**XXX单位**

**安全事件管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479447040)

[2 适用范围 1](#_Toc479447041)

[3 事件报告及处理 1](#_Toc479447042)

[3.1 安全事件报告时限 1](#_Toc479447043)

[3.2 事件处理流程 2](#_Toc479447044)

[3.3 信息安全事件处罚 2](#_Toc479447045)

[3.4 信息安全事件改进 2](#_Toc479447046)

[4 信息安全事件总结分析 2](#_Toc479447047)

[5 附则 3](#_Toc479447048)

# 目的

为了进一步规范单位系统对信息安全事件的处理过程，及时控制、解决各类信息安全事件。依据XXX单位信息安全目标、策略方针，以及相关规范和标准的规定，编制本管理制度。

# 适用范围

本制度适用于XXX单位的信息安全事件的管理活动。

信息安全事件指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。单位信息中心负责处理与信息安全事件相关的全部工作。

为了有效检测信息安全异常现象、对已确定的信息安全事件进行评估，将信息安全事件对组织及其业务运行的负面影响降至最小、及时总结信息安全事件及其管理的经验教训，组织应按照信息安全事件分类分级指南对信息安全事件进行定性，同时按照本管理制度的流程及时处理。

# 事件报告及处理

## 安全事件报告时限

员工或第三方人员发现信息安全相关异常及隐患必须在第一时间上报相关部门，由主要负责人初步判断是否为信息安全事件。

重大信息安全事件必须在2小时内、严重信息安全事件必须在12小时内向信息中心报告。

信息中心负责统一协调处理重大信息安全事件和严重信息安全事件。组织应密切关注组织外部信息安全事件及可能给组织带来的影响，必要时向上级报告。

## 事件处理流程

1）事件相关部门应立即安排人员进行调查取证、指定人员共同参与分析事件原因并采取补救措施。涉及第三方的事件，应在12小时内将补救措施正式报告给相关人员；

2）必须在12小时内向信息中心上报事件，获取处理意见和指导方针，并通知所有可能受到影响的部门和相关方，共同商讨、制定解决措施；

3）信息中心组织事件直接责任部门及相关部门进行事件原因的深层次剖析，制定相应检查措施及后续改善措施，并在36小时内提交相关方；

4）处理过程中，信息中心要及时向上级组织汇报进展，并获得指导。

## 信息安全事件处罚

根据事件的影响程度，将按照组织相关规定处罚事件责任人，要求其赔偿损失，处罚部门承担管理责任的相关负责人。情节严重者，将与执法机关联系，追究责任人刑事责任。

## 信息安全事件改进

1）信息中心应将与事件相关的所有书面记录纳入组织信息安全事件库；

2）信息安全管理部门对事件进行分析，识别信息安全管理流程和制度方面存在的不足，完善并细化信息安全管理制度，根据事件的影响程度，必要时在组织更大范围内进行审核、培训，避免类似事件再次发生；

3）信息中心负责跟踪相关部门检查活动和改善活动的执行情况；

4）根据事件的影响程度和造成的损失，必要时对外公开。

# 信息安全事件总结分析

在事件处理完毕以后一周内，信息中心应编制信息安全事件总结分析报告，并制定下一步的改善计划及相关预防措施。事件总结报告及相关记录应纳入组织信息安全事件库。

信息安全事件库应指定专人负责维护并定期分析，分析内容应该包括事件发生的趋势、范围及降低类似事件再次发生的预防措施等，并依据分析结果识别改善机会，避免同类事件重复发生。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。