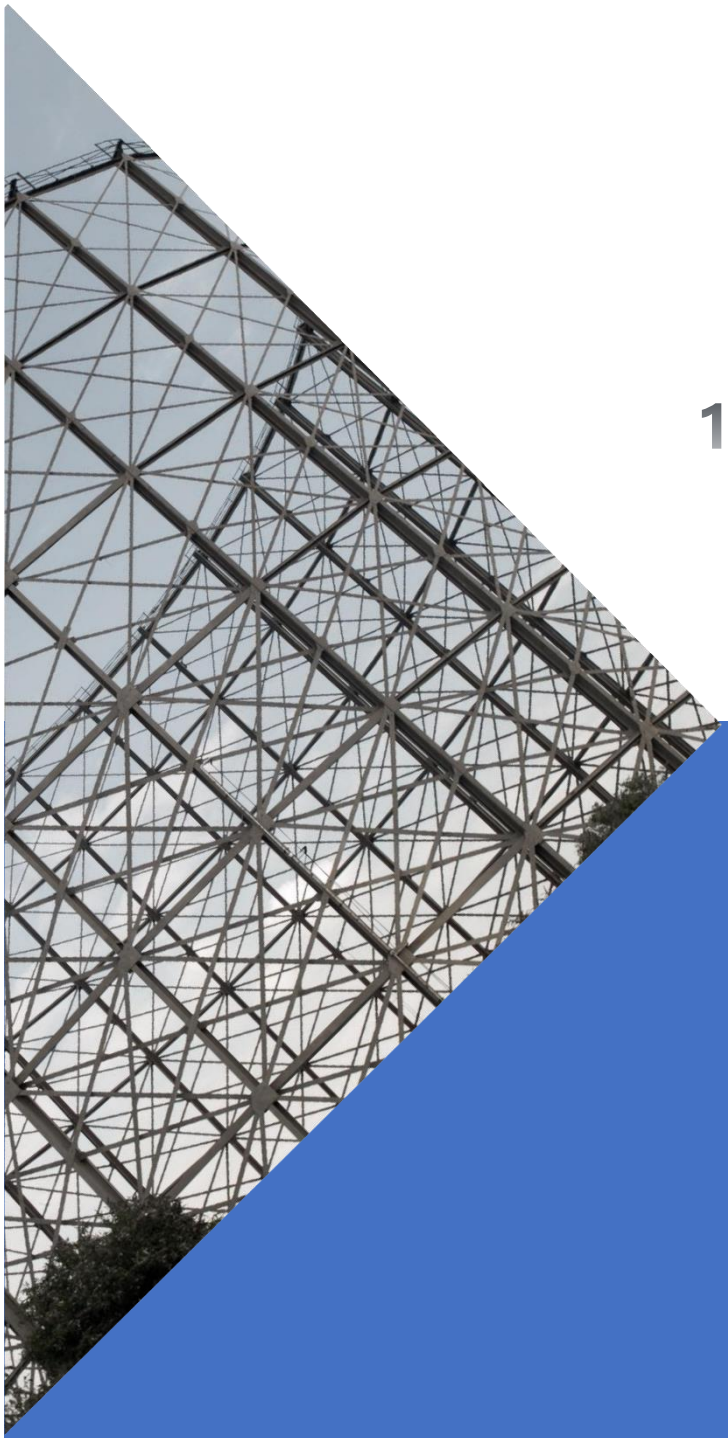
51CTO



1000门IT实践精品课程

使用手册

目 录

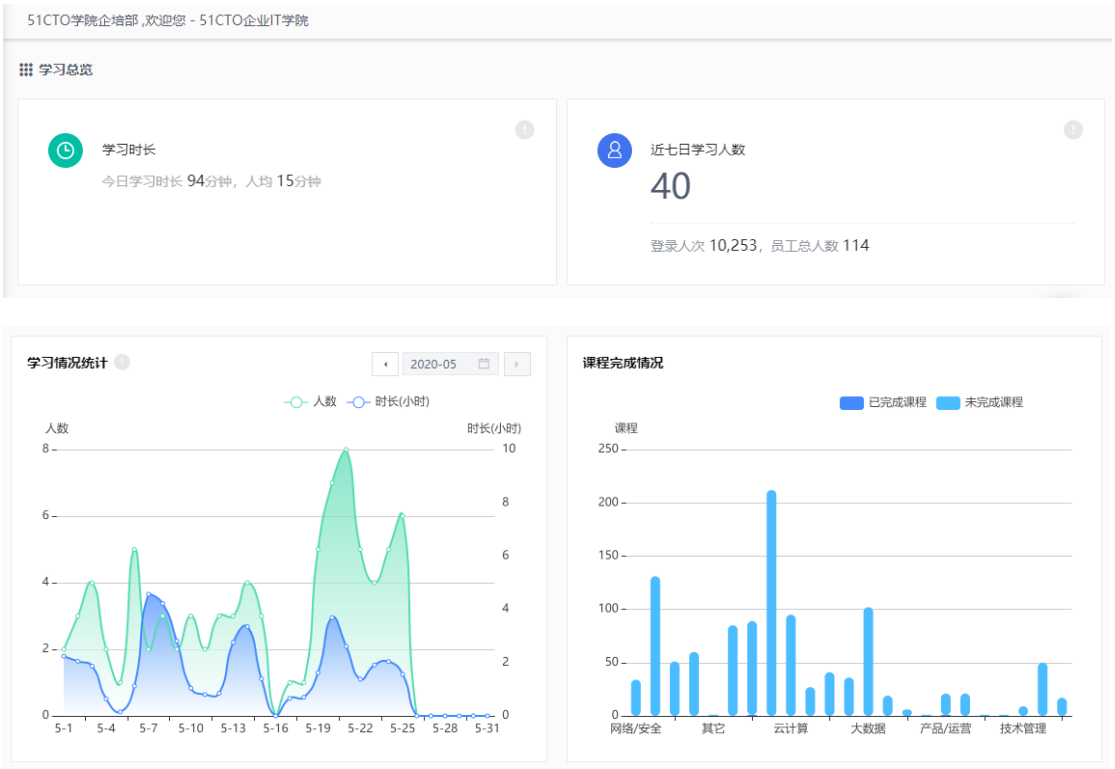
一．平台操作指南

1.管理员操作指南

1.1视频学习管理

1.1.1学习情况总览

