Enterprise Knowledge Decay Prevention Agent (EKDPA)

1. Purpose

This document defines critical organizational knowledge, identifies risks associated with knowledge loss, and provides guidelines to prevent knowledge decay. It serves as the foundational knowledge base for the Knowledge Guardian Agent.

---

2. Critical Knowledge Definition

Critical knowledge includes:

- **Processes not documented:** Key workflows, decision-making, and operational procedures that exist only in employees' heads.
- **Single person dependencies:** Knowledge that resides with one individual without redundancy.
- **Business-critical systems:** Knowledge necessary for revenue, compliance, security, or operational continuity.
- **Historical decisions and rationale:** Context for past decisions, vendor negotiations, and system configurations.

---

3. Risk Thresholds

Risk Level	Criteria
HIGH	Tenure > 3 years AND Documentation < 40% OR Ownership = 1
MEDIUM	Tenure 1–3 years AND Documentation 40–70%
LOW	All other combinations; documentation ≥70% OR multiple knowledge owners

---

4. Knowledge Capture Checklist

To secure knowledge at risk, follow these steps:

1. **Identify critical processes and systems**

    - Interview key employees.
    - Map workflows.
2. **Collect artifacts**
    - Documentation, diagrams, recordings, templates.
3. **Guided prompts for capturing knowledge**
    - “Explain the key failure points in system X.”
    - “Top 3 things a replacement must know.”
    - “List undocumented dependencies or shortcuts.”
4. **Cross-training and redundancy**
    - Assign backup owners for each critical knowledge area.
    - Schedule shadowing or mentoring sessions.
5. **Validation**
    - Peer review and confirmation of captured knowledge.
    - Ensure a minimum of 2 confirmed owners per knowledge area.
6. **Handover and integration**
    - Update internal repositories (Confluence, SharePoint, Git, etc.).
    - Tag ownership, risk level, and next review date.

---

5. Metrics and Monitoring

- **Documentation coverage (%):** Aim for ≥70% for high-criticality roles within 6 months.
- **Ownership redundancy:** Minimum 2 owners per critical system or process.
- **Knowledge secured rate:** % of critical knowledge captured and validated.
- **Knowledge decay events prevented:** Number of scenarios where knowledge loss is mitigated.

---

6. Agent Usage

- This document is used by the **Knowledge Guardian Agent** in IBM watsonx Orchestrate to:
    - Evaluate knowledge at risk.
    - Trigger automated knowledge capture workflows.
    - Validate knowledge via human-in-loop review.
    - Ensure knowledge is integrated into central repositories.

---

7. Governance

- Assign a **Knowledge Steward** per department.
- Quarterly audits of knowledge coverage and ownership.
- Update workflows as processes or roles change.