前途千屿会议服务平台

NEXUS ARCHIPELAGO MUN

# 让协作有边界，
# 让信任有依据。

## 千屿平台安全白皮书

公开版 2.0 / 安全措施与共同责任

**一个账号，多个会场。**
**每一次访问，都应符合当前身份与授权。**

面向参会用户、会议主办方与合作伙伴，说明账号保护、会议隔离、资料处理、内容审核及安全运行的基本机制。

运营主体

**前途出国留学服务（广州）有限责任公司**

功能与证据核对日期：2026 年 10 月 17 日

本文件为公开说明，不是第三方测评报告、合规认证证书或无风险保证。

01 / 范围与结论

# 如何阅读这份白皮书

安全承诺应建立在可核实的措施上，也应保留清楚的适用边界。

## 核心结论

千屿平台已围绕账号认证、会议与委员会授权、重复提交保护、内容审核、审计记录和备份恢复建立应用层控制，并完成阶段性内部验证。本版依据分项回归与发布验证，不能据此认定全站无漏洞；本文件不将内部测试表述为正式等级保护测评。

## 覆盖范围

本文件覆盖平台注册与登录、会议报名、管理授权、会场协作、公开内容与资料处理。只说明截至核对日期有依据的控制目标及使用边界；个别环境与真实移动终端仍需专项验证；不公开内部部署拓扑、配置参数、攻击复现或运维凭据。

## 内容导航

03 身份、授权与会议隔离
04 账号与会话保护
05 个人信息与数据生命周期
06 报名与操作完整性
07 内容审核与 AI 边界
08 学术文件分工与流转
09 打印水印与资料使用
10 安全运行与恢复能力
11 验证范围与证据口径
12 共同责任与问题报告
13 治理边界、参考与版本

> **公开透明与必要保密**
>
> 不披露攻击细节，不等于省略安全边界。白皮书公开控制原则与限制；具体问题通过受控渠道核实与处理。

02 / 访问控制

# 身份真实，权限有范围

身份来自个人账号，权限来自当前会议与委员会中的有效授权。

## 服务端作出授权判断

受保护操作需要有效身份，平台在服务端核对用户、会议、组织及具体职责。页面传入的会议编号、用户自行修改的角色文字，不能替代正式授权。是否能看到按钮，也不是权限判断的依据。

| | |
|---|---|
| **平台管理** | 超级管理员承担平台维护与授权管理职责；权限集中意味着更高的保管和复核责任。 |
| **会议与委员会管理** | 一级管理员负责本会议；二级管理员管理获授权委员会。普通学术管理员和组委管理员按职责获得相应范围。 |
| **代表与私密分组** | 代表依据报名、席位及分组资格使用会场功能；不能借在另一场会议的身份查看当前会场私密资料。 |

## 授权撤回与角色交接

撤权、退出分组或交接生效后，后续访问重新核对当前权限。中心工作人员与同委员会分组接收人分开配置；关键负责人转让要求核对接任人并记录变更。

> **边界说明**
>
> 会议之间隔离的是相应业务资料与授权范围；这是应用权限控制，不应被理解为每场会议各有一台独立物理服务器。

03 / 身份鉴别与会话

# 账号保护从本人控制开始

一个人使用自己的邮箱账号，避免共享代表账号或管理账号。

## 验证邮箱，保护口令

注册通过邮箱验证码核验邮箱控制权，实行唯一邮箱账号与口令复杂度要求。密码以散列形式保存，不按明文保存。联系手机为选填资料，不应被当作已经完成短信验证的身份凭据。

## 找回密码与敏感操作

忘记密码可通过注册邮箱的重置验证码恢复访问。关键流程采用人机验证、登录失败保护及频率控制；会话有效性与注销处理限制旧会话继续使用。找回流程不能替代对邮箱控制权的核实。

## 传输、来源和操作确认

公开访问采用 HTTPS，并启用浏览器强制加密访问策略。需要身份的请求接受会话与来源相关校验，敏感操作结合操作确认与服务端校验，降低跨站请求和重复写入风险。浏览器安全警告不应被视为可以忽略的步骤。

### 你可以做的三件事

使用独立且足够强的密码；不转交验证码；共用电脑用完即退出。发现账号异常，通过站内联系核实，不把密码发给工作人员。

04 / 个人信息与数据生命周期

# 按用途处理，按范围提供

公开资料与会务私密资料采用不同的展示范围；姓名和角色抬头也属于需要审慎使用的信息。

| | |
|---|---|
| **公开内容** | 会议介绍、经审核公开的文件和博客可由访客阅读；会议作者标识随相关会议的公开状态展示，未公开或演示会议身份不作公开背书。 |
| **报名与联系资料** | 报名表、成员邮箱、选填手机、住宿需求及凭证供本人和有职责的人员使用，不因会议公开而一并公开。 |
| **学术私密资料** | 学测答案、个人席位、内阁或党团指令、内部反馈按委员会、分组与流转职责控制访问。 |