管理后台首页中，可以直接查看学习总览，其中包括：学习总时长、近一周的学习人数、学习情况统计图、学习排行榜等。如下图：



1.1.2学习数据

学习数据主要是从学生、课程、考试这三个方面来统计。

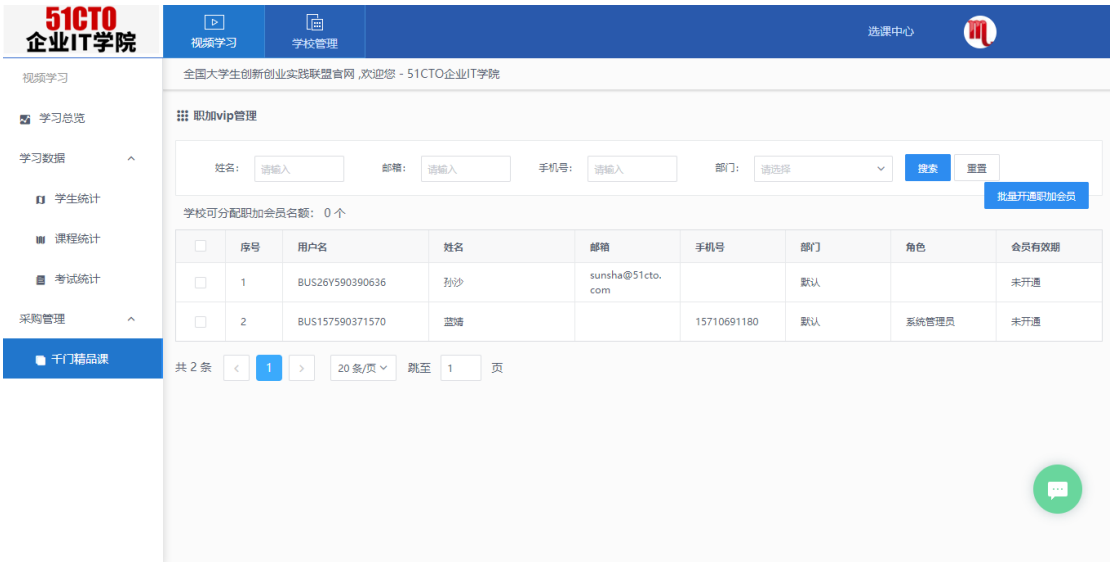
学生统计：从学生的角度统计学生学习的课程，已学完课时，已学习时长，课程时长，学习完成率等信息。可以点“导出详情”，导出Excel表格详细信息。

