第一章 总则

第一条 目的和依据

为保障OSS服务的安全、稳定和可靠性，规范OSS的使用和管理，制定本规定。

第二条 适用范围

本规定适用于公司所有人员使用和管理OSS服务的行为。

第三条 定义

OSS：指阿里云对象存储服务。

OSS管理员：指负责OSS管理和操作的人员。

OSS用户：指通过授权能够访问OSS服务的人员。

第二章 OSS账号管理

第四条 账号权限管理

OSS账号必须按照最小权限原则进行授权，不得越权访问。

禁止使用共享密码或弱密码，必须使用安全性强的密码并定期更换。

第五条 账号的监管

对于长期未使用的OSS账号应及时注销。

定期检查OSS账号的安全性，并及时更新账号信息和密码等。

第三章 数据加密

第六条 数据加密

对于重要数据和敏感数据必须进行加密处理。

建议使用TLS等加密协议来保护数据传输过程中的安全。

第四章 访问控制

第七条 访问策略管理

OSS管理员必须对OSS的访问凭证进行合理的分配和管理，规定访问策略。

禁止将OSS的访问凭证泄露给未经授权的人员。

第八条 访问控制列表

建立访问控制列表（ACL）来限制不同用户对存储桶和对象的访问权限。

对于重要数据和敏感数据，应设置更加严格的访问控制规则，只允许有必要权限的用户进行访问。

第五章 法律责任

第九条 法律责任

OSS管理员应遵守国家法律法规和公司安全规定，保障OSS服务的安全使用。

如因OSS服务使用问题导致法律纠纷或损失，OSS管理员需要承担相应的法律责任。

第六章 附则

第十条 本规定解释权归公司所有。

对本规定的解释权归公司信息安全部门所有。

本规定自发布之日起生效。

各分公司子公司可以根据实际情况制定具体操作细则，但不得违反本规定。