

企业应通过权限控制、访问控制、加密技术、知识管理培训等不同手段或工具来明确知识的使用和传输规则，确保知识得到有效保护，避免未授权的使用和传输。

6.4 知识的存储和更新

企业应通过技术手段管理知识，采用标准化的流程和丰富的技术功能进行知识的存储、更新和维护，以保障知识的可用性、完整性和安全性，进而支持知识的获取、使用、共享与协作。知识的更新是一个持续性过程，应保留知识更新日志，定期审查知识更新，以确保知识的时效性、准确性和完整性。

7 知识库系统建设

7.1 系统设计

7.1.1 总体架构图设计

知识库总体架构设计应基于实用性、业务相关性、兼容性、扩展性等原则，提出要求：

- 系统层面：总体架构图应清晰展示系统的各个组成部分及其相互之间的关系，包括前端展示层、业务逻辑层、数据访问层及数据存储层等。设计时应考虑未来功能扩展的需求，架构图需体现模块间的低耦合性，便于新增或修改功能模块；
- 业务层面：根据知识管理的要求，从知识生命周期管理层面，涵盖知识的创建、获取、分类、分级、使用、传输、存储、更新、删除等要素；
- 安全层面：明确标注安全组件和防护策略，如数据加密、访问控制、权限管理、分级标签、日志审计等要素，确保知识库数据的安全性和隐私保护；
- 功能层面：知识库总体架构图应涵盖知识展示、知识检索、知识推荐、知识学习、共享与协作等要素；
- 用户层面：知识库总体架构图应涵盖管理者、协作者等要素。

7.1.2 软硬件环境要求

知识库运行应适配组织内部软硬件环境，包括但不限于硬件设备、软件及相关中间件、操作系统、数据库、服务器等。

7.1.3 系统集成与接口设计要求

知识库应设置系统集成与接口设计要求，具体如下：

- 集成功能：知识库应具有良好的集成能力，在确保安全性的前提下，其接口设计应易于扩展和维护，具备开放性、兼容性；
- 信息安全机制：通过访问控制、入侵检测、口令认证、恶意代码防范等措施，确保接口及整体系统的安全性。

7.2 实现功能

7.2.1 知识展示

企业应通过多种方式与角度进行知识的展示，具体如下：

- a) 多样化展示，包括支持文本、图像、视频、音频、3D 等多种类型和 Word、EXCEL、PDF、PPT 等多种格式的知识展示；
- b) 多结构展示，根据知识类型（如 FAQ 是专业术语吗？、教程、案例等）进行分类展示，提供列表、平铺、瀑布流等多种形式的展示方式，以及分层式、主题式、流程式等不同导航结构；
- c) 个性化界面，界面设计应符合用户习惯，支持自定义主题、布局等，提升用户体验。

7.2.2 知识检索

知识库应支持高效的多维度检索能力，包括：

- 通过名称、色彩、标签、图片、格式、创建时间、更新时间等多种方式快速定位知识内容；
- 需支持全文搜索、模糊搜索、联想搜索等智能搜索功能；
- 支持通过关键词组合、条件筛选等方式进行高级查询，满足复杂查询需求；

——优化搜索算法，提高搜索速度和准确性，同时考虑搜索结果的排序、去重和展示方式。

7.2.3 知识推荐

知识库建设宜合理应用新技术，采用合适的推荐算法，构建适用于组织的领域知识图谱，引入用户反馈机制（详见8.5），以适应不同的知识应用场景和知识特性，提高知识推荐的准确性。

7.2.4 知识学习（学习与统计）

知识库建设应可合理设计用户中心，便于统计用户的知识学习进度，包括：

- 提供在线课程、视频教程等学习材料，支持进度跟踪、笔记记录等功能；
- 设置测试题、问卷等评估工具，帮助用户检验学习效果；
- 根据用户的学习目标和当前水平，推荐合适的学习路径；
- 设计收藏、评论、审阅等不同互动形式，便于用户学习。

7.2.5 知识反馈与评价机制

知识库建设应建立知识反馈与评价机制。

7.3 部署与运营

7.3.1 系统部署

知识库的部署应简化安装和配置流程，支持本地部署，支持与第三方业务系统的无缝集成，确保知识库的高可用性。

7.3.2 系统升级与维护

企业应建立知识库管理流程，制定知识库升级和维护计划，确保知识库的持续更新和优化。

8 知识库运营管理

8.1 访问控制

8.1.1 用户身份验证

知识库应设置用户身份验证，具体要求如下：

- 应实施多因素身份验证，包括但不限于用户名/密码、动态令牌、生物识别技术或单点登录（SSO）集成等；
- 定期审查用户身份验证信息的有效性，并提醒用户更新密码。

