北京弘医医学发展基金会
BEIJING HONGYI MEDICAL DEVELOPMENT FOUNDATION

北京弘医医学发展基金会网络与信息安全管理办法

（2019）第 1 号

第一章　总　则

第一条　为加强北京弘医医学发展基金会网络与信息安全以及计算机信息保密工作，进一步促进“互联网+医疗健康”发展，加强网络安全管理，防范网络安全事件发生，根据《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网安全保护管理办法》《基本医疗卫生与健康促进法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》以及网络安全等级保护制度等有关法律法规标准制定本办法。

第二条　本办法适用于北京弘医医学发展基金会全体工作人员

第三条　本办法规定北京弘医医学发展基金会全体工作人员在网络与信息安全方面的行为规范，明确北京弘医医学发展基金会网络管理人员保护北京弘医医学发展基金会网络、计算机安全环境的责任及相关情况下的安全要求。

第四条　本办法中网络与信息安全内容包括计算机及其相关配套设备、设施（含网络）的安全、运行环境的安全、数据和信息的安全等。

第五条　组织管理与职责

（一）北京弘医医学发展基金会秘书长办公会议是网络与信息安全的决策机构。办公室是管理和执行部门。

（二）办公室负责制定网络与信息安全相关管理制度；负责网络与信息安全保障体系建设；协调、监督和检查各部门网络与信息安全工作；承担信息安全应急协调工作，协调处理重大信息安全事件。

第二章　工作人员管理细则

第六条　计算机硬件设备安全管理

（一）各部门对本部门的所有计算机设备有保管责任。

（二）计算机只有网络安全管理员进行维护时有权拆封，其他工作人员不得私自拆封。

（三）工作人员应对计算机设置开机密码和屏保密码，暂时离开岗位时，应锁定计算机屏幕，计算机设备不使用时，应关掉设备的电源。

（四）计算机为北京弘医医学发展基金会固定资产，不得私用或转让借出；除笔记本电脑外，其它设备严禁无故带出办公场所。

（五）计算机及周边设备、计算机操作系统和所装办公软件均为北京弘医医学发展基金会财产，计算机使用者不得随意损坏或卸载。

（六）工作人员私人计算机及其他设备未经允许不得连接到北京弘医医学发展基金会网络。

（七）禁止使用会干扰或破坏网络上其它使用者或节点的硬件系统，禁止在北京弘医医学发展基金会办公区域内私自搭建路由器、交换机等电子设备。如发现工作人员因私自搭建以上设备，造成北京弘医医学发展基金会网络无法正常运行的情况，将追究其个人责任。

第七条 计算机系统应用及软件安全管理

（一）未经允许，工作期间，工作人员不得在网上观看或下载电影、电视剧等，不得使用电驴、BT、PPLive、QQLive、PT 等严重占用带宽的 P2P 下载软件，不得利用北京弘医医学发展基金会计算机及网络资源玩游戏。

（二）禁止在北京弘医医学发展基金会内使用 VPN 等翻墙软件，一经发现，将立即终止其网络访问权限。

（三）不得利用北京弘医医学发展基金会的网络资源发布或传播迷信、暴力、反动等信息，违者将移送公安机关处理。

（四）不得利用计算机技术及北京弘医医学发展基金会的网络资源进行入侵、破解、篡改网站、服务器等网络犯罪行为，一经发现将立即终止其网络访问权限，移送公安机关处理。

（五）北京弘医医学发展基金会计算机的 IP 地址由网络安全管理员统一规划分配，工作人员不得擅自更改其 IP 地址，更不得恶意占用他人的 IP 地址。

（六）北京弘医医学发展基金会各类授权计算机软件，统一由办公室负责保管。工作人员因业务需要使用时可提出申请，填写《软件安装申请单》，由办公室根据该软件的授权使用范围进行安装。

（七）工作人员不得将北京弘医医学发展基金会授权软件进行私自拷贝、转于他人。对于保管或使用的软件不可盗卖、循私营利或进行其他不法事情，一经发现，将追究当事人责任。

（八）重要资料、电子文档、重要数据等不应存放在计算机桌面、我的文档和系统盘（一般为 C 盘），以免系统崩溃导致数据丢失。与工作相关的重要文件及数据应保存两份以上的备份，以防丢失。

第八条 帐号与信息安全管理

（一）工作人员应对保管和使用的计算机操作系统和所安装软件帐号登录信息严格保密，初次使用时须更改默认密码，密码应满足复杂性原则，长度应不低于 8 位，并由大写字母、小写字母、数字和标点符号中至少 3 类混合组成；对于因为软件自身原因无法达到要求的，应按照软件允许的最高密码安全策略处理。

