《捷荟公司组织安全管理制度》

一、总则

1. **目的**

    a. 为加强公司安全管理，保障公司人员、资产和信息的安全，维护公司正常的生产经营秩序，特制定本制度。

2. **适用范围**

    a. 本制度适用于公司全体员工及各部门。

二、安全管理组织架构

公司设立专门的安全管理组织架构，明确各部门及负责人的安全管理职责，确保安全管理工作的有效开展。具体组织架构如下：

（一）安全管理委员会

1. **组成**

    a. 主任：张波

    b. 委员：各部门负责人（包括席志成、周昕点等）

2. **职责**

a. 全面负责公司的安全管理工作，制定公司安全战略和方针；

b. 审议和批准公司安全管理制度和安全策略；

c. 定期召开安全管理会议，听取各部门安全工作汇报，研究解决重大安全问题；

d. 组织开展安全检查和安全评估，督促各部门落实整改措施；

e. 对重大安全事故进行调查处理，提出处理意见和整改措施。

（二）各部门安全管理职责

1. 产品业务部门（负责人：张波）

- **职责**
  - 负责产品业务的安全稳定运行，确保产品符合安全标准和规范；
  - 制定产品业务安全管理制度和操作流程，组织员工进行安全培训；
  - 定期对产品业务系统进行安全检查和漏洞扫描，及时发现和修复安全漏洞；
  - 负责处理产品业务相关的安全事件，及时向安全管理委员会报告重大安全事件；

- 协助其他部门开展安全管理工作，提供技术支持和协助。

2. 服务运维部门（负责人：周昕点）

- **职责**
  - 负责公司服务运维的安全管理工作，保障公司各项服务的稳定运行；
  - 制定服务运维安全管理制度和操作流程，组织员工进行安全培训；
  - 定期对服务运维系统进行安全检查和维护，及时发现和处理安全隐患；
  - 负责服务运维过程中的安全事件应急处理，确保服务的快速恢复；
  - 协助其他部门开展安全管理工作，提供运维支持和协助。

3. 其他部门（负责人：各部门负责人）

- **职责**
  - 负责本部门的安全管理工作，落实公司安全管理制度和要求；
  - 组织员工进行安全培训和教育，提高员工的安全意识和技能；
  - 定期对本部门的工作环境和设备进行安全检查，及时发现和整改安全隐患；

- 负责本部门的安全事件处理，及时向安全管理委员会报告重大安全事件；
- 协助其他部门开展安全管理工作，共同维护公司安全环境。

三、安全管理制度

（一）人员安全管理制度

1. **员工入职安全培训**
    a. 公司对新入职员工进行安全培训，内容包括公司安全管理制度、安全操作规程、安全意识等方面，确保员工了解公司的安全要求和自身的安全责任。
2. **员工安全考核**
    a. 定期对员工进行安全考核，考核结果与员工绩效挂钩，对安全考核不合格的员工进行补考或培训，直至合格为止。
3. **员工离职安全交接**
    a. 员工离职时，必须进行安全交接，包括工作设备、文件资料、系统账号等方面的交接，确保公司信息安全和资产安全。

（二）信息安全管理制度

1. 网络安全管理制度

- **网络架构安全**
  - 采用分层网络架构，合理划分网络区域（如内网、外网、DMZ 区），通过防火墙、路由器等设备进行访问控制，防止未经授权的访问。
- **网络设备安全**
  - 定期对网络设备（如交换机、路由器）进行维护和升级，确保设备运行稳定。设备配置应备份并加密存储，防止配置信息泄露。
- **网络访问控制**
  - 实施严格的网络访问控制策略，采用身份认证、授权管理等技术，限制用户对网络资源的访问权限。例如，员工只能访问与工作相关的网络资源，对外部访问进行严格限制。

2. 应用安全管理制度

- **应用系统开发安全**
  - 在应用系统开发过程中，采用安全开发模型（如 SDL），在需求分析、

设计、编码、测试等阶段进行安全审查，确保应用系统的安全性。

- **应用系统部署安全**
  - 应用系统部署时，进行安全配置检查，关闭不必要的服务和端口，确保系统运行在安全的环境中。对应用系统的漏洞进行及时修复，定期更新系统版本。
- **应用系统运行安全**
  - 监控应用系统的运行状态，及时发现并处理异常行为。对应用系统的日志进行定期审计，分析潜在的安全威胁。