课程统计：从课程的维度可以统计每一门课程被学习的情况，包括学生，学习时长，学习完成率等信息。可以点“导出详情”，导出Excel表格详细信息。

考试统计：从考试的维度统计学生作业的情况，包括考试人数，应考人数，通过率等信息（只有课程中包含随堂考试题目的课程，学习做题后，这里才会有数据）。

1.1.3千门精品课账号管理

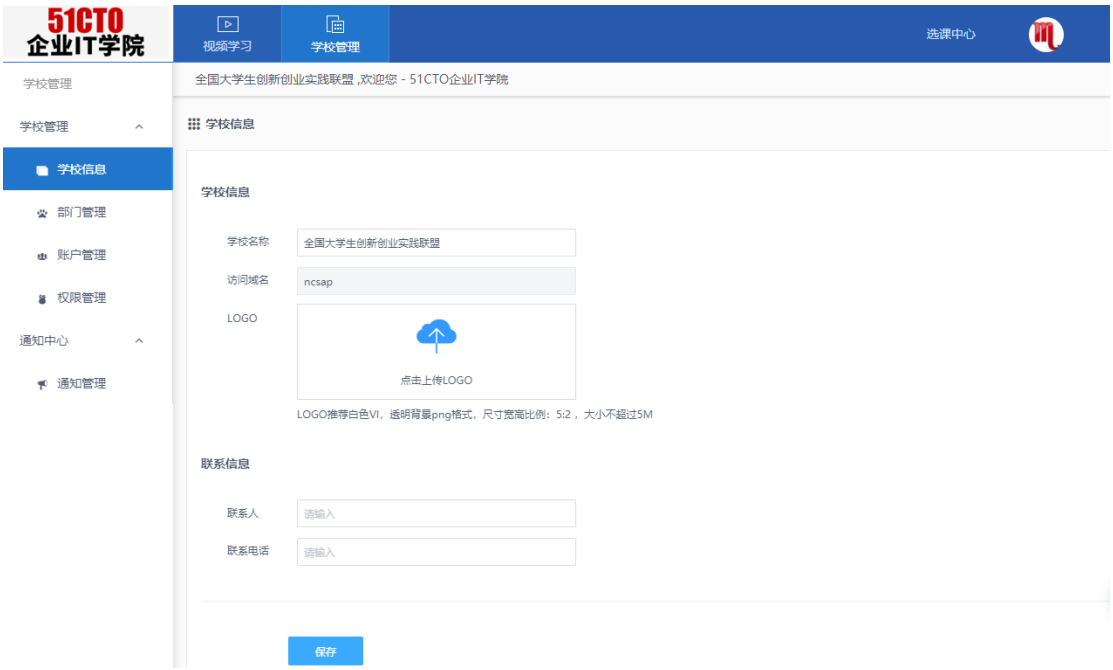
在千门精品课管理处可以查看到学校目前可用的账号VIP数量，如果有剩余名额的话，可以在需要分配的学生账户前白框处进行勾选，将名额分给出去，也可以同时对多个学生进行批量分配。



获得VIP权限的账号，登录平台并开始学习课程后，名额即已使用，不可以退换。

1.2学校管理

点击图示位置的【学校管理】，既可对学校基本信息、部门进行设置和修改，还可导入学生信息及管理学生信息。



1.2.1学校信息

在“学校信息”中可以修改或查询学校信息及LOGO，如上图。

1.2.2院系管理

在院系管理中，学校可以新增、删除院系，或者修改院系名称。

1.2.3账户管理

账户管理中，可以单个或者批量的导入新学生

红色字段为必填，邮箱或者手机号而这必须要填写一个

批量导入，先下载模板excel，将信息填到excel中，然后批量导入。

1.2.4权限管理

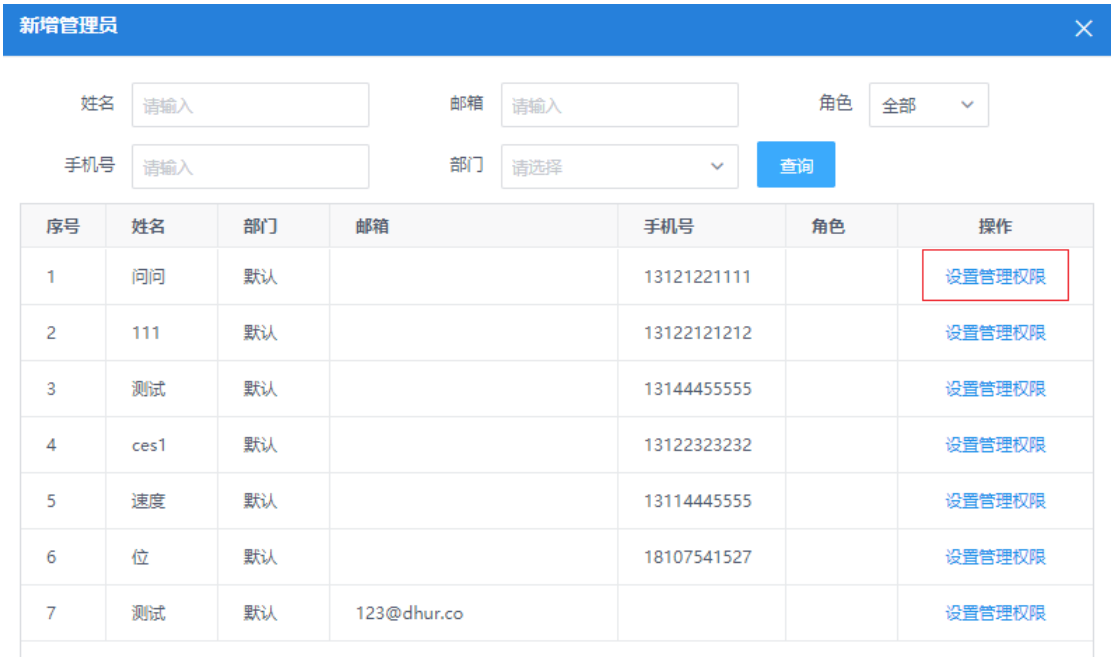
此处可以新建不同权限的管理员

创建的具体流程为：

1.将需要创建的人的信息通过上一步步骤进行录入

2.点击【权限管理】处右上方的【创建角色】，再接着点击新页面中的【新建角色】，对这个角色能够管理的院系及功能权限进行选择，点击【确认】进行保存

3.重新点击【权限管理】，点击右上方的【新增管理员】，找到需要创建为管理员的人，点击他信息最后一项的【设置管理权限】，选择好管理员的权限，一个管理员就创建成功了。



