# 北京新都远景网络技术有限公司

# 信息安全管理制度

文件编号：XDYJ-06-11

编制部门：运维管理部　　编制时间：2025.01.10

版　　本：V 1 . 0　　编制时间：2025.01.10

批 准 人：孙玥　　审批时间：2025.01.10

# 修订记录

| 日期 | 版本 | 变更说明 | 批准人 |
| --- | --- | --- | --- |
| 2025.01.10 | V1.0 | 新建 | 孙玥 |
| | | | |
| | | | |
| | | | |

目录

# 1. 总则

## 1.1. 目的

为规范北京新都远景网络技术有限公司运维服务过程中的信息安全管理，系统性地识别、评估并处置信息安全风险，确保客户及公司信息的机密性、完整性和可用性，构建稳定可靠的服务环境，特制定本制度。

## 1.2. 适用范围

本制度适用于公司运维管理部及其它所有参与运维服务的部门与人员，管理范围覆盖服务交付过程中涉及的所有信息资产及相关活动。

## 1.3. 、原则

1. 预防为主原则：采取主动措施识别和消除安全隐患，防患于未然。
2. 风险导向原则：所有安全决策和措施应基于风险评估的结果。
3. 全员参与原则：每位员工都有责任和义务维护信息安全。
4. 持续改进原则：定期评审信息安全状况，确保持续有效。

## 1.4. 岗位职责

### 1.4.1. 运维管理部经理

1. 负责信息安全管理的整体规划、实施与维护。
2. 领导并组织资产盘点与风险评估工作。
3. 审批重大安全控制措施与改进计划。

### 1.4.2. 运维工程师

1. 执行运维管理部经理分派的具体安全任务。
2. 负责日常安全监控、事件初步处理与记录。
3. 协助完成安全审计与报告编写。

# 2. 引用依据

本制度制定引用了以下国家标准与行业规范：

1. GB/T 28827.1-2022 《信息技术服务 运行维护 第1部分：通用要求》
2. GB/T 28827.2-2012 《信息技术服务 运行维护 第2部分：交付规范》
3. GB/T 28827.3-2012 《信息技术服务 运行维护 第3部分：应急响应规范》
4. T/CESA 1299—2023 《信息技术服务 运行维护服务能力成熟度模型》

# 3. 定义与术语

## 3.1. 信息资产

任何对组织具有价值的信息及相关载体，如硬件、软件、数据、文档等。

## 3.2. 信息安全事件

导致或可能导致信息的机密性、完整性、可用性遭受破坏的单起或多起事件。

## 3.3. 风险评估

识别信息资产的风险、评估风险影响并确定处置优先级的过程。

# 4. 管理内容与要求

## 4.1. 资产识别与分类

运维管理部经理应组织对运维服务相关的所有信息资产进行识别、登记与分类。资产分类应依据《资产分类表》进行，并填写《关键资产风险评估及控制表》，明确资产的责任人、位置、数量等关键属性。

## 4.2. 风险识别与评估

### 4.2.1. 风险识别

应参照《机房环境安全管理规范》等系列安全规范，识别各资产面临的安全

威胁与自身弱点。变更管理流程中必须充分考虑信息安全风险。

#### 4.2.2. 风险评估

采用风险值（Risk Value）进行量化评估。风险值由资产重要度（Asset Criticality）与风险发生概率（Risk Probability）相乘得出。

资产重要度判定表如图4-1所示

表4-1 资产重要度判定表

| 原值 | 关联的服务重要度 | 等级 |
|---|---|---|
| 低 | 低 | 1 |
| 较低 | 较低 | 2 |
| 中 | 中 | 3 |
| 较高 | 较高 | 4 |
| 高 | 高 | 5 |

风险发生概率判定表如图4-2所示

表4-2 风险发生概率判定表

| 发生可能性范围 | 等级 |
|---|---|
| 1%~20% | 1 |
| 21%~40% | 2 |
| 41%~60% | 3 |
| 61%~80% | 4 |
| 81%~100% | 5 |

风险等级：计算风险值（1-25），并依据公司设定的可接受风险水平（阈值）确定风险等级。

## 4.3. 风险处置策略

对于超过可接受水平的风险，应采取以下一种或多种方式进行处置：

实施控制措施：采用适当的技术或管理措施降低风险。

风险接受：在符合组织政策的前提下，明确接受该风险。

风险规避：通过取消相关活动来避免风险。

风险转移：通过保险或第三方服务转移风险。

处置后需重新评估，确保风险已降至可接受水平。

## 4.4. 安全事件管理

所有信息安全事件必须通过事件管理流程进行记录、处理和跟踪。信运维管理部经理应定期分析事件数据，编制《信息安全事件统计表》，并据此提出改进措施。

## 4.5. 关键控制点与测量指标

为确保信息安全管理流程的有效执行和持续改进，特设定以下关键控制点与量化测量指标。

### 4.5.1. 关键控制点

1. 所有关键信息资产必须被识别、登记并定期审核。
2. 所有变更必须经过信息安全风险评估。
3. 所有信息安全事件必须被记录、分析并用于持续改进。

### 4.5.2. 过程测量指标

信息安全管理考核标准如表4-2所示

表4-3过程测量指标表

| 序号 | 衡量指标 | 指标计算说明 | 考核频次 | 目标值 |
|---|---|---|---|---|
| 1 | 信息泄露次数 | 客户信息泄露的事件次数 | 年度 | ≤2次 |

# 5. 附则

1. 本制度最终解释权和修订权归运维管理部。
2. 本制度自颁布之日起施行。

# 6. 附件

1. 《资产分类表》

2. 《关键资产风险评估及控制表》
3. 《信息安全事件统计表》

# 7. 记录

信息安全管理制度运行过程中产生的所有记录，包括但不限于风险评估表、事件统计表、审计报告等，应由运维管理部统一保存，保存期限不少于3年。