**文件编号：ITSS-06-01-11**

**版本：V1.0**

万洲奇智（青岛）信息科技有限公司

信息安全管理制度

|  |  |
| --- | --- |
| 编制人:毛彦超 | 编制时间:2025.01.08 |
| 审核人:陈姝羽 | 编制时间:2025.01.08 |
| 批准人:郭万洲 | 审批时间:2025.01.08 |

**修订记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日期 | 版本 | 变更说明 | 编写人 | 审核人 | 批准人 |
| 2025.01.08 | V1.0 | 新建文档 | 毛彦超 | 陈姝羽 | 郭万洲 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目录

[万洲奇智（青岛）信息科技有限公司 1](#_Toc13957)

[信息安全管理制度 1](#_Toc5894)

[1. 目的 4](#_Toc3099)

[2. 原则 4](#_Toc19392)

[3. 适用范围 4](#_Toc18451)

[4. 岗位职责 4](#_Toc6536)

[4.1. 运维部 4](#_Toc10571)

[5. 信息安全管理流程 5](#_Toc10060)

[5.1. 过程描述 5](#_Toc14433)

[5.1.1. 需求识别和分析 5](#_Toc27401)

[5.1.2. 确定安全实施范围 6](#_Toc19401)

[5.1.3. 5.3 信息安全风险评估 6](#_Toc16)

[5.1.4. 设计安全规范 6](#_Toc23960)

[5.1.5. 实施安全规范 6](#_Toc7195)

[5.1.6. 监控安全状况 7](#_Toc18604)

[5.1.7. 维护安全规范 7](#_Toc602)

[5.1.8. 信息安全报告 7](#_Toc28699)

[5.2. 考核指标 8](#_Toc2982)

[6. 附则 8](#_Toc11021)

[7. 附件 8](#_Toc21874)

[8. 记录 8](#_Toc24682)

目的

本制度的目的是在客户服务工作中有效管理信息安全。

1. 满足信息系统集成、软件运维项目运行和客户服务中的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公司、运维部与研发部和服务台三个层面都得到贯彻。

原则

在保障可用性的前提下，保护信息的机密性与完整性，并基于风险实施全面、持续、闭环的管理。

适用范围

适用于运维服务过程中所有部门

岗位职责

运维部

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SLA中指定的安全需求；
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. 负责制定运维安全范围和规范、表格。
7. 负责安排项目中的信息安全风险评估；
8. 做好用户的沟通，协调关于信息安全的问题。
9. 负责该项目安全管理的严格实施和持续监控。
10. 出安全报告给用户。
11. 负责记录系统运行过程中的信息安全事件记录。
12. 负责现场处理系统运行过程中的信息安全事件。

信息安全管理流程

信息安全管理流程，如图5-1所示

图5-1 信息安全管理流程



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。

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。

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。

5.3 信息安全风险评估

运维服务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，在使用的技术方法和管理规范，进行总体分析得出风险的等级，编制《风险评估报告》。

设计安全规范

根据《风险评估报告》，运维服务人员制定和编写《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。

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：
2. 职位说明中的任务和职责；
3. 安全防护；
4. 针对个人的保密协议；
5. 责任划分的实施，以及岗位分离的实施；
6. 书面的操作指示，内部规章；
7. 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；
8. 将开发和测试环境与实际的运营环境分离开来；
9. 处理事件的制度；
10. 恢复设施的实施；
11. 为变更管理提供信息输入，病毒防护措施的实施；
12. 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；
13. 数据媒介的处理和安全。

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。

对发生的信息安全事件按照《事件管理制度》执行。

维护安全规范

运维服务人员根据系统运行及客户服务的风险变化，必要时对《信息安全管理制度》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,参照《变更管理制度》。

信息安全报告

运维服务人员根据信息安全管理的实施状况及日常发生的安全事件等，每季一次巡检，如发生信息安全事件则编写《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。

正确地了解有关措施（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。

除了在特殊情形下的例外事项，报告都是通过运维服务人员进行传达的。

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。参照《服务报告管理制度》

考核指标

|  |  |  |  |
| --- | --- | --- | --- |
| **指标度量性** | **计算方式** | **频次** | **指标要求** |
| 客户信息泄露次数 | 服务过程中不得发生客户信息泄露 | 每年 | 0次 |
| 信息安全事件客户投诉 | 服务过程中不得发生信息安全事件客户投诉 | 每年 | 0次 |

附则

1. 本制度最终解释权和修订权归运维部。
2. 本制度自颁布之日起施行。

附件

《服务报告管理制度》

《事件管理制度》

《变更管理制度》

记录

《风险评估报告》

《信息安全服务报告》

《信息安全管理制度》