1.2.5通知管理

在通知管理中可以收到系统信息，同时可以新建通知

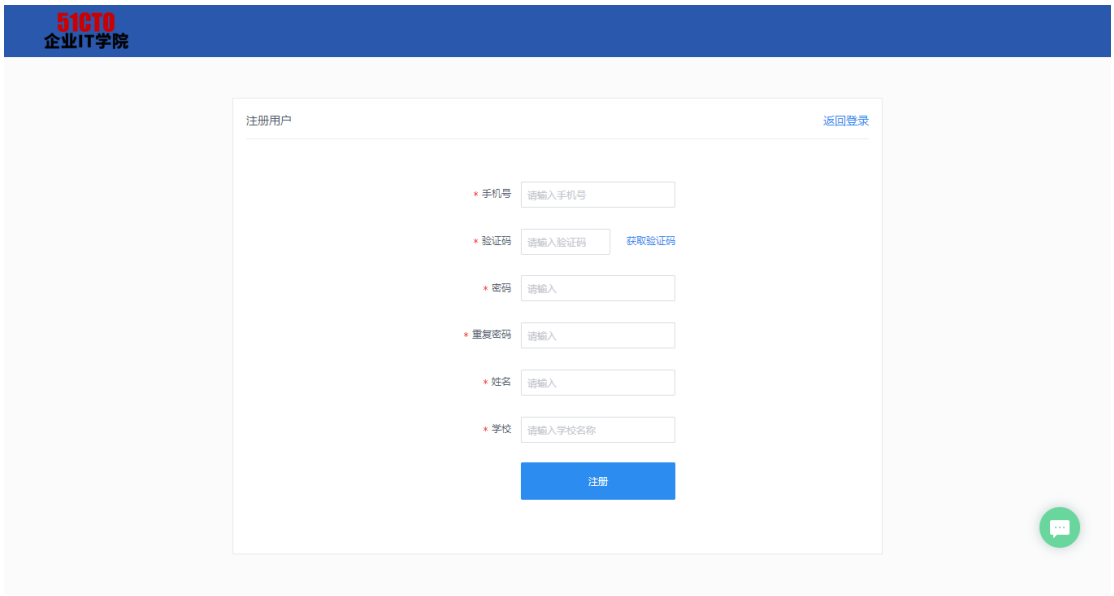
2.学生操作指南

2.1平台注册及登录

账号获取：

浏览器中打开网址：https://b.edu.51CTO.com/site/pro-plus-home/edu

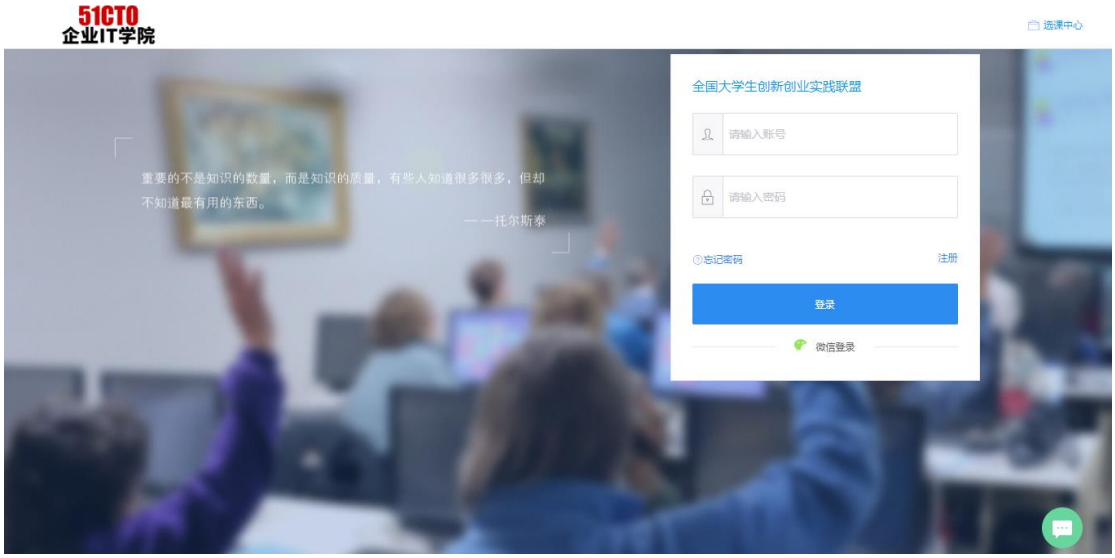
如果没有账号，在右上角点击注册，进入注册页面。



注册成功后，可以直接进入登录页面，使用手机号和注册的密码登

录。

如果有账号，点击登录，进入登录页面。



输入账号，账号使用手机号可以登录。

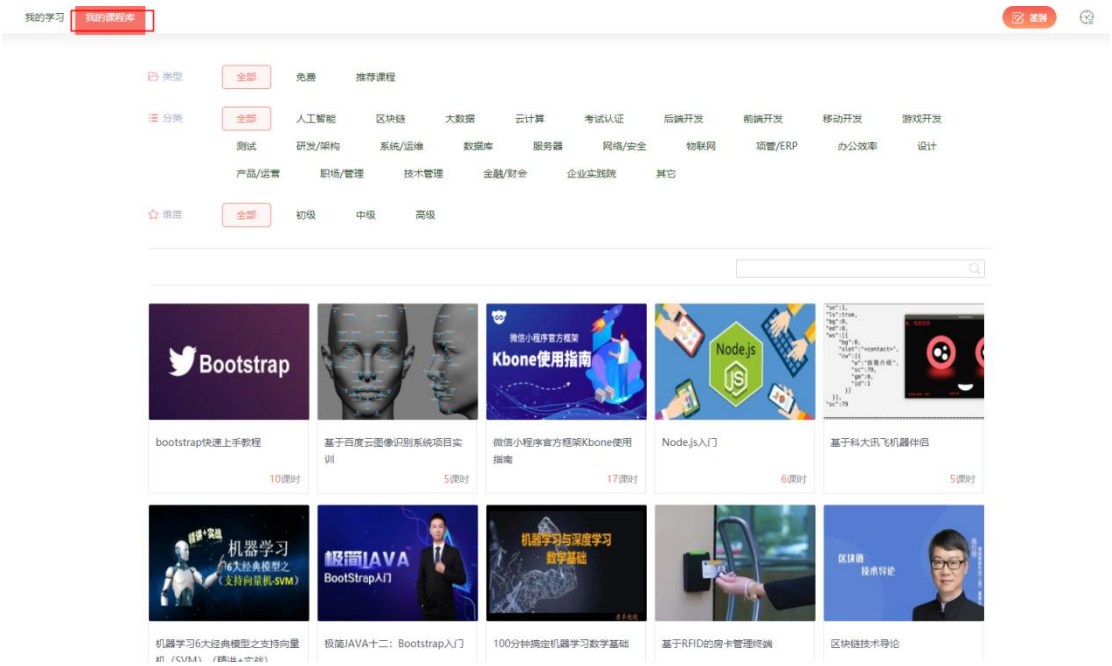
通过学校域名链接，打开学校平台，登陆账号密码，进入平台：

注：

免费课程都可以通过官网的登录入口进入；

购买1000门课程的学校的域名不一样，以开通时的域名为准。

登陆之后，在“我的课程库”选择自己想学习的课程，可以通过课程名称进行搜索，也可以根据分类进行筛选。



注：学习账号自开通之日起有效期一年，至有效期结束时所有功能停止服务。

2.2课程介绍及资料

在视频下面有关于视频课程的课程介绍、课程目录、学习资料等；

2.2.1课程介绍

简述课程的目标，以及课程的简介：

2.2.2课程目录

此次课程的目录信息，可以查看课程时数，已完成课时数以及未完成课时数：

