文档密级：

C

信息安全事件管理规范

一、 总则

1. 目的

信息安全是业务应用的保障，确保信息系统的安全是每位员工的责任和义务。加强信息安全意识、安全防范、及时汇报可能或已经发生的信息安全问题，是信息安全问题能够得到快速响应、有效跟踪和及时解决的保障。

为了把安全事故和故障的损害降低到最低程度，追踪并从事故中吸取教训。明确有关事故、故障和薄弱点的管理部门，并能不断完善一个报告、反映、评价和惩戒的机制，以保证事故能提前预防、事故发生后能快速反应。

2. 范围

本文档适用于公司所有信息安全事件的处理。

3. 职责

（1） 信息安全领导委员会

信息安全领导委员会是组织信息安全事件管理的领导机构，负责组织信息安全事件的评审、响应和改进，其他部门配合

（2） 信息安全应急工作组，主要职责包括：

a) 信息安全领导委员会部署的各项任务。

b) 监督执行信息安全领导委员会下达的应急指令、重大应急决策和部署，协调各方面资源。

c) 及时了解和掌握信息安全突发事件预应急处置工作情况，向信息安全领导委员会报告时间处置过程中发现的重大问题，并协调解决。

d) 参与信息安全事件调查，总结应急处理经验和教训等后期处置工作。

（3） 所有员工

所有员工都有义务报告信息安全事件事态/事件。

二、 管理细则

1. 信息安全事件分类分级

信息安全突发事件级别分为四级：一般(IV 级)、较大(III 级)、重大(II 级)和特别重大(I 级)，对应颜色依次为蓝色、黄色、橙色和红色。

一般(IV 级)：指能够导致较小影响或破坏的信息安全事件。

较大(III 级)：指能够导致较严重影响或破坏的信息安全事件。

重大(II 级)：指能够导致严重影响或破坏的信息安全事件。

特别重大(I 级)：指能够导致特别严重影响或破坏的信息安全事件

（1） 特别重大信息安全事件

指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：

a)组织的财务数据、重大决策数据、敏感的人事数据（属于内部机密级的信息）发生泄漏、篡改或丢失。

b)组织签订的合同内容（属于内部机密级的信息）发生泄漏。

c)组织生产数据库中用户数据相关敏感信息发送泄漏、篡改或丢失。

d)网络终端、电路故障、通信终端等问题导致的生产正常业务大部分中断时间超过一小时。

e)组织服务器宕机而导致的正常生产 50%业务中断时间超过 1 小时。

f)造成人员伤亡的所有事件。

（2） 重大信息安全事件

重大信息安全事件是指能导致严重影响有或破坏的重大信息安全事件。包括以下情况：

a)网络终端、电路故障、通信终端等问题导致的关键业务中断时间超过 30 分钟。

b)组织服务器宕机而导致的正常生产 50%业务中断时间超过 30 分钟。

