**北京沃丰时代数据科技有限公司**

**信息系统日志管理规范**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 信息系统日志管理规范 | | |
| **文档编号** | WF-DM0012 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 赵栋 | **编制日期** | 2019-12-19 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **状态** | **修订内容说明** | **修订日期** | **编制人** |
| V1.0 | 新建 | 新增 | 2019-12-19 | 赵栋 |
| V1.1 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

[1. 目的 3](#_Toc414736631)

[2. 适用范围 3](#_Toc414736632)

[3. 名词定义 3](#_Toc414736633)

[4. 日志管理规范 3](#_Toc414736634)

[4.1 总要求 3](#_Toc414736635)

[4.2 日志分类 3](#_Toc414736636)

[4.3 日常管理 5](#_Toc414736637)

[5. 角色与职责 6](#_Toc414736638)

[6. 日志管理策略 7](#_Toc414736639)

# 目的

制定本文件目的在于规范管理公司所属业务系统的主机设备以及网络设备所产生的系统日志、重要应用日志，确保各类日志的及时、完全归档，及时发现设备与系统的故障，提高信息系统的可靠性。

# 适用范围

本文件适用于公司的主机与网络设备日志管理。

# 名词定义

|  |  |
| --- | --- |
| **名词** | **定义** |
| 日志 | 是记录系统活动的重要信息。包括各信息系统主机、网络设备所产生的syslog以及重要应用程序所产生的日志。 |

# 日志管理规范

## 总要求

本文件所包含的所有日志信息任何人没有权利删除、添加或变更，故意删除、添加或者变更重要日志的责任人按相关法律法规和制定处理。

## 日志分类

日志的分类包括：操作系统日志、应用系统日志、数据库日志、网络设备日志和信息安全设备日志。每一类日志记录中都必须记录以下基本内容：事件发生的日期和时间、事件描述，操作者信息，成功和失败操作。

1. 操作系统日志还应记录以下信息：
   * 操作系统的启动/关闭信息；
   * 用户登录/退出信息；
   * 特殊权限使用；
   * 系统运行状态信息(包括报警、故障信息)；
   * 主机系统服务或配置变更信息。
2. 应用系统日志还应记录以下信息:
   * 应用系统的启动/关闭信息；
   * 关键模块的启动/关闭信息；
   * 用户的登录/退出信息；
   * 用户的关键操作信息；
   * 应用系统运行状态信息(包括报警、故障信息)；
   * 服务和配置参数的变更信息。
   * 隐私信息不允许输入到日志中(如密码信息)
3. 数据库日志还应记录以下信息：
   * 数据库系统的启动/关闭信息；
   * 用户的登录/退出信息；
   * 用户的关键操作信息（如添加或删除数据库）；
   * 数据库运行状态信息(包括报警、故障信息)。
4. 网络设备日志还应记录以下信息：
   * 设备的启动/关闭信息；
   * 用户登录/退出信息；
   * 端口变化信息；
   * 设备运行状态信息(包括报警、故障信息)。
5. 信息安全设备日志还应记录以下信息：
   * 设备的启动/关闭信息；
   * 用户登录/退出信息；
   * 端口变化信息；
   * 信息安全事件信息（如病毒爆发、攻击事件）；
   * 设备运行状态信息(包括报警、故障信息)。

## 日常管理

1. 记录日志的系统必须保持时钟信息与时钟同步服务器同步，信息系统维护人员每月检查时间同步是否正常。
2. 信息系统和IT设备的维护人员应按照日志管理策略保存操作日志。详见本文第六条。
3. 所有的操作活动都必须被记入日志,不得停用日志服务。
4. 信息系统和IT设备的维护人员应按日志管理策略中的检查频率对所管理的信息系统产生的相关日志进行检查，对日志中的错误或可疑项进行记录，如发现可疑的日志记录事件或无法分析判断，应及时进行分析处理，处理结果应补充记录到日志检查记录中。
5. 日志文件集中管理, 统一上报到Graylog日志系统, 并通过系统权限控制加以保护，同时设置日志文件访问控制权限，防止未授权的访问篡改。
6. 对于故障日志，参照事件管理流程进行处理，及时发现故障原因并分析解决，进行记录。
7. 安全审计员每季度对重要应用系统的日志配置策略和日志检查记录等进行复查，对各系统管理员和系统操作员的活动记录日志每季度进行审计。

# 角色与职责

| **角色** | **职责** | **人员** |
| --- | --- | --- |
| 系统管理员 | 负责生产网业务主机的信息系统日志维护和管理工作，并对可疑日志进行分析、处理。 | 研发部运维工程师 |
| 网络管理员 | 负责生产网网络设备的信息系统日志维护和管理工作，并对可疑日志进行分析、处理。 | 研发部运维工程师 |
| 安全审计员 | 负责对生产网各系统日志进行定期审计、查看和分析、处理可疑情况，复查重要日志文件。 | 研发部授权工程师 |

# 日志管理策略

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 日志名称 | 保存周期 | 检查频率 | 检查人员 |
| 1 | 操作系统日志 | 至少90天以上 | 每季度 | 系统管理员/安全审计员 |
| 2 | 数据库系统日志 | 至少90天以上 | 每季度 | 系统管理员/安全审计员 |
| 3 | 业务应用系统日志 | 至少90天以上 | 每季度 | 系统管理员/安全审计员 |
| 4 | 网络安全设备日志 | 至少90天以上 | 每季度 | 网络管理员/安全审计员 |
| 5 | 数据中心监控日志 | 至少90天以上 | 每季度 | 网络管理员/安全审计员 |