中国科学院自动化研究所网络与信息安全管理制度

一．目的

为规范所内网络资源的使用和所内网络用户的上网行为，保证研究所网络与信息的安全，保障研究所科研和管理工作对网络和信息系统的正常需求。

二．适用范围

中国科学院自动化研究所所有网络用户。

三．网络与信息安全职责

1. 中科院自动化所科研支持部为全所网络与信息安全工作主管部门，网络安全主管领导由分管科研支持部的所领导担任。

2．中科院自动化所科研支持部承担职责：

- 研究所公用网络安全日常管理，包括人员管理、外包服务管理、研究所网站内容管理和电子信息管理；
- 研究所信息安全防护管理，包括机房安全、网络边界安全、网络设备和应用系统以及数据安全；
- 制定研究所网络安全事件应急预案并开展网络安全应急演练，在发生网络安全重大事件后及时通报网络安全主管部门；
- 面向所内人员开展网络安全教育培训，为所内用户提供网络与信息安全咨询和技术支持；
- 对研究所废弃的公用存储介质和设备进行信息销毁。

3．所内各实体部门需明确一名部门正职或副职领导分管本部门网络与信息安全工作。分管部门领导需承担以下职责：

- 与研究所签订网络与信息安全责任书；
- 制定本部门的网络安全保障政策并确定部门内部信息安全防范内容；
- 指定至少一名职工专职或兼职担任部门网络安全员；
- 保障兼职的网络安全员每周有不少于两个小时的工作时间用于处理部门（研究组）的网络与信息安全管理相关事务；
- 鼓励并支持部门网络安全员参加所内网络与信息安全相关培训；

4. 各部门（研究组）网络安全员职责如下：

- 及时了解本部门（研究组）的网络与信息安全状况，发现网络及系统安全异常情况及时反馈至科研支持部；
- 在发生网络故障时配合研究所进行快速准确定位；
- 协助研究所加强用户计算机系统安全防范工作；
- 协助研究所提醒网站负责人对部门(研究组)接入互联网的网站进行备案；
- 在发生网络与信息安全突发事件时配合取证；

5. 因工作原因需在研究所内开通对外信息服务网站或在部门（研究组）内部架设子网需向网络安全主管部门提交申请并签订网络与信息系统安全责任书。建有子网的部门（研究组）负责其子网内的运行和管理，并接受科研支持部的监督与管理。

6. 凡使用研究所网络上线运行的系统（含个人自行采购的电子和网络设备）的网络安全责任主体为该资产（设备）的领用人（所有人）。

7. 研究所官方网站发布的信息内容由综合处负责审核与管理。

四．网络接入规则

1．科研支持部负责所级网络的接入管理和资源分配，包括线路、路由器、交换机、IP 地址等网络资源。符合入网条件的用户可设置自动获取 IP。

2. 个人终端（台式机、笔记本、手机等）接入互联网，采用实名认证，通过认证账户登录上网，每个账户允许最多同时接入三台设备。对于使用期限不足三个月的短期个人用户，可根据需要采用公共账户接入，也可由所在部门或研究组申请认证账户。未经认证的用户将无法接入互联网。

3. 个人用户需向研究所提出申请，科研支持部为其建立、开通认证账户。在职职工（含返聘人员和博士后）由本人或人力资源处提出申请，部门负责人和人力资源处签字确认；在读研究生（含联合培养研究生）由本人或研究生部提出申请，导师和研究生部签字确认；访问人员（含长短期）由课题组或本人提出申请并注明使用期限，所内合作人和课题负责人签字确认。

4. 服务器接入互联网，需向科研支持部提交申请并报备，由科研支持部分配特殊网段 IP 地址。没有报备的服务器将无法接入互联网。

5. 对于需要传输大数据量的用户，可向科研支持部提出申请，经批准后，根据当时网络运行情况调整接入带宽，由此产生的额外费用由用户承担。

五．网络使用安全规则

1．所有网络用户必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》等国家有关法律、法规。 在发生网络与信息安全突发事件时立即启动《自动化所突发事件应急管理暂行规定》，并努力将损失减到最小。

2．所内的计算机网络及计算机软、硬件资源用于保障与科研和管理相关的

业务，通过网络系统进行的数据传输、邮件通讯或新闻发布不得违反国家对计算机和国际互联网有关的安全条例和规定，严格执行安全保密制度，对所提供的信息负责。

3. 所内计算机用户需对变更用途的存储介质上的重要信息进行消除。

4. 所内计算机的帐号只授予个人使用，被授权者对自己享用（或因特殊需要由集体享用的）资源负有保护责任，口令密码应为六个字符以上且至少包含两类字符。公用账号在上网时要有完善的登记制度。账号信息如有泄漏，应及时变更，严格禁止将本人帐号让与他人使用。建议不在邮件服务器端保留已收取的包含重要信息的邮件。

5. 遵守有利于科技交流的国际惯例，在非授权情况下，不得私自拷贝不属于自己的软件资源，严禁将带病毒的文件故意输入计算机。要及时安装最新系统补丁，并定期对病毒库进行更新。

6. 遵守国家有关法律、行政法规，严格执行自动化所安全保密规章制度，不得利用网络从事危害国家安全、泄漏国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息；接入互联网的计算机严禁处理涉密信息,严禁通过任何无保密保障措施的通信设备传递国家秘密信息，涉密计算机系统须符合国家有关规定和标准。

7. 对在计算机上被动收到的不良信息，严禁扩散，应及时报告网络管理员，协助删除，并报有关部门处理。

8. 严禁私自在网络和计算机上进行大量消耗资源且没有科学意义的黑客行为、测试操作、广告型或链式通讯操作、游戏型或赌博型操作。

9. 任何人不得利用研究所网络发布含有下列内容之一的信息：

(1)反对宪法所确定的基本原则的；

(2)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(3)损害国家荣誉和利益的；

(4)煽动民族仇恨、民族歧视，破坏民族团结的；

(5)破坏国家宗教政策，宣扬邪教和封建迷信的；

(6)散布谣言，扰乱社会秩序，破坏社会稳定的；

(7)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(8)侮辱或者诽谤他人，侵害他人合法权益的；

(9)含有法律、行政法规禁止的其他内容的。

10. 如发现违反上述任何规定者，将视情节严重程度及造成的影响和损失，给予停止使用网络3～6个月的处罚，直至提交有关部门追究法律责任。

11. 如发现他人有违反上述任何规定的行为，应立即报告科研支持部。

六．本管理制度由科研支持部负责解释。