c)组织签订的合同内容（属于内部 A\B 类信息资产）发生泄漏。

d)商户数据发生泄漏、篡改或丢失。

e)数据发生泄漏、篡改或丢失。

f)造成人员伤亡的所有事件

（3） 较大的信息安全事件

较大信息安全事件是指能导致严重影响有或破坏的信息安全事件。包括以下情况：

a) 网络终端、电路故障、通信终端等问题导致的生产部分正常 30%业务中断超过 15 分钟。

b) 网络终端、电路故障、通信终端等问题导致的办公正常业务中断时间超过 60 分钟。

c) 组织服务器宕机而导致的正常生产 30%业务中断 5 分钟。

d) 内部公开级数据的信息资产发生外部泄漏、篡改或丢失。

（4） 一般信息安全事件

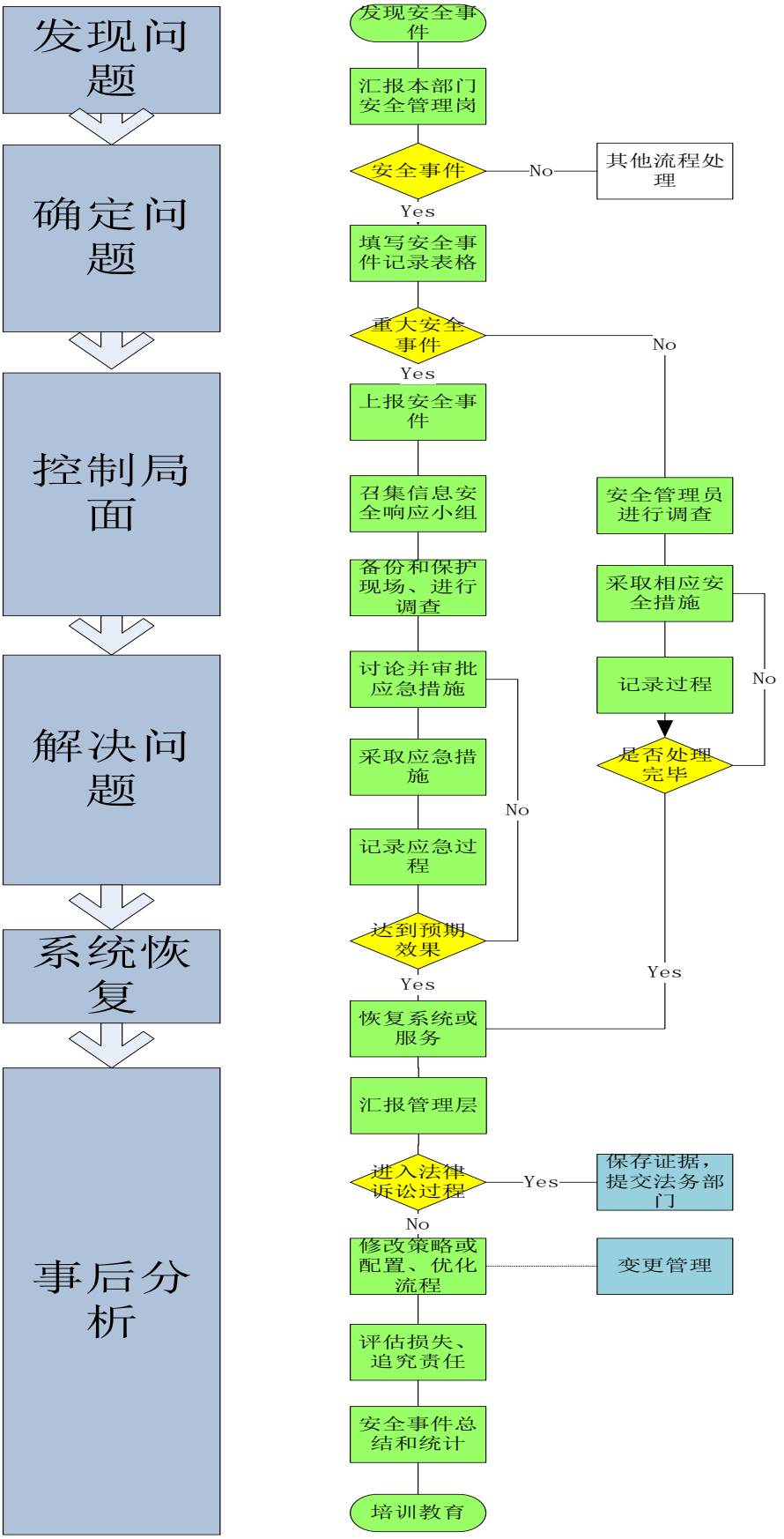
一般信息安全事件是指不满足以上条件的信息安全事件，包括以下情况：

a) 组织安全等级为一般的信息资产发生泄漏、篡改、或不可用。

b) 违法组织信息安全策略的操作，但未导致实际后果的事件

2. 信息安全事件的处理流程

安全事件的处理分为五个步骤：发现问题、确定问题、控制局面、解决问题、系统恢复和总结分析。操作流程如下图所示：


发现问题
确定问题
控制局面
解决问题
系统恢复
事后分析
发现安全事件
汇报本部门安全管理岗
安全事件
No
其他流程处理
Yes
填写安全事件记录表格
重大安全事件
No
Yes
上报安全事件
召集信息安全响应小组
备份和保护现场、进行调查
讨论并审批应急措施
采取应急措施
记录应急过程
达到预期效果
No
Yes
安全管理员进行调查
采取相应安全措施
记录过程
是否处理完毕
No
Yes
恢复系统或服务
汇报管理层
进入法律诉讼过程
Yes
保存证据，提交法务部门
No
修改策略或配置、优化流程
变更管理
评估损失、追究责任
安全事件总结和统计
培训教育

（1） 发现问题

a）所有员工都有责任和义务在遇到或怀疑发生信息安全问题时，应该第一时间报告到本部门信息安全管理岗，或者风险管理部。

b）员工在报告时，应描述问题发生的地点、事件、事件经过、已经造成的损失、相关人员的联系方式。作为报告的接收人，应记录下报告的内容，并及时告知报告人应采取的措施，包括如何保护现场，如何防止问题扩大，以及可能的解决办法等。对于严重的网络安全问题，问题接收人应遵循一边处理一边向上汇报的方法迅速向上汇报的方法，迅速向信息安全应急工作组报告。

c）对于一些事故、故障、脆弱点在相关人员或部门来处理之前，发现人尽量不要试图怀疑问题并改变现状，。

（2） 确定问题

a）部门安全管理岗在接受安全事件报告后，首先需要判断这是否是个安全事件，如果是，应该及时填写《安全事件报告表格》。如紧急情况下可以先向上报告，随后在附上《安全事件报告表格》也可。

