高新兴科技集团股份有限公司

受　　控

信息安全管理过程

文件编号：GSB／T 306.01

文件版本：A2

批　　准：刘伟辉

实施日期：2015-10-30

受控状态：受控

版本记录

版本	日期	修订页次	制/修订记录	制/修订者
A0	2013-12-18	/	新版制定	罗建明
A1	2014-10-21	3	“6.1 过程策略”有部分内容重新修订	罗建明
A2	2015-10-30	4	“6.2 过程描述”部分内容有修订	李旻

目　　录

信息安全管理过程

1 目的

本程序的目的是在运维服务工作中有效管理信息安全。

1) 满足运维服务中的客户安全性需求以及合同、法律和外部政策等外部要求；
2) 提供一个满足需求的基本的信息系统安全基线；
3) 确保有效的信息安全措施在管理层、运营部及相关部门、服务人员三个层面都得到贯彻。

2 范围

本程序适用于运维服务覆盖的所有部门。

3 术语和定义

安全管理是顺应信息安全的需要而产生的，其主要目标是确保信息的安全性。

安全管理致力于确保服务的安全性在任何时候都能达到与客户约定的级别。

安全性在服务中被视为可用性管理的一部分。安全管理已经成为现代服务管理中一个重要的问题。

安全性是指不易遭到已知风险的侵袭，并且尽可能地规避未知风险的性能。提供这种性能的工具是安全措施。

安全措施的目标是要保护信息的价值，这种价值取决于机密性、完整性和可用性三个方面。

术语	定义
机密性	指保护信息免受未经授权的访问和使用。
完整性	指信息的准确性、完全性和及时性。
可用性	是信息在任何约定的时间内都可以被访问，这取决于由信息处理系统所提供的持续性。

4 管理职责

4.1 过程负责人

安全管理负责人。

4.2 主要输入

输入	来源
服务级别需求	服务级别协议
配置管理	系统的配置项，记录和报告配置

4.3 主要输出

输出	去向
风险评估报告	信息安全管理负责人、部门经理
信息安全规范	信息安全管理负责人、部门经理
变更管理	服务实施过程中，服务交付过程的主要步骤。
服务报告管理	服务实施过程中，服务交付过程的主要步骤。

4.4 职责权限

安全管理负责人负责整个安全管理流程的有效运作。

安全管理负责人（运营业务部总监）职责

1) 监控安全管理流程；
2) 根据组织安全需求，开发与维护安全计划；
3) 处理与安全相关的问题和事件；
4) 确保满足运维服务指定的安全需求；
5) 完成包含流程结果，自评估及内部审计的信息安全风险评估报告；
6) 人员组成：信息安全管理员、部门经理等。

