网站管理制度

为了进一步加强基金会网站的管理与维护，充分发挥网站的作用，促进基金会内外部信息交流与沟通，及时掌握反馈信息，拓展交流渠道，提高网站管理水平，扩大基金会对外知名度，提升外部形象，制定本管理规定：

一、信息的搜集与发布

（一）网站管理员负责网站内容信息的搜集和整理，各部门主管或专人根据部门职能及时向网站管理员提供最新相关信息。重大事务、外事活动、访问考察活动活动、会领导重要出访活动等信息由办公室提供。

（二）网站管理员及时对各部门提供的信息，进行统一分类、整理、汇总成发布稿件按下列程序审批后发布：网站需报送、上传的信息要逐级审核。重要信息需报经会长审核把关，方可上传。信息资源必须遵循“谁发布，谁负责；谁承诺，谁办理”原则。所有经过部门负责同志审核的信息，要及时存档备查。

二、网站管理员管理制度

未经批准，基金会网站管理员不得随意发布信息或更改网站页面版式及内容；不得在基金会网站上发布违反国家法律、法规、有损国家利益、基金会形象以及不道德的言论；不得利用基金会网站传播反动、淫秽、不道德以及其他违反国家法律、社会公德的信息；不得利用基金会网站发布虚假信息或违反基金会规定、影响基金会形象、泄露基金会机密的信息。 网站管理员一经发现有上述内容的信息，必须立即予以删除，并追究当事者的行政或法律责任。

三、信息保密制度

网站发布的任何信息都必须遵守《中华人民共和国保守国家秘密法》、《中华人民共和国计算机系统安全保护条例》、《计算机信息网络国际安全保护管理办法》、《计算机信息系统国际联网保密管理规定》等有关国家政策、法规规定。

口令管理制度。网站应当设置后台管理及上传的登录口令。口令的位数不应少于8位，且不应与管理者个人信息、单位信息、设备（系统）信息等相关联。每三个月须更换一次网站登录口令，严禁将各个人登录帐号和密码泄露给他人使用。同时，根据国家有关保密法律、法规，严禁涉密信息上网。

四、网络安全管理制度

（一）安全测评制度。网站系统应当由信息化管理办公室按照《计算机信息系统安全测评通用技术规范》的要求，对系统安全性进行测评。

（二）服务器和网站定期检测制度。网站应及时对网站管理及服务器系统漏洞进行定期检测，并根据检测结果采取相应的措施。要及时对操作系统、数据库等系统软件进行补丁包升级或者版本升级，以防黑客利用系统漏洞和弱点非法入侵。

（三）客户端或录入电脑安全防范制度。网站负责人、技术开发人员和信息采编人员所用电脑必须加强病毒、黑客安全防范措施，必须有相应的安全软件实施保护，确保电脑内的资料和帐号、密码的安全、可靠。

（四）应急响应制度。网站应当充分估计各种突发事件的可能性，做好应急响应方案。同时，要与岗位责任制度相结合，保证应急响应方案的及时实施，将损失降到最低程度。

（五）安全事件报告及处理制度。网站在发生安全突发事件后，除在第一时间组织人员进行解决外，应当及时向会信息处报告，由其给予及时的指导和必要的技术支持，并视安全突发事件的严重程度，及时协调公安、电信通等部门进行处理。

（六）人员管理制度。网站应当制定详细的工作人员管理制度，明确工作人员的职责和权限。要通过定期开展业务培训，提高人员素质，重点加强负责系统操作和维护工作的人员的培训考核工作，实行考核上岗制度。同时，规范人员调离制度，做好保密义务承诺、资料退还、系统口令更换等必要的安全保密工作。

五、网站更新与维护

网站管理员应按照规定及时对基金会网站进行管理、维护与更新，保证信息及时性、通达性、有效性。有关设备要定期巡检，保证网站每天 24 小时正常开通运转，以方便公众访问。

定期备份。网站管理员应当对重要文件、数据、操作系统及应用系统作定期备份，以便应急恢复。特别重要的部门还应当对重要文件和数据进行异地备份。