3. 数据安全管理制度

- **数据分类与分级**
  - 对公司数据进行分类（如业务数据、用户数据、系统数据）和分级（如高敏感数据、中敏感数据、低敏感数据），根据数据的敏感程度采取不同的保护措施。
- **数据存储安全**
  - 对高敏感数据进行加密存储，采用安全的存储介质（如加密硬盘）。定期对数据进行备份，备份数据应存储在安全的环境中，并进行加密保

护。

- **数据访问控制**
  - 严格控制数据访问权限，采用身份认证、授权管理等技术，确保只有授权用户才能访问数据。对数据访问行为进行审计，记录访问日志。
- **数据传输安全**
  - 在数据传输过程中，采用加密协议（如 TLS/SSL）进行传输，防止数据在传输过程中被窃取或篡改。

（三）设备设施安全管理制度

1. **设备设施采购与验收**
   a. 在设备设施采购过程中，严格要求供应商提供安全认证和质量保证，对采购的设备设施进行严格的验收，确保设备设施符合安全标准和要求。
2. **设备设施使用与维护**
   a. 制定设备设施使用和维护管理制度，规范员工的操作行为，定期对设备设施进行维护和保养，确保设备设施的安全运行。
3. **设备设施报废与处置**

a. 对报废的设备设施进行安全处理，确保设备设施中的信息安全和环境安全，防止设备设施被非法利用或造成环境污染。

（四）安全检查与隐患整改制度

1. **定期安全检查**

a. 公司定期组织安全检查，包括综合安全检查、专项安全检查和日常安全检查，检查内容涵盖人员安全、信息安全、设备设施安全等方面，及时发现安全隐患。

2. **隐患整改**

a. 对安全检查中发现的安全隐患，相关部门必须及时制定整改措施，明确整改责任人和整改期限，确保隐患得到彻底整改。整改完成后，必须进行复查验收，确保整改效果。

（五）安全事故应急预案与处理制度

1. **安全事故应急预案**

a. 公司制定安全事故应急预案，明确安全事故的应急处理流程、应急组织架构、应急资源调配等内容，确保在发生安全事故时能够快速、有效地进行应急处理，减少事故损失。

2. **安全事故处理**

    a. 发生安全事故后，相关部门必须立即启动应急预案，组织人员进行应急处理，及时控制事故影响范围，防止事故扩大。同时，必须对事故进行调查分析，查明事故原因，追究相关责任人的责任，并制定整改措施，防止类似事故再次发生。

四、安全事故应急预案

（一）数据泄露应急预案

1. 应急响应流程

- **事件报告**
    - 一旦发现数据泄露事件，事件发现者应立即向部门负责人报告，部门负责人在[具体时间]内向安全管理委员会报告。
- **启动应急预案**
    - 安全管理委员会接到报告后，立即启动数据泄露应急预案，成立应急处理小组，明确各小组成员的职责。
- **事件调查**

- 应急处理小组对数据泄露事件进行调查，确定泄露的数据范围、泄露途径和影响范围。调查过程中，应收集相关证据，如系统日志、网络流量记录等。

- **控制措施**
  - 根据调查结果，采取相应的控制措施，如关闭相关系统、限制网络访问、通知受影响用户等，防止数据泄露事件进一步扩大。

- **数据恢复与修复**
  - 对泄露的数据进行评估，确定是否需要进行数据恢复和修复。如果需要，应尽快恢复数据的完整性和可用性。

- **事件总结**
  - 对数据泄露事件进行总结，分析事件原因，制定整改措施，完善公司安全管理制度和应急预案，防止类似事件再次发生。

2. 数据泄露应急处理记录

- **记录内容**
  - 事件发生时间、事件发现者、事件报告时间、事件描述、调查结果、采取的控制措施、数据恢复情况、事件总结等。

- **记录保存**
    - 数据泄露应急处理记录应保存在安全的环境中，便于后续审计和分析。

（二）数据破坏应急预案

1. **应急响应流程**

- **事件报告**
    - 一旦发现数据破坏事件，事件发现者应立即向部门负责人报告，部门负责人在[具体时间]内向安全管理委员会报告。报告内容包括事件发生时间、地点、初步判断的破坏类型（如删除、篡改、损坏等）和影响范围。
- **启动应急预案**
    - 安全管理委员会接到报告后，立即启动数据破坏应急预案，成立应急处理小组，明确各小组成员的职责。应急处理小组成员应包括技术专家、安全管理人员、相关业务部门代表等。
- **事件调查**