（二）北京弘医医学发展基金会综合管理信息平台、官方网站、邮箱等属于北京弘医医学发展基金会版权的系统或平台的帐号必须由本帐号授权工作人员使用，不得将帐号授权给他人使用。

（三）北京弘医医学发展基金会登记注册的银行、第三方支付平台、财务管理、人力资源、微博、微信等平台、专用软件及社交媒体上的北京弘医医学发展基金会帐号必须由本帐号授权工作人员使用，不得将帐号授权给他人使用。

（四）任何人不得将工作中使用的各类软件、系统、平台等帐号登录信息告知他人或发布、传播到互联网。

（五）北京弘医医学发展基金会各类软件、系统、平台中所产生的一切文件、资料、图表和数据以及各类编码、目录等均属于北京弘医医学发展基金会信息资源范畴，任何人不得擅自泄露以上信息资料和数据，不得发布或传播到互联网。

由于工作人员个人安全管理不到位，造成泄密并致使单位利益受到损失，应追究相关责任人的责任。

第九条 防病毒管理

（一）病毒防治管理是计算机信息系统安全的一个重要组成部分，北京弘医医学发展基金会全体工作人员应提高防范计算机病毒的安全意识，切实履行各项职责。

（二）未经办公室同意，不得私自在计算机中安装非北京弘医医学发展基金会统一规定的

任何防病毒软件及个人防火墙。所有计算机必须及时升级操作系统补丁和更新防病毒软件。

（三）任何人不得在北京弘医医学发展基金会的局域网上制造或传播任何计算机病毒，不得故意引入病毒。

（四）因工作需要使用 QQ 等通讯工具传输文件时，应当仔细辨别后再接收，对接收的文件应用安全软件查杀后确认无毒再打开。

（五）使用电子邮件时，附件都应用安全软件查杀后确认无毒再打开。收到不明电子邮件，不得浏览和运行，以免感染计算机病毒。

（六）不得随意下载和运行未确定安全性的软件、程序和文档。

（七）杜绝病毒传播的各种途径。光盘、U 盘和移动硬盘等存储介质在使用前必须进行病毒检测。

（八）工作人员在使用计算机过程中一旦发现病毒，应立即关机并及时通知办公室进行处理。

第三章 网络安全管理员管理细则

第十条 计算机基础设备安全管理

（一）所有计算机在连入北京弘医医学发展基金会局域网前，网络安全管理员需对计算机硬件设备的基本配置信息、用途、使用人、使用的端口和服务、MAC 地址等登记备案，填写《计算机基本信息登记表》并进行安全审核后方可入网。

（二）经办公室负责人同意，网络安全管理员方可将工作人员私人计算机连接到北京弘医医学发展基金会网络，并进行登记备案，填写《私人计算机接入网络登记表》

（三）计算机出现故障需要送到外部维修或进行报废处理时，网络安全管理员必须将计算机的硬盘拆除并交予计算机使用人保管，不得随主机带出机构。

（四）网络安全管理员应定期对北京弘医医学发展基金会局域网网络运行设备进行巡视，并建立相应日志，包括信息系统服务器、财务服务器、备份服务器及其它应用服务器的 CPU 和内存、防火墙、网站、交换机的工作状况及客户端的网络运行速度等。

第十一条 计算机网络环境安全管理

（一）北京弘医医学发展基金会内网 IP 地址由网络安全管理员统一规划分配，未经办公室负责人同意，网络安全管理员不得擅自将内网 IP 地址分配给他人使用。

（二）网络安全管理员根据登记信息对计算机及相关设备进行网络配置，包括 IP 地址设置、MAC 地址与 IP 地址的绑定等。

（三）网络安全管理员要根据局域网运行情况，随时调整上网行为管理软、硬件参数，调度资源，保持网络安全、稳定、畅通。发生网络重大突发事件时，网络安全管理员应立即报告，采取应急措施，尽快恢复网络的正常运行，同时对事件情况进行记录。

（四）网络安全管理员负责北京弘医医学发展基金会在外托管机房机柜的日常管理。

（五）网络安全管理员与财务部人员分别持有安放财务管理软件服务器的机柜钥匙，财务部要指定专人保管此钥匙，不得让与他人使用。财务管理部人员每次打开机柜前，须提前告知办公室并由网络安全管理员进行登记。

第十二条 计算机系统及软件安全管理

（一）北京弘医医学发展基金会各类授权计算机操作系统、软件，统一由办公室专人或网络安全管理员保管。网络安全管理员必须收到工作人员提交的《软件安装申请单》后，方可将工作人员所申请的操作系统或软件安装到其计算机上。