2.2.3学习资料

可以下载与课程相关的课件资料：

2.2.4作业考试

进入详情页后，点击“作业试卷”即可进行答题（只有部分课程含作业）。

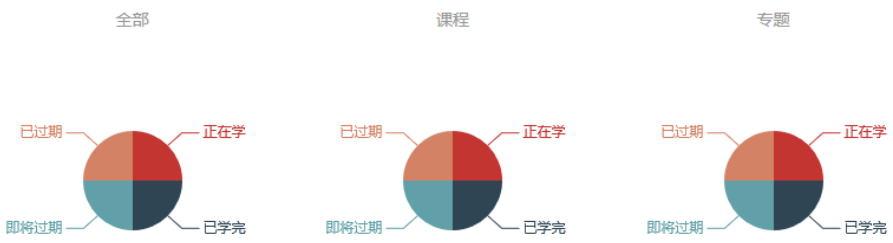
2.3个人中心

2.3.1学习概况

将鼠标移到界面右上角的头像，点击“个人中心”，在“学习概况”里面可以查看自己的学习情况，包括已学课程数，正在学的课程数，所有课程数以及学习时长。

课程概况

-	总数	正在学	已学完	即将过期	已过期
课程	3	0	0	0	0
专题	0	0	0	0	0



2.3.2我的成就

可以查看自己某一周的学习报告情况：

2.3.3账户信息

1）账户信息-个人信息：查看自己的账户信息，并且可以更改姓名及职位：

2）账户信息-修改密码：可以修改当前密码：

2.3.4账户认证

若学生在平台没有做过账户认证，则在下载学习资料时会显示点击认证，并且在“个人中心”的“学习概况”中显示未认证。

以上2处需要认证的地方，任点一处会跳到“账户认证”界面：

- 若该用户邮箱或手机号没有注册51CTO的任何一个账号，点击“获取验证码”，输入验证码之后，点“提交”即可。
- 若该用户已经注册51CTO平台账号，则需要输入注册的账号密码进行认证即可。
- 若用户在注册51CTO平台账号的时候提供手机号码，则认证的时候邮箱、手机号码任选一个认证即可。