运维服务负责人(运维项目经理)职责

1) 负责安排项目中的信息安全风险评估；
2) 做好用户的沟通，协调关于信息安全的问题。

4.5 过程重要控制点

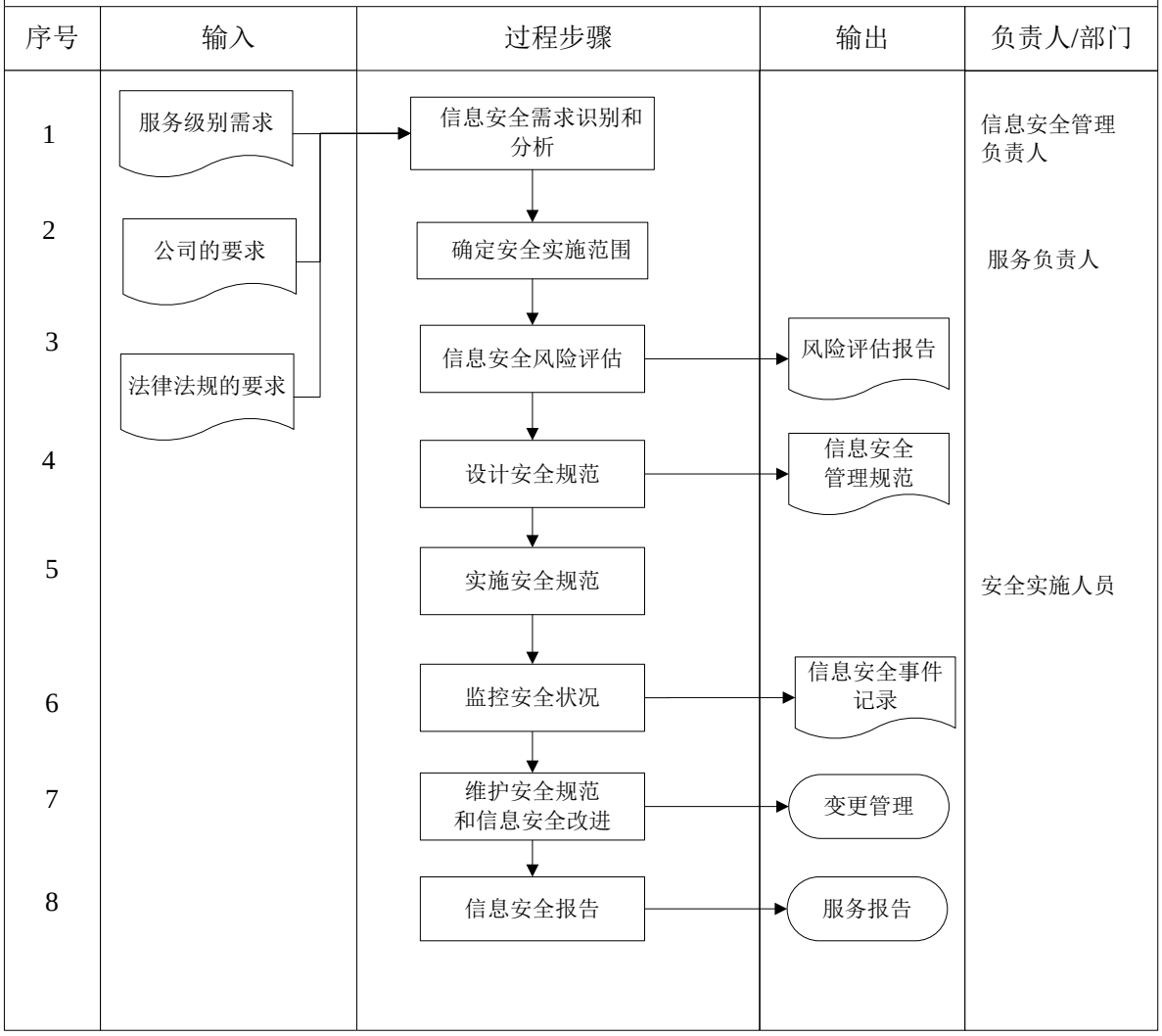
风险评估报告；
信息安全管理规范；
安全事件记录。

4.6 过程测量指标

安全事件次数。

5 工作流程

图1、信息安全管理流程



6 管理过程策略和描述

6.1 过程策略

6.1.1 安全方针

遵循公司“统一规划、分级管理、积极防范、人人有责”的原则，按照公司统一部署，结合服务/经营活动的特点，采取一切必要的措施，加强信息安全体系的建设和推进管理。

6.1.2 风险识别

运维项目经理应组织人员主动检查客户/公司在信息技术的安全方面所面临的风险。

针对安全要求高，客户明确运维对象的信息安全属于我方责任范围的项目。

针对客户明确运维对象的信息安全属于客户责任范围的项目，遵循以下原则进行列举检查表形式的风险评估：

1) 主动识别来自法律法规、行业规定、客户要求（包括服务级别协议）的安全需求，制定安全措施和安全规范满足安全需求；
2) 制定措施确保服务相关人员遵守客户现场的安全制度；