## 减少不必要的披露

公开数据输出采用必要字段筛选与规则脱敏。代表团成员查看自己的报名摘要，不能由此查看其他团员完整资料或团体凭证。规则处理不是对所有图片、自由文本和变形个人信息的全量识别保证。

## 更正、注销与保留

用户可按页面更正资料、清空选填手机或申请注销。注销不等于所有会务记录即时消失；仍需核验或依法保留的信息限制用途。保留、删除与备份处理以隐私政策和核实后的请求为准。

> **上传前先最小化**
>
> 公开文件不放私人联系方式；凭证遮住无关余额与交易；住宿备注只填协调所必需的信息。

05 / 报名与操作完整性

# 业务结果由服务端确认

即时预估帮助填写，正式结果以服务端确认的名单、名额、金额和流程状态为准。

01 **名单与名额核对**

根据实际参会名单和所选委员会计算人数；有限额时先预留，再继续后续步骤。

02 **正式提交与并发控制**

名额变更与报名写入保持一致，重复提交采用操作保护，降低多次点击产生重复记录的风险。

03 **人工核验与状态流转**

到账、报名结果与学术流程按各自职责处理。上传截图、内容审核通过或预留成功，不代表其他状态自动通过。

## 重复操作与失效请求

平台结合操作编号、时效校验和会话相关保护处理关键写入。请求被拒绝或结果不确定时，正确做法是查看已有记录，而不是反复发起新操作。不同业务对重复操作的反馈可能不同。

> **不把前端当作安全边界**
>
> 修改页面上显示的价格、门槛、人数或状态，不应改变服务端的业务判断。预留过期且已付款时，应联系主办方处理。

06 / 人工、规则与 AI

# 内容审核与文件安全分开看

审核是否适合公开，不等于证明附件没有恶意内容，也不等于授予额外访问权限。

## 处理范围与分工

博客、需审核的频道正文及可处理的公开文件文本可进入辅助审核。AI 仅在已启用范围内工作；不确定内容交人工复核。内容修改后，旧版本的分析结果不得覆盖新的内容或人工决定。

## 资料检查不评判个人资格

报名完整性由确定性规则检查必要字段。模型不用于自动决定录取、席位、管理员授权、实际到账、匿名投诉结论或中心推演。自动通过比例不代表准确率，也不是对用户的结果承诺。

## 处理数据与文件边界

现有内容审核模型本地部署，审核正文不发送给外部 AI 服务。只处理适用范围内的必要文本；报名个人资料与私密指令不因开启审核助手而进入模型。上传采用类型、结构与权限检查，复杂附件仍需人工审阅。

### 人工保留最终处理权

排队、不可解析或服务异常不应被当作自动通过。对审核结果有异议可申请人工复核；收到文件时仍不要运行不明程序或宏。

07 / 学术协作与职责分离

# 把文件交给正确的人

内容可见范围随职责分配，不因参与同一会议就默认共享全部文件。

01 **分组负责人发起正式提交**

国会委由党首、危机联动由内阁首脑提交；普通成员的个人特别渠道需由对应管理员开放。

↓

02 **接收管理员整理后转交**

按负责分组接收材料，重新上传给中心的文件包。一位接收人可以负责多个内阁或党团。

↓

03 **独立指定的中心工作人员处理**

国会委使用会议指导中心，危机联动使用推演中心；中心读取已转交文件包，回传接收管理员。

↓

04 **接收管理员发送最终反馈**

将可向代表提供的结论与附件送达。正式分组反馈按分组展示，个人特别提交按个人范围展示。

独立委员会采用代表向指定学术接收人直接提交的路径；学测仍由负责委员会的二级管理员发布与接收，不能混作文件流转。

> **避免自审与越级处理**
>
> 同委员会的中心人员与分组接收人不得兼任；流转次序、接收范围和附件访问由服务端校验，不能靠切换页面跳过。

08 / 水印与离线资料

# 打印留标识，使用有责任

水印用于保密提醒和辅助溯源，不替代访问控制，也不构成不可泄露保证。

## 网页打印的归属提示

敏感管理页面在打印或另存 PDF 时显示归属水印，包含当前账号标识、脱敏邮箱与北京时间；正常浏览保持清晰。身份未完成校验时，应先完成登录，不应输出无归属的敏感内容。

示意 / 非真实账户

账号 ID：示例标识
l***@example.invalid
2026 年 10 月 17 日 09:30（北京时间）

## 学术文件的打印副本

适用的 PDF 可生成带水印打印版，保留原文件独立存放。打印副本的时间是生成时间；再次使用时可刷新。不同阅读器对打印图层支持不同，输出前应检查预览及每页标识。

## 离开平台后的责任

下载、打印或获得授权不等于可以公开转发。持有人应核对收件人、避免上传公开网盘，并在用途结束后按会议管理要求处理副本。水印不能代替对泄露事件的证据核实。

### 功能边界

Web 页面不检测系统截屏。裁剪、编辑、转拍和阅读器差异均可能影响标识；水印仅作为辅助线索。

09 / 安全运行与持续改进

# 可观察、可恢复、可核对

运行能力以实际监控、备份和恢复证据为基础，不只以“已设置定时任务”作为完成标准。

## 监控与异常处理

平台监控服务健康与备份状态；告警邮件已完成实际收件确认。告警发送采用次数限制，日志采集采用容量保护，避免异常扩大资源消耗。外部请求限制目标与重定向；可用性仍受终端网络及访问链路影响。