2.4移动客户端

2.4.1下载方式

- 扫描下方二维码；

- 在各应用商店或搜索引擎搜索：51CTO企业IT学院；
- 在学校学习平台右侧，点击手机形状的图表。

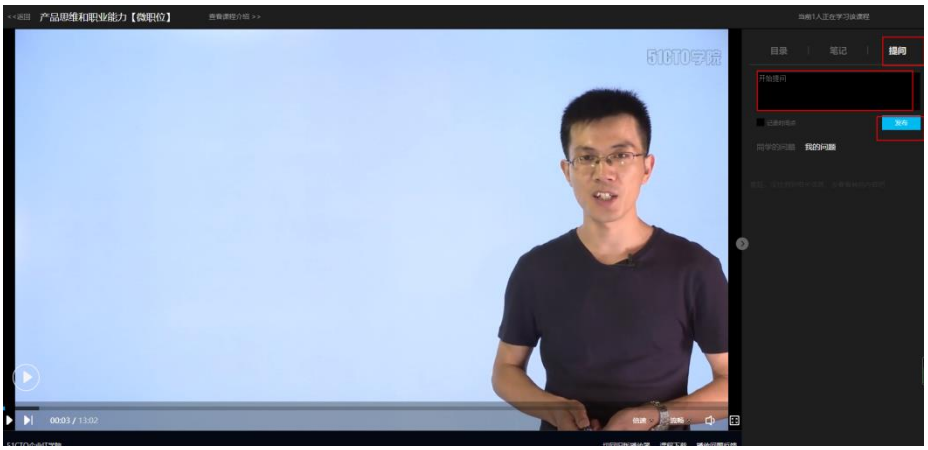
2.4.2支持设备

可支持手机,暂不支持iPad下载。

二．平台使用支持

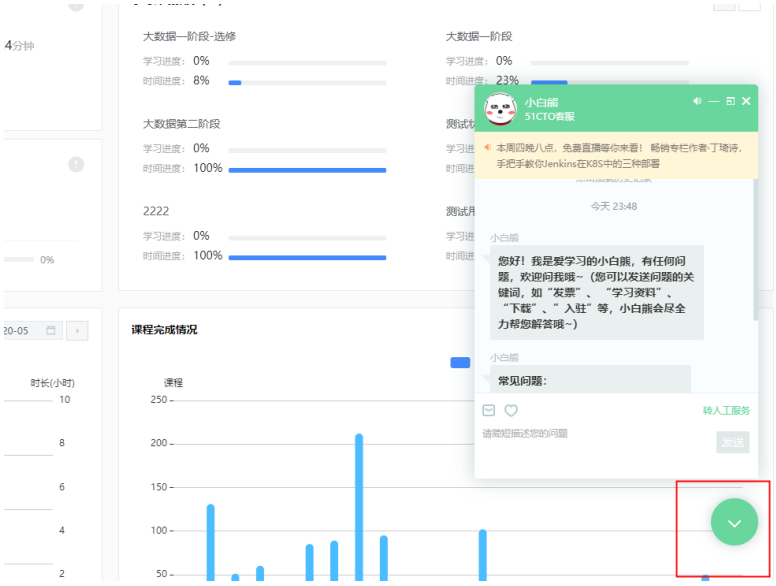
1.平台答疑支持

在线平台课程播放页设置有提问入口，使用过程中可以直接将问题提交，所提交的问题会进入到讲师后台，授课讲师会在问题提交的24小时内进行回复。



2. 在线客服

点击平台上的绿色按钮，可以联系人工客服，进行相关问题解答。

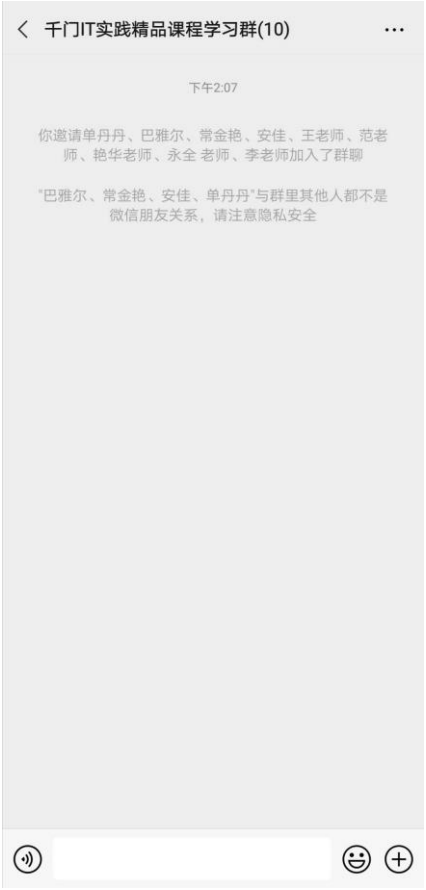


3. 运营微信群

建立专属微信群，匹配一名平台运营老师和一名活动运营老师，对合作高校进行对接服务。

活动运营老师主要负责：活动及咨询分享（每日晨报、技术专栏文章、51CTO打卡直播公开课免费名额、线上学习活动）

平台运营老师主要负责：使用问题答疑、课程问题使用支持。



三．平台应急处理机制

应急处置总则

本预案的适用范围为51CTO企业IT学院企业学习平台，测评平台，教育学习平台，短信服务平台等网络事件应急处理。

1.日常安全工作职责

运维部门工作人员根据分工、做好以下工作：

对网站、网络进行日常检查、分析风险、排除隐患、做好网站数据备份，形成日常工作机制，预防安全事故发生。

制定相关安全事件的预警方案和解决方案。

掌握网络技术发展趋势，不断提升安全防范水平。

及时处置各类突发安全事件。

1.1安全应急处置原则

报告原则：发生突发安全事件，第一时间向网站负责人报告，同时积极进行处置，处置全程要及时汇报工作进展。

安全原则：处理安全事件时，要科学客观，要保证设备数据安全。

效率原则：处置突发事件要及时迅速，讲究方法，善于协调，争取在最短时间内解决问题。

协调配合原则：出现大规模故障后，根据工作需求，积极配合，协同处理，提高工作质量与效率。

1.2信息安全应急事件

（一）安全事件分类

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备实施故障和灾害性事件等六类。

1、 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

2、 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

3、 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

4、 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

5、 设备设施故障事件分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

6、 灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

（二）安全事件等级

一般故障：指区域性网络安全事件，具体包括：局部网络瘫痪，个别服务及服务器停止工作等。

重大故障：指发生大规模或整体性网络瘫痪、个别硬件设备损坏或被窃、数据丢失或网站遭篡改破坏等。

特大故障：指机房发生火灾或遭可抗拒力破坏造成机房损毁等。

（三）处置时限

发生突发安全事件，一般故障2小时内解决，重大故障24小时内解决，特大故障48小时内解决。

