恶意代码防范管理制度

编制人：	朱伯荣	2018	年 9 月 12 日
审核人：	孙聪	2018	年 9 月 17 日
批准人：	肖宇	2018	年 9 月 20 日
分发人：	孙聪	2018	年 9 月 25 日

厦门安达出行科技有限公司

V1.0

发布日期： 2018/x/x 实施日期： 2018/x/x

版本变更记录

版本号	修订人	审核人	批准人	生效日期	备注
V1.0					新建

1 目的

为了加强公司信息安全保障能力， 规范公司恶意代码防范的安全管理，加强对公司设备恶意代码的防护，特制订本制度。

2 适用范围

本制度适用于公司防病毒和防恶意代码管理工作。

3 职责

由信息中心负责公司恶意代码防范的日常管理工作。

各计算机系统使用人负责本机防病毒工作。

4 恶意代码防范日常管理

4.1 恶意代码防范检查

4.1.1 信息中心负责定期对公司防恶意代码工作进行监督检查。

4.1.2 公司接入网络的计算机， 必须统一安装联网杀毒软件。 杀毒软件安装完毕应进行正确的配置， 开启实时防护功能， 开启自动升级软件和病毒库的功能。

4.1.3 不能联网的计算机应由安全管理员负责安装杀毒软件， 并定期对病毒库进行升级。

4.2 恶意代码防范系统使用

4.2.1 信息中心定期对公司的恶意代码防范工作进行检查， 由安全管理员定期进行恶意代码查杀，并填写《恶意代码检测记录表》。

4.2.2 安全管理员定期检查信息系统内各种产品恶意代码库的升级

情况并填写《恶意代码防范软件升级记录表》，对恶意代码防范产品截获的恶意代码及时进行分析处理，并形成书面的分析报告。

4.2.3 信息中心定期对恶意代码防范产品进行测试，保证恶意代码防范产品的有效性。

4.2.4 终端用户要学会杀毒软件的安装和使用，不能自行停用或卸载杀毒软件，不能随意修改杀毒软件的配置信息，并及时安装系统升级补丁。

4.2.5 公司员工从网上下载文件和接收文件时，应确保杀毒软件的实时防护功能已开启。

4.2.6 公司员工在使用计算机读取移动存储设备时，应先进行恶意代码检查。

4.2.7 因业务需要使用外来计算机或存储设备时，需先进行恶意代码检查。移动存储设备需接入杀毒专用计算机进行恶意代码检测，确定设备无毒后才能接入公司网络。

4.2.8 公司员工应提高恶意代码防范意识，应从正规渠道下载和安装软件，不下载和运行来历不明的程序。收到来历不明的邮件时，不要随意打开邮件中的链接或附件。

4.2.9 部门新增计算机在安装恶意代码防范软件时，需经过信息中心的授权后才能安装和使用。

4.2.10 各部门安装的外购软件和自行开发的软件都必须由信息中心测试其安全性，经确认后方可安装。

4.3 恶意代码防范培训

4.3.1 信息中心定期组织各部门进行恶意代码防范工作培训，提高公司员工的恶意代码防范意识和安全技能。

4.4 恶意代码应急处置

4.4.1 当部门计算机发现有恶意代码入侵时， 员工需立即断网， 并第一时间通知信息中心，由信息中心进行处理。

4.4.2 当部门发生因计算机病毒引起的信息系统瘫痪、 程序和数据受到严重破坏等重大事故时， 员工需保护好现场， 并第一时间通知信息中心，由信息中心进行处理，必要时可请求第三方援助。

4.4.3 如某种新型病毒大规模爆发时（例如勒索病毒），安全管理员应立即升级病毒库， 并编制相应的病毒处置指南， 各部门按照指南进行操作。

5 相关文档

《恶意代码检测记录表》

《恶意代码防范软件升级记录表》

6 附则

此管理规定由信息中心负责解释并督促执行；

本规定自印发之日起执行。

恶意代码检测记录表

序号	检测对象	检测日期	检测方法	检测结果	处理结果	检测人	备注
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

恶意代码防范软件升级记录表

序号	升级对象（软件 / 病毒库）	升级前版本	升级后版本	升级日期	操作人	备注
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						