Risk Summary Report – SentraNova AI Solutions

Date: 1/4/2026
Prepared By: Ariel Bethea

Executive Overview

This report summarizes the highest-priority information security and privacy risks identified during the current risk assessment cycle. Risks are ranked based on **inherent risk scores** and evaluated against the organization's defined **risk appetite**. All risks listed below currently **exceed appetite and require active management attention**.

Top Enterprise Risks Requiring Management Attention

1. Data Breach Due to Unauthorized Access

- **Risk ID:** R-001
- **Inherent Risk Score:** 25 (High – Exceeds Appetite)
- **Key Impact:** Data breach, regulatory exposure, reputational harm
- **Recommended Management Actions:**
    - Implement multi-factor authentication (MFA) for all privileged and remote access
    - Enforce least privilege access controls across systems and data repositories
    - Establish weekly access log review procedures
- **Primary Controls:** A.5.15 (Access Control), A.5.16 (Identity Management)

---

2. Loss of Personally Identifiable Information (PII) Due to Improper Deletion

- **Risk ID:** R-007
- **Inherent Risk Score:** 20 (High – Exceeds Appetite)
- **Key Impact:** Regulatory fines, contractual exposure, loss of customer trust
- **Recommended Management Actions:**
    - Implement standardized secure data deletion procedures

    - Validate deletion effectiveness through periodic testing and review
- **Primary Controls:** A.8.10 (Information Deletion), A.5.34 (Privacy and Protection of PII)

---

3. Unauthorized Access to Source Code

- **Risk ID:** R-010
- **Inherent Risk Score**: 20 (High – Exceeds Appetite)
- **Key Impact:** Intellectual property loss, competitive disadvantage
- **Recommended Management Actions:**
    - Restrict source code access based on defined roles and responsibilities
    - Perform regular audits of repository permissions and access logs
- **Primary Controls:** A.8.4 (Access to Source Code)

Next Steps

- Assign accountable owners for all mitigation actions
- Track residual risk levels, target dates, and review cycles in the Risk Register
- Monitor remediation progress and risk trends through ISMS governance and management review meetings