（四）处置措施

1. 发生突发事件，工作人员第一时间报告领导进行处置。
2. 迅速准确判断事件原因，在保证设备、数据安全的情况下，进行针对性处置。
3. 属于一般性故障 ，运维人员及时进行处置。属于云网络系统故障的，联系云服务商进行处置。属于系统故障的， 要及时联系对应的系统维护人员进行处置，属遭受攻击的，要及时取证留存，并由系统维护人员进行处置。
4. 事后总结本次事件的处置情况，形成分析报告。

2.网站安全应急处置规范

2.1日常维护

（一）、检查各服务器运行和访问日志，及时升级补丁包。

（二）、每天对各网站系统及服务和数据进行备份，并传入存档服务器。

2.3安全事情分类及应急处置方法

（一）、恶意篡改事故处理预案

指网站系统信息遭到页面被篡改或出现非法信息。

1.一旦发现学校网站上出现不良信息（或者被黑客攻击修改 了网页），立刻关闭网站。

2.备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的

HTTP连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志。

3.打印不良信息页面留存。

4.完全隔离出现不良信息的目录,使其不能再被访问。

5.删除不良信息,并清查整个网站所有内容,确保没有任何不良信息,重新开通网站服务，并测试网站运行。

6.修改该目录名,对该目录进行安全性检测,升级安全级别,升级程序,去除不安全隐患,关闭不安全栏目，重梳妆打扮开放目录的网络加接，并进行测试，正常后，重新修改该目录的上级链接。

7.全面查对HTTP日志,防火墙网络连接日志,确定该不良信息的源IP地址,全面升级此次事件为最高紧急事件，立刻向领导小组组长汇报，视情节严重程序领导小组可决定是否向公安机关报案。

8.从事故一发生到处理事件的整个过程,必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

（二）网络恶意攻击事故处理预案

指网站系统遭到网络攻击不能正常运行。

1.发现出现网络恶意攻击，立刻确定该攻击来自局域网内还是互联网上。受攻击的设备有哪些，影响苦海无边有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断服务器及互联网的相关服务，以保护重要数据及信息。

2.如果攻击来自互联网，立刻从防火墙中查出对方IP地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

3.如果攻击来自局域网内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台服务器。关闭该服务器的对外数据包，并立刻对该服务器进行分析处理，确定攻击出于无意、有意还是补利用。

4.重新该服务器所连接的网络设备，直至完成恢复网络通信。

5.对该服务器进行分析、清除所有病毒，恶意程序、木马程序以及垃圾文档，测试运行该电脑5小时以上，并同时进行监控。

6.从事故一发生到处理事件的整个过程，必须保持向领导小组汇报、解释此次事故的发生情况、发生原因、处理过程。

（二）、病毒木马类故障

指网站服务器感染病毒木马，存在安全隐患

1. 每周对服务器杀毒安全软件进行系统升级，并进行病毒木马扫描，封堵系统漏洞。
2. 由于病毒木马入侵服务器造成数据丢失或系统崩溃的，第一时间报告责任人，并联系相关维护人员进行数据恢复。
3. 发现服务器感染病毒木马，要立即对其进行查杀，报告负责人，根据具体情况，酌情通知相关服务器进行终端的病毒木马查杀。

