|  |  |  |
| --- | --- | --- |
| 文件编号 | **网络安全应急响应管理制度** | 受控状态 |
|  |  |
| 拟 制 人 |  | 版本/修订 | A/A0 |
| 审 核 人 |  | 制作份数 | 1 |
| 批 准 人 |  | 生效日期 | 2018年10月26日 |
| 发放部门 |  |

1. **目的**

为保障公司整体信息系统安全，减少因信息安全事件造成的损失采取纠正预防措施编制本制度。

1. **范围**

适用于公司信息安全管理。

1. **职责**
2. 各部门人员发现疑似信息安全疑似事件均有责任进行上报。
3. IT部负责组建信息安全执行小组，对所有发现有关信息安全异常事件进行分析和处理。
4. **程序**
	1. 信息安全事件分类：系统攻击事件、信息破坏事件、信息容安全事件、设备故障事件、灾害事件、其他事件。
5. 系统攻击事件：通过网络攻击、有害程序或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷造成信息系统异常。
6. 信息破坏事件：通过技术手段造成该信息系统中的信息被篡改、假冒、泄露、窃取等手段导致的信息安全事件。
7. 信息容安全事件：利用网络发布、传播危害安全、破坏社会稳定、损害公共利益的安全事件。
8. 设施设备故障：由于人为操作导致系统自身故障或外部设施故障导致的信息安全事件。
9. 由于不可抗力造成物理性破坏导致的信息安全事件。
10. 不属于上述原因造成的信息安全事件。
	1. 安全事件的分级：根据损失程度和影响将信息安全事件划分为4个等级；
11. 特别重大信息安全事件：能够导致特别严重的影响或破坏信息事件，造成极严重的损失和极坏的社会影响。
12. 重大信息安全事件：导致严重影响或破坏的信息安全事件，造成严重的系统损失。
13. 较大信息安全事件：导致较严重的系统信息安全事件，会使重要信通信息遭受损失，一般信息系统遭受特别大的损失。
14. 一般信息安全事件：会使特别重要的信息系统遭受较小的损失或一般信息系统受到较大损失。
	1. 应急处置
15. 任何岗位人员发现疑似信息安全事件第一时间上报主管领导，由主管领导与IT部联系对一是时间进行确认。
16. IT部信息安全执行小组对上报疑似安全事件进行分析。
17. 分析判定为非信息安全事件的，需及时回复上报人。
18. 分析判定为信息安全事件的需进一步分析事件影响，确定安全等级并根据安全等级影响采取相应的处理措施。
19. 信息安全危害响应时间及处理周期
20. 特别重大信息安全事件：响应时间15分钟，故障处理周期1小时。
21. 重大信息安全事件：响应时间30分钟，故障处理周期3小时。
22. 重大信息安全事件：响应时间1小时，故障处理周期1工作日。
23. 一般信息安全事件：响应时间2小时，故障处理周期2工作日。
24. 安全事件应急处理结束后，应对本次安全事件发生的原因、事件规模进行调查，估算造成的损失后果并对应急处理措施进行风险评估。总结应急处理的经验形成完整的《安全事件应急处理报告》由IT部归档保存。
25. **相关文件**

无

1. **相关记录**

《安全事件应急处理报告》