- 应急处理小组对数据破坏事件进行调查，确定破坏的数据范围、破坏方式和影响范围。调查过程中，应收集相关证据，如系统日志、备份数据、网络流量记录等，以便后续分析和恢复。

- **控制措施**
  - 根据调查结果，采取相应的控制措施，如隔离受影响的系统、暂停相关服务、限制网络访问等，防止数据破坏事件进一步扩大。同时，评估数据破坏对业务的影响，制定临时应对方案，确保关键业务的持续运行。

- **数据恢复与修复**
  - 对破坏的数据进行恢复和修复。如果数据有备份，应尽快从备份中恢复数据；如果没有备份，应尝试通过技术手段（如数据恢复工具）恢复数据。对于无法恢复的数据，应评估其重要性，制定数据重建计划。

- **事件总结**
  - 对数据破坏事件进行总结，分析事件原因，制定整改措施，完善公司安全管理制度和应急预案，防止类似事件再次发生。同时，对应急处理过程进行评估，总结经验教训，优化应急响应流程。

2. **数据破坏应急处理记录**

- **记录内容**
  - 事件发生时间、事件发现者、事件报告时间、事件描述、调查结果、采取的控制措施、数据恢复情况、事件总结等。
- **记录保存**
  - 数据破坏应急处理记录应保存在安全的环境中，便于后续审计和分析。记录应详细、准确，能够反映事件处理的全过程。

五、安全管理工作流程

（一）安全检查工作流程

1. **制定安全检查计划**
   a. 安全管理委员会根据公司实际情况，制定年度安全检查计划，明确检查时间、检查内容、检查方式和检查责任人。
2. **组织实施安全检查**
   a. 按照安全检查计划，各部门组织人员对本部门的安全工作进行自查，同时安全管理委员会组织人员对各部门进行综合检查和专项检查。
3. **汇总检查结果**

a. 检查人员将检查结果进行汇总，形成安全检查报告，报告内容包括检查发现的安全隐患、整改建议等。

4. **下发整改通知**

a. 安全管理委员会根据安全检查报告，向相关部门下发整改通知，明确整改责任人、整改期限和整改要求。

5. **整改落实与复查**

a. 相关部门按照整改通知要求，制定整改措施，落实整改工作。整改完成后，向安全管理委员会提交整改报告。安全管理委员会组织人员对整改情况进行复查验收，确保隐患得到彻底整改。

（二）安全事故处理工作流程

1. **事故报告**

a. 发生安全事故后，事故现场人员必须立即向本部门负责人报告，部门负责人接到报告后，必须在[具体时间]内向安全管理委员会报告。

2. **启动应急预案**

a. 安全管理委员会接到事故报告后，立即启动安全事故应急预案，组织人员进行应急处理，控制事故影响范围，防止事故扩大。

3. **事故调查**

    a. 成立事故调查小组，对事故进行调查分析，查明事故原因、经过和责任，形成事故调查报告。

4. **事故处理**

    a. 根据事故调查报告，对事故责任人进行处理，追究相关责任人的责任。同时，制定整改措施，落实整改工作，防止类似事故再次发生。

5. **事故总结**

    a. 对事故处理情况进行总结，分析事故教训，完善公司安全管理制度和应急预案，提高公司安全管理水平。

六、安全管理工作考核与奖惩

1. **考核**

    a. 公司将安全管理工作纳入各部门和员工的绩效考核体系，定期对各部门和员工的安全管理工作进行考核评价。考核内容包括安全管理制度的落实情况、安全隐患的整改情况、安全事故的发生情况等。

2. **奖励**

a. 对在安全管理工作方面表现突出的部门和个人，公司将给予表彰和奖励，奖励形式包括奖金、荣誉证书、晋升机会等。

3. **处罚**

a. 对违反安全管理制度、造成安全隐患或安全事故的部门和个人，公司将根据情节轻重给予相应的处罚，处罚形式包括罚款、通报批评、降职降级等。对造成重大安全事故的责任人，公司将依法追究其法律责任。

七、附则

1. 本制度由公司安全管理委员会负责解释。

2. 本制度自发布之日起生效实施。

捷荟信息技术（上海）有限公司

2024-10-12