网络安全管理

版 本 历 史

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **说明** | **作者** |
| 2017-5-27 | 0.1 | 新建 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[**1.** **目的** 3](#_Toc490493057)

[**2.** **范围** 3](#_Toc490493058)

[**3.** **总则** 3](#_Toc490493059)

[**4.** **网络安全管理规定** 3](#_Toc490493060)

1. **目的**

为进一步规范公司网络的管理，确保公司网络资源高效、安全运行，加强对网络资源安全性保护，特制定本办法。

1. **范围**

本管理办法适用于公司范围内网络系统的安全和信息安全的管理。

1. **总则**
2. 本管理办法所称的网络安全：是指公司所使用的网络，包括在此网络上提供各种应用和服务的所有硬件和软件等信息资产的安全。
3. 本管理办法所称的信息安全：是指包括由服务器、客户机及其附属设备上的，根据开发设计、技术文档、财务报表、培训资料、人事管理等要求建立的信息系统、报表文档、数据库、图片以及其它包含公司商业机密的相关文档、文件和资料的保密和安全。
4. 公司网络与信息的安全管理，应当保障计算机网络设备和配套设施的安全、信息的安全、运行环境的安全。保障公司网络系统的正常运行，保障信息系统的安全运行。
5. 由网管负责全公司的网络安全和信息安全工作,不定期对网络内所有人员进行网络安全和信息安全方面的教育，并对网络中的信息进行有效的监督和审查。
6. 公司网络内的所有部门和人员必须接受并配合技术部依法进行的监督检查，必须接受技术部进行的网络系统及信息系统的安全检查。
7. 公司网络内的所有部门和人员有义务向技术部报告违反本管理办法的部门和个人或对公司网络正常安全运行有害的行为。
8. **网络安全管理规定**
9. 公司网络由网管统一规划、建设并负责运行、监督、管理和维护，包括设置路由器、交换机、防火墙、台式电脑、笔记本电脑及与网络安全相关的软硬件。
10. 公司网络的IP地址、子网规划以及涉及网络安全的各种系统登录帐户和默认密码的软硬件设备等均由网管集中部署管理，登记后分配至个人，并不定期进行监督和检查。任何人必须严格使用由技术部分配的“IP地址”、“机器名”、“系统登录帐户”以及个人电脑等软硬件配置，严禁私自更改或盗用他人的软硬件配置。
11. 严禁利用公司信息类资产包括电脑，打印机、传真机或QQ、微信等软硬件以及网络资源进行与工作无关或无益的私人活动。
12. 严禁以空密码登录公司内部各种涉及网络安全的信息系统或软硬件设备。个人在获得分配的各种系统登录默认密码后，应及时更改密码。各类密码的设置，均应遵循不易被破译的原则，密码的位数应在七位以上。不得把自己的密码告诉他人，也不得把密码写在纸上。密码应经常更换，尤其是重要涉密岗位，同一密码最长使用时间不应超过二个月。
13. 严禁以任何手段窃取或试图窃取未授权使用的各种涉及网络安全的软硬件设备的系统登录密码，也不得以他人帐号、IP地址等任何形式登录或试图登录未授权使用的包括电脑在内的各种涉及网络安全的软硬件设备。严禁以任何手段、任何形式查询、访问、修改和删除或试图查询、访问、修改和删除未授权的网络资源。
14. 严禁在公司网络内制作、散播计算机病毒或木马程序。所有接入公司网络的电脑均须保证安装有防病毒软件，任何人在发现陌生或可疑邮件、计算机非正常运行或是电脑未安装防病毒软件等情况时应及时向技术部相关人员报告。
15. 严禁以任何方式、任何理由对影响公司网络系统正常运行的服务和软硬件设备实施攻击、干扰和破坏。