信息安全管理程序

编　　号	****-ITSM-2007-2011
版 本 号	V2.0
受控状态	受控
密　　级	内部

2012-3-8 发布　　**2012-3-10** 实施

***公司　发布

文档变更记录

信息安全管理程序

1 范围

本流程文档是****在 IT 运维中信息安全管理流程的指南，目的在于规范服务管理人员在信息安全管理过程中的行为，保证其对公司服务管理体系策略、计划以及信息安全管理策略的遵从，保证信息安全管理目标的实现。

2 角色与职责

信息安全管理负责人

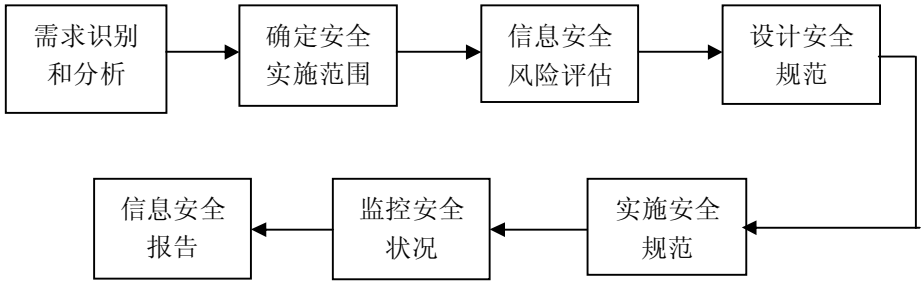
- 负责整个安全管理流程的有效运作
- 定义并维护信息安全管理相关的文件及所需要的记录模板；
- 管理信息安全管理的实施；
- 确保信息安全管理目标的实现；
- 识别信息安全管理过程中存在的问题并提出改进措施；
- 定期向 IT 服务管理小组汇报实施过程中存在的问题；
- 定期组织进行漏洞扫描，并根据漏洞扫描的结果提出、并落实改进措施；

3 方针

在所有活动中有效管理信息安全。经授权的管理者制定信息安全策略；实施信息安全策略的要求，管理与服务或系统访问有关的风险；组织应基于正式的协议访问信息系统和服务；按事件管理程序记录并处理安全事故；建立机制，量化并监视安全事故和失效的类型、程度和影响，记录改进措施，并作为服务改进计划的输入。

4 流程

4.1 信息安全管理流程



4.2 流程说明

4.2.1 需求识别和分析

根据服务级别协议中签订的关于安全的详细说明，确定安全需求并进行分析。服务级别协议中应该定义安全需求，在可能的情况下还应该以可测量的术语进行定义。该协议的安全部分应当确保客户所有的安全需求和标准能够实现，并且实现的结果能够进行明确的验证。需求识别包括人员安全的风险需求、

数据安全的需求，机房、设备等安全风险的需求。

4.2.2 确定安全实施范围

根据安全需求确定安全实施范围。安全实施范围包括列为相应安全等级的数据、人员、机房设备等。

4.2.3 信息安全风险评估

根据《信息安全风险管理程序》对公司与所提供 IT 服务有关的关键资产进行风险评估，并提交风险评估报告。

4.2.3 设计安全规范

根据风险评估结果制定相关安全管理制度，如《现金整点风险管理制度》、《现金中心值班管理制度》、《计算机机房管理制度》。

4.2.4 安全规范的培训

根据安全规范《现金整点风险管理制度》、《现金中心值班管理制度》、《计算机机房管理制度》等对技术人员进行培训。

4.2.5 实施安全规范

在设计好安全规范后，日常须按照安全规范来实施安全管理。

对发生的信息安全事件按照《事件管理程序》执行。

4.2.6 监控安全状况

对安全规范实施进行监控。

对发生的信息安全事件按照《事件管理程序》执行。

4.2.7 信息安全报告

- 对信息安全管理的实施状况及日常发生的安全事件等需编写安全报告。输出为服务报告流程。
- 报告可以提供有关已实现安全绩效方面的信息，并可以让客户了解有关的安全问题。这些报告通常是在与客户签订的协议中所要求的。
- 不论对于客户还是服务提供商来说，报告都是很重要的。客户必须正确地了解有关努力（如安全措施的实施）所取得的效率以及实际被采用的安全措施。
- 客户还需要了解所有的安全事件。为报告服务级别协议中定义的安全事件，可通过服务级别流程经理、事件流程经理或信息安全流程经理与客户代表建立直接的沟通渠道。
- 根据信息安全管理需要报告信息安全的实施情况，并提交给《服务报告》中。

5 流程持续改进

流程的改进计划由流程经理初步整理后，报告汇总到实施组长。

6 相关文件

《事件管理程序》

《服务报告管理程序》

《信息安全风险管理程序》《现金整点风险管理制度》《计算机机房管理制度》

7 相关记录

《IT 服务风险评估报告》