信息安全管理程序

青岛慧海联创信息技术有限公司

2022-1-4

文档信息

文档名称编号	信息安全管理程序（HHLC-ITSS-XXAQGL）			
编制单位	青岛慧海联创信息技术有限公司			
文档版本	版本日期	版本说明	作者	审核
V1.0	2025-1-4	发布版本	宫海亭	张仲全

目录

1. 概述

1.1. 目的

本文档编写的目的是为了规范 IT 服务团队对用户信息系统的安全性管理。所有的信息安全技术都是为了达到一定的安全目标，其核心包括：保密性、完整性、可用性、可控性和不可否认性五个安全目标。

- 保密性（Confidentiality）：是指阻止非授权的主体阅读信息。它是信息安全一诞生就具有的特性，也是信息安全主要的研究内容之一。对纸质文档信息，我们只需要保护好文件，不被非授权者接触即可。而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读，也要阻止授权者将其访问的信息传递给非授权者，以致信息被泄漏。
- 完整性（Integrity）：是指防止信息被未经授权的篡改。它是保护信息保持原始的状态，使信息保持其真实性。如果这些信息被蓄意地修改、插入、删除等，形成虚假信息将带来严重的后果。
- 可用性（Usability）：是指授权主体在需要信息时能及时得到服务的能力。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。
- 可控性（Controllability）：是指对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。
- 不可否认性（Non-repudiation）：是指在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。

1.2. 范围

本文档适用于运维服务部所有服务对象；用于进行关键资产的识别、风险识别和评估的管理。

2. 术语、缩略词和定义

术语	缩略词	定义
信息安全	IS (Information security)	信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。它是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。
信息安全管理	ISM (Information security management)	信息安全管理即通过维护信息保密性、完整性和可用性，来管理和保护组织所有信息资产的一项体制。它涵盖了信息安全政策制定、风险评估、控制目标与方式的选择、制定规范的操作规程、信息安全培训等内容。 信息安全管理涉及领域：安全方针策略、组织安全、资产分类与控制、人员安全、物理与环境安全、通信与运营安全、访问控制、系统开发与维护、业务连续性、法律符合性等。

2.1. 角色与职责

角色	职 责
项目经理	负责信息安全管理流程中所有活动的协调和监控； 负责进行资产识别及风险评估，并制定相应的防范措施。
安全检测人员	执行项目经理分派的任务。

3. 信息安全管理

3.1. 资产识别

项目合同签订后，根据项目级服务目录的内容，对 IT 服务活动中的资产进行识别，安全检测人员根据项目的《资产信息统计表》完成《资产识别表》，并提交项目经理审批。

3.2. 风险识别

- **识别风险**

安全检测人员负责填写《资产风险评估及控制表》，内容包括但不限于资产类别、名称、物理位置、责任人及数量等，然后提交项目经理审批。

对资产进行风险识别，首先要确定信息安全威胁源，才能确定风险存在点，威胁源的分类如下所示：

（1）信息泄露：信息被泄露或透露给某个非授权的实体。

（2）破坏信息的完整性：数据被非授权地进行增删、修改或破坏而受到损失。

（3）拒绝服务：对信息或其他资源的合法访问被无条件地阻止。

（4）非法使用(非授权访问)：某一资源被某个非授权的人，或以非授权的方式使。

（5）窃听：用各种可能的合法或非法的手段窃取系统中的信息资源。例如对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄露截取有用信息等。

（6）业务流分析：通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

（7）假冒：非法用户通过欺骗通信系统冒充合法用户；或者特权小的用户冒充成为特权大的用户。黑客大多是采用假冒攻击。

（8）旁路控制：攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本保密，但却暴露出来的一些系统“特性”，利用这些“特性”，攻击者可以绕过防线守卫者侵入系统的内部，进行非法活动。