b）在判断接受的报告时安全事件后，还需要确定这个安全事件的等级，如果是重大安全事件，应立即上报给信息安全应急组。如果是一般安全事件，由信息安全工程师进行处理。

（3） 控制局面

a） 在明确为安全事件后，必须马上通知相关责任人和部门。

b） 保护好现场，防止问题扩大，做好取证工作，如电子文档处理时最好用数据镜像或者拷贝，纸本文档最好为安全保存。对证据的要求要注意可用性，质量。

c） 紧急情况下，可以先做一些必要的处理，如拔掉病毒发作的服务器的网线。

d） 负责处理部门对于安全事件的响应和处理应遵循以下次序：

- 保护人员的生命和安全。
- 保护敏感的设备和资料。
- 保护重要的数据资源。
- 防止系统破坏。

- 将公司遭受到的损失降至最小。

（4） 解决问题

a） 在控制好安全事件局面后，马上要调查事件原因，找出应对措施。

b） 对不能立即找出事件原因的，应及时组织，会同相关部门的技术和业务人员进行跟踪解决，对于重大安全事件，通过成立信息安全应急工作组进行解决，信息安全应急工作组在问题解决前应采取响应应急措施防止事件进一步扩大。

c） 重大安全事件应急处理方案需经过信息安全领导委员会批准，紧急时可向信息安全领导委员会口头汇报同意后方可实施。

（5） 系统恢复

在采取一定的安全措施或紧急措施后，保证业务运行一段时间后没有异常后，及时恢复系统或服务。在系统恢复的时候要注意以下原则：

a）只有授权的人才可采取行动。

b）将采取的行动进行记录。

c）将采取的行动对管理层进行报告。

（6） 总结分析

a）事件处理完毕，系统恢复正常运行后，事件负责人要对整个事故进行分析研究，总结经验教训，并形成安全事件处理报告。报告中应详细记录事件的类型、严重程度、事件的起因、处理过程、造成的直接损失、责任人以及建议改进的安全方案等。并对现有的一些流程进行重新梳理，对不适宜的环节进行修改。

b）对事件责任人要根据事故的严重程度和产生的损失，产生的原因进行处罚。惩戒手段可包括行政警告、经济处罚、调离岗位、依据合同辞退，对于触犯刑律者可送司法机关处理。

c）部门信息安全管理岗要对事件的调查结果、处罚结果和处理方法及时整理事故档案（记录安全事件报告表格编号来对应），以日期为索引专门存放。

- 对于一般安全事件，在问题解决以后，需由负责解决的技术支持人员给出技术报告。报告应包含事件描述、原因分析、解决方案、防范措施、经验教训、并提交安全中心备案。

- 对于重大安全事件，在问题解决后的一周内，由信息安全

应急工作组负责对该次安全事件进行重点分析，提出改善建议，并制定总结报告，然后上报信息安全领导委员会，由信息安全领导委员会审核并反馈相关意见，最后归档备案。

d）由信息安全领导委员会向其他各级部门通报典型安全事件。安全管理岗将整理后的安全事件档案定期组织全公司员工学习和培训。

e）每年在进行信息安全审计的时候，必须整理所有安全事件的档案，进行总结和分析。总结和统计必须包括安全事件清单、安全事件造成的后果、改进措施执行情况、解决方案执行情况以及解决事件需要的成本分析等。

（7） 注意要点

a）安全事件可能在任何事件发生，因此响应的速度是很重要的。如果第一个被通知的人不能及时到达现场应该立即通知另一个相关的人员，因此时间相应人员应该确定自己能否及时赶到。以免延误对安全事件的处理。

b）发生安全事件以后，应该谨慎对待媒体。如果将消息透露给不适当的人可能会导致一些意想不到的后果，下面的章节中会详细谈到信息发布的策略。

c）在安全事件发生和调查的过程中应该注意消息的保密，将消息透露给不适当的人，特别是媒体的记者可能会导致不良的后果。因此所有消息的公布都应该得到公司最高管理层的同意或最高管理层指派的负责人的同意。

d）媒体的采访要求应该向部门领导汇报，同意通过公司公关部门处理，诸如事件所牵涉的账户、程序和系统等特殊信息不能通过电话提供给任何无关人员，即使他也声称是受到影响的其他节点的安全负责人。一些可以的电话询问应当上报信息安全局或者部门领导。

e）如果不能确定某些消息是否可以发布，请向公关部门询问。

f）事件日志对于安全事件的处理和调查非常重要，安全事件可能在其刚刚发生时就暴露，也可能在发生的过程中或发现以后才被发现，因此所有安全事件都应该有一份书面的经过调查证明足够客观的日志，而且应该把日志妥善保存以免被修改。由于在线日志很容易被修改和删除，所以手工记录是必要的。另外这些记录安全事件汇报表和事故档案一同归档。应该记录的信息有：

- 与事件相关的所有电话的日期和事件。
- 相关事件发生（或者发现）的日期和事件。

- 处理相应事件所用的时间。
- 值班人员或事件协调小组通知的人员和与事件相关的人员。
- 受影响的系统名称（或 IP 地址），受影响的程序和网络。

三、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。
2. 本制度由公司信息安全局负责解释和修订。
3. 本制度自发布之日起开始执行。