百融云创科技股份有限公司信息安全管理要点

在百融云创科技股份有限公司，我们严格遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规的要求，致力于保护客户数据和公司信息的安全。以下是我们在信息安全管理方面的关键措施：

一、数据安全策略

1. 数据访问权限控制

实施严格的数据访问审批和授权机制，确保数据访问的最小授权和必要性。

数据访问的网络策略控制，防止未经授权的访问。

2. 数据加密传输

使用专线、VPN、HTTPS 等安全链路和加密协议进行数据传输，确保数据在传输过程中的安全性。

3. 数据存储

- 使用安全的加密技术 AES256、SHA256 对重要数据进行加密存储。
- 根据数据安全级别，对数据进行分域分级存储，确保不同存储域之间的物理或逻辑隔离。
- 建立数据备份与恢复机制，定期测试备份数据，确保在需要时可用。

4. 数据删除

数据删除与销毁已建立完善的流程和处理机制，判定为存储“企业机密”的磁盘必须消磁处理，存储“企业秘密”和“内部公开”信息的磁盘复用前必须反复擦写确保数据不可复用，所有的操作过程必须有双人进行，并对销毁过程进行记录和确认。

二、数据合规性管理

1. 法律法规遵循

- 积极配合外部监管机构的安全监督，梳理外部信息安全合规相关法律法规、标准等，建立并维护合规清单。
- 重要系统根据《网络安全法》要求进行等级保护三级备案，并按照等级保护三级的测评要求进行系统创建和运营维护。

2. 国际标准认证

- 参照国际先进标准进行信息安全管理体系建设，并于 2016 年获得 ISO27001 信息安全管理体系认证。
- 2020 年 9 月，百融率先通过国内权威认证机构中国质量认证的审核，获得了 ISO27701 隐私信息管理体系认证。

三、安全意识培训

1. 定期培训

定期组织安全意识及数据安全相关培训，包括政策、法律、法规、标准等安全知识保护培训工作。

针对关键和特殊岗位开展专门的数据安全培训，并定期审核和更新培训内容。

2. 每月期刊

每月底针对最新信息安全时事向全员发送信息安全期刊，通过具体案例，向全员传达信息安全关注要点，持续提升员工信息安全意识。

四、信息安全应急响应

1. 应急响应机制

- 建立完善的信息安全应急响应机制，制定详细的应急预案，确保在发生信息安全事件时能够迅速响应和处理。
- 定期进行应急演练，检验和提升应急响应能力，确保应急预案的有效性和可操作性。

2. 事件报告与处理

- 设立信息安全事件报告渠道，确保员工能够及时报告安全事件。
- 对信息安全事件进行及时处理，记录事件详细过程。

3. 持续改进

- 对信息安全事件进行总结和分析，找出问题根源，制定改进措施，防止类似事件再次发生。
- 定期评估和更新应急预案，确保其与时俱进，符合最新的安全形势和要求。

以上内容展示了百融云创科技股份有限公司在信息安全管理方面的承诺和措施，确保客户数据和公司信息的安全与合规。