3) 应主动识别服务相关人员可能接触到的客户机密和敏感信息，制定措施确保服务相关人员不会故意或无意泄漏客户的有价值信息；
4) 应主动识别服务相关人员在服务过程中可能造成客户信息的不完整或不可用，制定服务规范和相应措施规避此风险；
5) 应做到“适当勤奋”，识别出服务相关人员接触到的客户信息系统所面临的物理、人员、管理、设置等方面的安全风险，告知客户并提供相应建议；
6) 进行适度的安全检查，以确保安全风险和安全事件的暴露和处理；
7) 进行全面的信息安全教育，做到信息安全，人人有责；
8) 主动地进行信息安全方面的评审和改进，确保安全体系的有效。

6.2 过程描述

信息安全活动划分为三个部分，包括规划、实施和监控。规划包括需求识别和分析、确定安全实施范围、信息安全风险评估、安全规范设计；实施包括安全规范实施；监控包括安全状况监控、维护安全规范、信息安全报告。

6.2.1 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度的术语进行定义。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。需求识别的范围包括人员安全、数据安全、机房环境、设备安全、系统安全等的安全需求。

6.2.2 确定安全实施范围

根据安全需求的识别情况确定安全实施范围。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、系统等。

6.2.3 信息安全风险评估

服务管理人员根据确定的安全实施范围进行风险分析与评估工作，并提交风险分析与评估报告。

风险评估包括识别安全实施范围内的资产状况、资产面临的威胁，现在使用的技术方法和管理规范，并进行总体分析得出风险的等级，编制《风险评估报告》。

6.2.4 设计安全规范

根据《风险评估报告》，服务负责人制定和编写《信息安全管理规范》。并根据信息安全规范制定信息安全策略、针对个人的保密协议、岗位职责说明、机房管理制度。

6.2.5 实施安全规范

在设计好安全规范后，日常需按照安全规范来实施安全管理。

1) 在人员安全方面的实施：
   a) 岗位说明书中的任务和职责；
   b) 安全防护教育；
   c) 员工个人电脑及涉密文档需做加密处理；
   d) 针对个人的保密协议。
2) 责任划分的实施，以及岗位分离的实施。
3) 书面的操作指示，内部规章。
4) 安全问题涉及整个生命周期，应针对系统开发、测试、验收、运营、维护和终止制定安全指南。
5) 将开发和测试环境与实际的运营环境分离开来。
6) 处理事件的程序（由事件管理负责处理）。
7) 恢复设施的实施。
8) 为变更管理提供信息输入，病毒防护措施的实施。
9) 针对计算机、操作系统、应用系统、数据、网络和网络服务的安全管理措施的实施。

10）数据媒介的处理和安全。

6.2.6 监控安全状况

对安全规范实施进行监控，在工作周报、服务月报中体现。

6.2.7 维护安全规范和信息安全改进

服务管理人员根据系统运行及客户服务的风险变化，必要时对《信息安全管理规范》进行修改。

由于基础架构、组织和业务流程方面的变化导致相关的风险也随着发生变化，因此安全也需要进行维护。

安全维护包括服务级别协议中安全部分的维护以及详细的安全规范的维护。

维护需要根据评估子系统流程的结果以及对风险变化的评估结果进行。这些建议既可以直接被计划子流程所采纳，也可以纳入总体的服务级别协议的维护中。

安全规范更新通过变更管理实施。

通过安全检查记录和相关信息，分析企业或客户是否存在信息安全风险或信息安全风险隐患，针对发现的问题，制定相应的改进计划和改进措施。

6.2.8 信息安全报告

信息管理负责人根据信息安全管理的实施状况及日常发生的安全事件等，每年一次巡检，编写《信息安全服务报告》。

报告可以提供有关已实现安全绩效方面的信息，并可以了解有关的安全问题。

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。

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，可通过服务级别管理负责人、事件管理负责人或安全管理负责人与部门经理直接的沟通渠道。

除了在特殊情形下的例外事项，报告都是通过服务级别管理负责人进行传达的。

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。

7 相关文件

《服务报告程序》

《事件管理程序》

《变更管理程序》

8 相关记录

《风险评估报告》

《信息安全服务报告》

《安全事件记录》

《信息安全管理制度》

《个人保密协议》