（三）、系统类故障

指网站系统由于长时间运行或系统存在的bug造成网站不能正常运行。

1. 相关维护人员每天要对数据进行备份和存档。

2. 发现此类问题，要报告负责人，并联系网站运维人员进行检测修复。

（四）、应急保障

1、记录网站 IDC 托管机房、云运营商大客户经理、 服务器供应商及网站维护负责人电话，出现问题能及时联络处理。

2、运维人员应掌握应急服务器数据备份和恢复的使用。

3、运维人员应学习各类软硬件知识，提高应对和处理 突发网络故障的能力

3.硬件设备应急处置

3.1适用范围

信息中心负责建设管理的网络安全事件

3.2日常维护

1. 每季度对设备进行例行检查及卫生保洁，检查项目包括设备运行状态，温度、供电及设备周边环境是否安全。
2. 每月对各机房进行实地走访，查看实际情况。

3.3应急处置

1、发生故障后，首先排查故障范围，确定是软件故障 还是硬件故障，是光路故障还是以太网故障。

2、对于大面积网络故障或硬件线路设备损坏，要第一时间报告负责人。

3、如发生光路设备故障，及时联络运营商客户经理协调处理。

4、如发生以太网故障，要及时进行处理，必要时联系 设备供应商及相关单位联合处理。

3.4机房及办公区安全应急处理

（一）、用电安全

（1）坚持正确的用电规范。

（2）不使用超负荷电器设备。

（3）不随意改变工程设计的供电线路。

（4）每天下班，最后离开办公室的人员关闭办公区主 电源。

（5）每个月对机房各电源设备进行检查。遇节假日， 除关闭办公区主电源外，检查机房内电源和线路，确保设备安全稳定运行。

（6）外电中断后，应立即查明原因，并向负责人汇报。

（7）如因机关内部线路故障，请机关物业公司迅速恢复。

（8）如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

（9）如果供电局告知需长时间停电，应做如下安排：

1、预计停电 4 小时以内，由 UPS 供电。

2、预计停电 24 小时，请示负责人，关掉非关键设备， 确保关键设备供电。

3、预计停电超过 24 小时的，关闭机房所有管辖设备，并通知服务器的相关维护人员进行设备停机。

（10）机房及各设备恢复供电时，执行以下步骤：

1、机房恢复供电前，首先确认各设备的电源态处于下 电状态，以防止电源柜加电对设备的冲击。

2、等待 10--20 分钟后，开始给电源柜加电，以防止供电不稳或再次掉电。

3、供电正常后，确定设备处于下电状态后，打开电力柜的总控开。

4、根据设备加电顺序，启动分项控开。

5、启动数据库及各项应用程序。

（11）发生火警事件发生后，机房人员应根据所属区域和现场情况， 判断和选择正确的方法，及时上报负责人，同时配合相关人员处置，降低事件带来的影响。

1、对于设备发生烟雾，机房主管人员协同相关人员寻找烟雾点并切断相关区域电源。

2、当设备发生可以控制火情时，机房主管人员应协同相关人员进行灭火工作。

3、当主机房发生火灾而无法控制，应采取施救方法等措施。

（二）、空调及通风设备

正常情况：

温度：冬季： 18℃-20℃±2℃ 夏季： 18℃-23℃±2℃

温度变化≤5℃/H

湿度: 40%-50%±5%

一、 每周对机房温湿度进行监控，防患于未然。

空调系统故障导致机房内温度、湿度升高或设备出现温度告警等异常现象时，执行以下步骤：

（1）首先查看故障空调的位置和现象，联系空调厂家加紧维修。

（2）如果故障较为严重，影响范围大，则立即汇报给负责人。

（3）启用备用风扇、加湿器等设备降低室内温度、湿度，并打开机柜门和房间门，以便于设备散热和空气流通。

（4）相关工作人员要密切注意各设备的运行情况，如出现告警，查看日志了解情况，必要时请设备厂家派人立即赶到现场进行技术支持。

（5）相关负责人员对各个维护业务进行检查，如已经影响到系统和业务的正常运行，尤其是一些重要业务，应立即汇报负责人，做进一步处理。

（6）若此时空调已修好，室内温度、湿度恢复正常或在下降中，相关负责人员对各个设备的运行情况详细检查，确保恢复正常。

（7）待室内温度、湿度恢复正常并监控一段时间后无异常，将备用风扇、加湿器关闭并放回原位，保持机房卫生和整洁。

（8）相关负责人员对此次故障做好记录。

（三）、核心设备安全

（1）根据实际情况对核心设备进行检查，确保设备安全稳定运行。

（2）发生核心设备硬件故障后，工作人员应及时报告负责人，并查找、确定故障设备及故障原因，进行先期处置。同时联系设备提供商共同检测并排除故障。

（3）若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（4）故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系厂商进行返厂维修或调换设备。

（四）、数据安全与恢复

（1）日常维护参照《网站安全应急预案》中"一、日常维护"各项进行。

（2）发生业务数据损坏时，工作人员应及时报告负责人，检查、备份系统当前数据。

（3）信息中心负责调用备份服务器备份数据，若备份数据损坏，则调用异地光盘备份数据。

（4）数据损坏事件较严重无法保证正常工作的，经部门领导同意，及时通知各部门以手工方式开展工作。

（5）运维人员应待数据系统恢复后，检查基础数据的完整性；重新备份数据，并写出故障分析报告。

五、其他事项

（一）无关人员未经负责人批准不得进入机房。

（二）对各设备和线路进行维护或改造，需经负责人批准，由工作人员陪同进行。

（三）使用充分控干水份的抹布及拖把进行保洁，尽量不使用干布或扫帚，避免扬尘。

（四）保洁时，注意不要触碰电源接口及网络接口等，以免漏电或导致线路接触不良。