# 网站《APO 的 OJ 成果展示》网络安全应急预案

## 一、日常安全工作职责

网站管理者需要做好以下工作:

1、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。

2、制定相关安全事件的预警方案和解决方案。

3、掌握网络网站技术发展趋势，不断提升安全防范水平。

4、及时处置各类突发安全事件。

## 二、安全应急事件分类

1、一般故障: 指一般性网络安全事件, 具体包括: 局部网络瘫痪、SSL 证书异常、DNS 异常、网站服务器停止工作等。

2、重大故障：指发生大规模或整体性网络瘫痪、或被窃、数据丢失或网站遭恶意篡改破坏等。

## 三、安全应急事件处理时限

1、对于一般故障， 24 小时内解决;

2、对于重大故障， 12 小时内解决;

## 四、安全应急事件处理措施

**1、一般性的 DNS、SSL 证书等异常**

由网站管理员查看具体情况，设置 DNS 解析、SSL 证书续费等。

必要时可以进行重启操作。

**2、攻击、篡改类故障**

发现网站出现非法信息或页面被篡改，要第一时间对其进行删除，恢复相关信息及页面；若在 2 小时内无法恢复，则需要关闭网站服务器，待检测无故障后再开启服务。

故障修复后立即追查非法信息来源，将有关情况进行记录，情况非常严重的要向公安部门报案。

**3、病毒木马类故障**

发现服务器感染病毒木马，要立即对其进行查杀，根据具体情况，酌情发布网站公告并联系网站提供商提供帮助。

由于病毒木马入侵服务器造成数据丢失或系统崩溃的，要第一时间关闭网站进行保护，并联系服务器提供商进行数据恢复。

每周对服务器各个常用软件进行升级，封堵系统漏洞。、

## 五、应急保障

1、记录网站域名 DNS 提供商、服务器提供商的联系方式，出现问题能及时联络处理。

2、网站管理员应学习各类网络故障知识，提高应对和处理突发网络故障的能力。