第一章 总则

第一条 目的和依据

为保障K8S服务的安全、稳定和可靠性，规范K8S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K8S服务的行为。

第三条 定义

K8S：指Kubernetes容器编排工具。

K8S管理员：指负责K8S管理和操作的人员。

K8S用户：指通过授权能够访问K8S服务的人员。

第二章 K8S集群、节点安全

第四条 集群、节点的安全

禁止在K8S集群中允许任何未经验证和未知来源的镜像。

对于K8S节点，必须对系统进行加固，并采取必要的安全措施，如关闭不必要的服务、限制访问权限、强化账号密码等。

第五条 节点的监管

定期检查K8S节点的安全性，并及时更新节点信息和密码等。

对长期未使用的K8S节点应及时停用或注销。

第三章 应用程序安全

第六条 应用程序的安全

禁止在K8S集群中运行未经授权或不明确来源的应用程序。

对于容器镜像，必须定期检查并更新，保证其安全性。

第七条 基础设施安全

对于K8S的基础设施，如etcd、API Server等组件，必须进行加固和安全配置。

对于敏感数据，建议使用Secret来存储和管理。

第四章 访问控制

第八条 访问策略管理

K8S管理员必须对K8S的访问凭证进行合理的分配和管理，规定访问策略。

禁止将K8S的访问凭证泄露给未经授权的人员。

第九条 访问控制列表

建立访问控制列表（ACL）来限制不同用户对K8S资源的访问权限。

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

第十条 法律责任

K8S管理员应遵守国家法律法规和公司安全规定，保障K8S服务的安全使用。

如因K8S服务使用问题导致法律纠纷或损失，K8S管理员需要承担相应的法律责任。

第六章 附则

第十一条 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。