

附件 4 《网络安全管理须知》

1. 总体要求

参展商、搭建商或服务商须认真贯彻中华人民共和国、上海市有关网络安全管理的方针及政策,严格执行各项法规、条例和规定,包括《中华人民共和国网络安全法》《中华人民共和国电信条例》《全国人民代表大会常务委员会关于维护互联网安全的决定》《计算机信息网络国际联网安全保护管理办法》《互联网安全保护技术措施规定》及有关法律、法规和行政规章制度、文件规定。

2. 接入须知

- 2.1 展会现场提供有线网络宽带和免费公共无线WiFi接入两种上网方式,用户自备网络接入设备(如路由器、电脑、智能手机等)。
- 2.2 展会现场有线网络宽带应按照承办单位互联网申请流程办理网络开通相关事宜,不得自行从其他途径申请互联网接入服务。未经报备从非官方途径接入互联网,承办单位有权暂停该用户的互联网接入。对于情节严重者,承办单位将配合有关部门依法对相关责任人进行查处。
- 2.3 承办单位有权采用技术手段监控网络的使用情况。如未经批准,利用所申请的网络资源开展经营性活动(如有线宽带跨摊位组网、有线宽带转无线信号组网等),承办单位有权追缴相关网络费用并采取断网、禁止接入等相关措施。
- 2.4 参展商、搭建商或服务商不得损坏展馆内的网络设施或租赁设备;如有损坏,须承担相关赔偿责任。

3. 安全管理

- 3.1 遵守中华人民共和国有关网络安全的法律法规、公共秩序及社会公德,不得危害网络安全;不得利用网络从事危害中华人民共和国国家安全、荣誉和利益,煽动颠覆中华人民共和国国家政权,推翻社会主义制度,煽动分裂、破坏中华人民共和国国家统一的活动。
- 3.2 不得利用网络宣扬恐怖主义、极端主义,宣扬民族仇恨、民族歧视,传播暴力、淫秽色情信息;不得编造、传播虚假信息扰乱经济秩序和社会秩序,非法获取个人信息以及侵害他人名誉、隐私、知识产权和其他合法权益。
- 3.3 根据中华人民共和国有关网络安全的法律法规,参展商、搭建商或服务商工作人员需要联网的,需身份验证登录,留存用户注册信息,并在必要时配合政府有关单位,提供相关数据。
- 3.4 参展商、搭建商或服务商须合理使用网络服务,不得私自对外提供WiFi热点;如存在影响网络安全及正常运营的情况,承办单位有权终止使用网络。
- 3.5 网络具有一定的开放性,参展商应自行做好计算机安全防护,打好系统补丁,安装安全管理及防病毒软件,以防止个人信息的泄露。因个人信息泄露而导致的一切后果须自行承担。
- 3.6 如果参展商自行搭建电子大屏对外进行展示的,应安排专业人员进行管理;电子大屏需要连接互联网的,应当做好防侵入、防篡改、防干扰、防未经授权的设置。
- 3.7 为确保网络服务安全、平稳运行,承办单位有权在未经提前告知的情况下,在部分时段对部分区域进行网络管制,调整或禁止部分网络访问端口(如证券、BT、迅雷、游戏等)的访问权。