（二）网络安全管理员不得将北京弘医医学发展基金会授权软件私自拷贝、盗卖、借于他人或私自将软件带回家中。

（三）北京弘医医学发展基金会综合管理信息平台、网站的网络数据必须由网络安全管理员在指定的备份服务器上进行异地备份。

第十三条 帐号与信息安全管理

（一）网络安全管理员应严格保密北京弘医医学发展基金会服务器、路由器等网络资源的各种帐号，超级用户权限只有网络安全管理员及经北京弘医医学发展基金会授权的人员方可拥有。不得将工作中使用的各类软件、系统、平台等帐号登录信息告知他人或发布、传播到互联网，如造成相关软件、系统、平台中数据信息的泄露，将追究个人责任，并保留通过法律追究的权利。

（二）网络安全管理员应对保管和使用的服务器、路由器等帐号登录密码至少三个月更改一次，密码要满足复杂性原则，长度不得低于 8 位。

（三）北京弘医医学发展基金会各类软件、系统、平台中所产生的一切文件、资料、图表和数据以及各类编码、目录等均属于北京弘医医学发展基金会信息资源范畴，网络安全管理员

必须遵照《保密协议》的约定，不得擅自泄露以上信息资料和数据，不得发布或传播到互联网。如造成相关信息的泄露，将追究个人责任，并保留通过法律追究的权利。

第十四条 防火墙与安全网关管理

（一）办公室指定网络安全管理员负责北京弘医医学发展基金会办公区及在外托管服务器的防火墙和安全网关的管理工作。

（二）网络安全管理员对防火墙和安全网关所做的一切配置和修改工作都必须由办公室负责人批准后实施。

（三）北京弘医医学发展基金会和外部网络连接的所有设备均须安装防火墙或通过安全网关以确保网络及连接的安全，通过防火墙或安全网关的设置对内外网络访问按照权限进行控制。

（四）网络安全管理员应定期检查各服务器的系统日志，如发现有入侵情况，应及时采取措施，保留原始数据，以便进行调查取证，并第一时间上报办公室，做好入侵情况登记。

（五）网络安全管理员应每月进行一次防火墙访问控制策略审查工作，对过期和权限过大的策略进行优化，并建立日志备查。

（六）网络安全管理员应及时了解各设备厂商发布的软硬件升级包，防火墙和安全网关的升级应严格按照厂商提供的配置说明及流程进行。防火墙厂商工程师必须在网络安全管理员的陪同下进行调试，调试完毕后网络安全管理员应立即更改管理口令。

第十五条 防病毒管理

（一）办公室负责对北京弘医医学发展基金会计算机病毒防治工作进行部署、监管和指导，网络安全管理员负责具体病毒防治工作。

（二）办公室负责在全网范围内建立多层次的防病毒体系，要使用国家规定的、具有《计算机信息系统安全专用产品销售许可证》的防病毒产品。应安装防病毒软件、防火墙以及安全卫士等恶意软件防治工具。

（三）所有计算机设备必须由网络安全管理员安装统一的防病毒软件，没有安装防病毒软件的计算机不得接入到北京弘医医学发展基金会网络中。未经办公室同意，网络安全管理员不得在计算机中安装非北京弘医医学发展基金会统一规定的任何防病毒软件及个人防火墙。

（四）网络安全管理员应及时向工作人员发布“新病毒预告”，同时将特定病毒专杀工具、相关安全补丁提供给北京弘医医学发展基金会工作人员使用，并提供相应技术指导和服务。

（五）网络安全管理员应定期检查所有计算机操作系统补丁的升级和防病毒软件更新的情况，对于操作系统、病毒软件异常情况的计算机应及时进行处理，未清除病毒的计算机不准连入网络。

第四章　附　则

第十六条　工作人员离职时，网络安全管理员须在第一时间取消该工作人员在北京弘医医学发展基金会所有的软、硬件、各应用平台和系统帐号权限及网络资源使用权限。

第十七条　网络安全管理员离职时，须立即将所保管的北京弘医医学发展基金会服务器、路由器、各类软件、平台等资源登录信息与办公室专人进行书面交接，双方须签字确认。

第十八条　任何人员如违反上述规定，造成北京弘医医学发展基金会信息泄露、财产损失或名誉受损等，北京弘医医学发展基金会将追究其个人责任，并保留通过法律追究的权利。

第十九条　本办法由北京弘医医学发展基金会秘书处负责解释。