8.1.2 访问权限设置

知识库应设置访问权限，具体要求如下：

- 根据用户角色和岗位需求，设定精细化的访问权限控制，权限应涵盖读取、编辑、删除等不同操作级别；
- 实施最小权限原则，即只授予用户所需的最小权限。

8.2 信息加密与脱敏

8.2.1 加密标准与方式

为确保知识库的安全，应做好加密相关工作：

- 明确加密范围，包括但不限于用户数据、知识文档、账号信息等，确保数据在传输和存储过程中的安全性；
- 应遵循国际或行业内公认的加密标准，如AES（高级加密标准）、RSA（非对称加密算法）等。

8.2.2 脱敏标准与策略

知识库管理注重保密的同时，应制定脱敏策略与方法：

- 制定数据脱敏策略，对非必要公开的敏感信息（如身份证号、电话号码、银行账户等）进行脱敏处理，降低数据泄露风险；
- 根据数据类型和业务需求选择合适的脱敏方法，如替换、掩码、哈希等，并确保脱敏后的数据仍能满足业务分析需求。

8.3 稳定性保障

8.3.1 数据备份

知识库应定期做好备份，具体要求如下：

- 建立定期自动备份机制，确保知识库数据的完整性和可恢复性，备份数据应存储在物理上分离的安全位置；
- 定期测试备份数据的恢复流程，以确保在紧急情况下可以快速恢复数据。

8.3.2 灾难恢复

有条件的情况下，应建立恢复计划，具体要求如下：

- 制定详细的灾难恢复计划，包括灾难识别、应急响应、数据恢复、业务恢复等流程，以应对自然灾害、人为错误、系统故障等突发事件；
- 定期进行演练和评估，以优化恢复流程和缩短恢复时间。

8.3.3 应急响应流程

企业应建立应急响应团队与流程：

- 建立应急响应团队，明确团队成员职责和应急响应流程，包括事件报告、初步评估、应急措施执行、事后总结等；
- 定期进行应急响应演练，确保流程的快速启动和有效执行。

8.4 定期更新与维护

8.4.1 内容更新策略

知识库的内容应做好定期更新：

- 制定内容更新策略，包括更新频率、更新范围、更新流程等，确保知识库内容的时效性和准确性；
- 建立内容审核机制，对增减或修改的内容进行审核，确保信息的准确性和合规性。

8.4.2 系统维护计划

制定系统维护计划，包括维护时间、维护内容、影响范围等，确保知识库系统的稳定运行。

8.4.3 更新与维护记录

知识库应有定期更新与维修记录：

- 记录每次更新和维护的详细信息，包括时间、人员、操作内容、结果等；
- 定期对更新和维护记录进行审查和分析，以改进未来的更新和维护工作。

8.5 用户反馈收集

8.5.1 反馈渠道建立

为方便使用并能及时做好更新，应建立用户反馈渠道：

- 提供多种用户反馈渠道，如在线表单、电子邮件、电话等；
- 确保反馈渠道的畅通和易用性，并及时响应用户反馈。

8.5.2 反馈处理流程

针对用户反馈，应制定反馈处理流程：

- 制定反馈处理流程，包括接收反馈、分类处理、反馈回复、改进措施等步骤，确保用户反馈得到妥善处理；

——对反馈进行分类和优先级排序，快速响应并有效解决用户问题，同时根据反馈结果不断优化知识库服务和内容。

9 知识库评估

9.1 知识库的定期盘点和评估

9.1.1 知识价值的评估

企业应定期通过内容分析、用户满意度调研等方式检查知识库里知识的时效性、准确性、相关性、完整性以及对业务的影响力，根据评估结果及时对知识内容进行删减和更新，以保持知识价值满足企业发展需求。

9.1.2 访问及使用情况的评估

企业应定期使用统计和分析工具追踪知识库的关键指标，包括但不限于访问量、使用频率、搜索次数、页面浏览次数，及时了解用户的兴趣点和行为模式，发现潜在的问题和改进点，以提升用户体验。

9.1.3 知识架构及安全性的评估

企业应定期根据用户的反馈评估知识架构是否清晰、合理，导航及搜索功能是否准确、高效，知识安全等级设置是否合理，并根据评估结果及时做出调整。

9.2 知识分享的评价与奖励

9.2.1 知识分享的评价

企业宜建立知识分享评级机制，鼓励内部员工分享知识。根据课后人员参与度、满意度调研等方式进行评价，评级为优秀的课程可推荐至公司层面进行宣讲授课。

9.2.2 知识分享的奖励

企业宜设置知识分享的奖励机制，对于分享的企业员工进行物质奖励，鼓励企业知识的积累与传承。

9.3 知识库的持续改进

企业通过综合、深入、全面的评估，了解知识库运行情况，及时发现问题、解决问题，为持续改进和不断优化提供方向，以确保更好地满足用户的需求。