（9）授权侵犯：被授权使用某种权限，却将此权限用于其他非授权的目的，也称作“内部攻击”。

（10）抵赖：这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。

（11）重放：出于非法目的，将所截获的某次合法的通信数据进行拷贝，重新发送。

（12）计算机病毒：一种在计算机系统运行过程中能够实现传染和侵害系统功能的程序。

（13）人员不慎：一个授权的人为了某种利益，或由于粗心，将信息泄露给一个非授权的人。

（14）媒体废弃：信息被从废弃的磁介质或纸介质中获取。

（15）物理侵入：侵入者绕过物理控制而获得对系统的访问。

（16）窃取：重要的安全物品（如令牌或身份卡）被盗。

应在变更审批时充分考虑信息安全因素，识别可能发生的风险隐患，使信息安全风险的判断和评估作为变更审批与否的重要依据。对于违反信息安全要求的变更操作，应当及时终止以避免风险发生。

- **确认已经存在的风险防范措施**

针对已识别的资产风险进行确认，并对已经存在的风险控制方法进行确认或者制定新的风险防范措施。风险等级的判别可以参照资产赋值、威胁赋值、脆弱性赋值和《资产风险评估及控制表》的相关内容来综合评定。对应防范措施的制定参照《机房环境安全管理规范》、《系统安全管理规范》、《网络安全管理规范》和《应用系统安全管理规范》来进行。

针对变更对 IT 基础架构带来的影响，应当对原先的防护和控制措施进行重新的评估，以使当前的控制措施能够满足组织的信息安全要求。

3.3. 风险分析及判定

风险分析是系统地运用相关信息来确认风险的来源，并对风险进行估计。风险分析要考虑导致风险的原因和风险源、风险事件的正面和负面的后果及其发生的可能性、影响后果和可能性的因素、不同风险及其风险源的相互关系以及风险的其他特性，还要考虑现有的管理措施及其效果和效率。

在完成了风险识别以及已有安全措施确认后，将采用适当的方法与工具确定导致安全事件发生的可能性。综合安全事件所作用的资产价值，判断安全事件造成的损失对组织的影响，从而判断风险的等级。可以依据下表中准则判断风险的等级。

风险等级划分表

等级	描述
高	一旦发生组织信誉严重破坏、严重影响组织的正常经营，影响组织范围或一定范围，经济损失重大、社会影响恶劣
中	一旦发生会造成组织一定的经济、生产经营或社会影响，但影响面和影响程度不大
低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段或简单手段很快能解决

风险分析的结果为具有不同等级的风险列表并形成《风险评估表》。

3.4. 超过可接受风险的处置

超过可接受风险水平值时可按以下方法进行处理：

- 采用适当的控制措施(可参照《机房环境安全管理规范》、《系统安全管理规范》、《网络安全管理规范》和《应用系统安全管理规范》中的各项安全措施来进行控制)；

- 若风险符合组织的政策与风险承受准则，可在掌握状况下客观地接受此等风险；
- 风险规避：将相关的风险转移至其它机构，如保险公司、第三方服务商；
- 对于不可接受风险的资产，采取控制措施并实施后，重新评估以确认其风险等级，确保所采取的控制措施是充分的，直到其风险值降至可接受风险值为止。

3.5. 定期评估、改进

每年至少一次全面审查风险评估内容与状态的适应性，以确定是否存在新的风险及是否需要增加新的控制措施，对发生以下情况需及时进行风险评估：

- 当发生重大信息安全事件时；
- 当信息网络系统发生重大变更时；
- 当新增加服务时。

在风险评估结束后，项目经理要针对新风险和已存在风险的防范措施进行优化改善，提交《信息系统安全评估报告》。

3.6. 信息安全事件

所有引起信息的机密性（预防数据欺骗及组织敏感信息泄漏），完整性（防止数据被篡改）和可用性缺失（核心业务的连续性）的事件都是信息安全事件（例如病毒引起的故障）。有关信息安全事件按事件管理流程来执行。

3.7. 信息安全事件分析

项目经理定期分析和汇总信息安全事件，生成《信息安全事件统计表》。

4. 信息安全方针

- 签署保密协议

运维服务人员在客户单位工作期间，签订保密协议或在其他文件中明确信息安全条款。

- 与第三方签署安全保密协议

为了保障客户信息安全，运维服务部要与第三方组织签订信息安全协议。

5. 相关文件及模板

- 《资产识别表》
- 《资产风险评估及控制表》
- 《信息安全事件统计表》
- 《信息系统安全评估报告》