## 审计记录与责任追踪

重要操作记录相应操作者、业务范围、动作与时间，用于排查和责任核对。安全日志按不少于六个月的策略管理，访问受职责限制；持续核对容量、留存与完整性。设置留存策略不等于已经积累完整长期历史。

## 备份与恢复验证

最新发布前备份覆盖数据库、附件与运行配置，并在隔离环境实际执行恢复和一致性核对。备份可用性、恢复后权限以及业务数据完整性都需复核。小样本演练的耗时不应被直接当成正式恢复时间承诺。

> **持续建设，不作未经证明的保证**
>
> 灾难恢复、长期审计、主机防护与组织流程需要持续验证。本文件不宣称已达到跨地域容灾、零数据损失或全天候即时恢复。

10 / 安全保证的证据口径

# 验证说明：看范围，也看限制

截至核对日期，已有阶段性内部验收记录；本次编写白皮书没有重新执行一轮完整渗透测试。

| | |
|---|---|
| **身份与授权** | 已覆盖不同会议间的越权尝试、代表调用管理功能、失效或伪造身份等代表性场景。 |
| **数据与操作完整性** | 已覆盖公开输出检查、重复写入、业务参数篡改、并发名额控制与关键流转约束。 |
| **应用安全检查** | 结合自动化扫描与手工验证，检查已选入口和业务路径；测试使用隔离环境及合成数据。 |
| **回归与恢复** | 发布前完成业务、前端、后端及独立日志服务回归，发布后连续观察服务健康，并保留回滚准备；不将跳过项计为通过。 |

## 如何解读阶段性结果

所列内部测试范围内，已发现的严重和高危问题完成修复复测后方可关闭；未发现或已关闭，不代表不存在未知风险。整体安全验收仍有覆盖边界，后续改进与终端兼容性验证继续按内部记录跟进。

> **不把内部自测当作外部认证**
>
> 本白皮书不等于第三方渗透测试证书或等级保护测评结论。正式定级、备案及测评由运营方另行组织，并以正式材料为准。

11 / 共同责任与反馈

# 安全由平台、主办方和用户共建

请优先通过网站“咨询 / 站内联系”提交问题；公开评论区不适合承载敏感证据。

| | |
|---|---|
| **平台维护人员** | 维护访问控制、运行监控与备份；核实报告、处理授权问题并记录整改。重大变化需同步相关说明。 |
| **会议负责人及工作人员** | 准确配置委员会与分组权限，及时交接和撤权；核对公开文件与影像授权；妥善保存导出和打印资料。 |
| **参会用户** | 使用自己的账号，保管密码与查询码；核对目标会议和上传范围；发现异常时停止进一步传播并报告。 |

## 报告问题，先提供最少必要信息

说明发生时间、页面名称、会议名称、预期结果和实际现象。截图请遮盖无关个人资料。不要发送密码、验证码、访问令牌或完整报名库；需要进一步证据时，由平台提供受控沟通方式。

## 问题处理建议流程

提交线索 → 核实影响与权限 → 控制风险 → 修复并复测 → 按适用情况沟通结果。不得为验证问题而访问他人私密资料、扩大探测范围或中断服务；公开说明不构成主动测试授权。

> **保留回执**
>
> 保存站内联系查询码并用于后续查询。账号或报名争议由相应负责人核实；内容审核异议可请求人工复核。

12 / 参考与后续更新

# 治理边界与版本说明

以功能证据、公开政策与正式测评材料各自说明其能够证明的事项。

## 等级保护与治理

运营方已开展等级保护相关技术差距自查，应用安全控制只是其中一部分。制度建设、人员职责、正式定级备案与第三方测评需另行落实；本文件不宣称已通过二级测评。

## 个人信息与第三方服务

使用云基础设施、邮件或访问加速服务时，需按实际处理链路明确责任与数据范围。模型本地运行不等于所有网络链路均不涉及第三方。用户权利、保留期限与未成年人保护须结合实际流程及适用规则落实；本文件不证明所有治理要求已完成。

## 参考资料与使用方式

### GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

国家标准公开信息；用于治理参照，不表示已经取得认证。

### OWASP Application Security Verification Standard

应用安全验证参考；引用该框架不代表全部条款已验证。

### 千屿平台隐私政策与用户协议

请从当前网站页脚进入，查看最新说明与联系入口。

### 版本依据与更新

公开版 2.0 · 2026-10-17。更新公开身份边界、密码找回、告警与容量保护、受控外部请求及发布恢复证据。不公开内部配置与攻击复现细节。