Microsoft Dataverse Security

Enterprise Governance & Compliance Checklist

Microsoft Dataverse offers the most robust security model in the Power Platform, but only if configured correctly. This checklist covers the essential layers of defense required to protect sensitive HR, Legal, and Corporate data in a production environment.

Phase 1: Environment & Identity

- [ ] **Security Group Strategy**
  Assign an Entra ID (formerly Azure AD) Security Group to the Dataverse environment to restrict entry at the gate.
- [ ] **Business Unit (BU) Hierarchy**
  Define the BU structure to match organizational data silos, ensuring managers can only see their team's records.
- [ ] **Administrative Role Minimization**
  Audit 'System Administrator' roles. Assign 'Environment Admin' only to those requiring full platform control.

Phase 2: Table & Record Security

- [ ] **Security Role Customization**
  Avoid using out-of-the-box roles. Create custom roles following the Principle of Least Privilege (PoLP).
- [ ] **Row-Level Security (RLS)**
  Configure ownership-based access so users can only Read/Update records they own or those shared with their BU.
- [ ] **Field-Level Security (FLS)**
  Identify highly sensitive columns (e.g., SSN, Salary) and enable FLS to hide them from unauthorized users within a role.

THE "LEGAL & HR" PILLAR:

For Legal and HR teams, implement **COLUMN SECURITY PROFILES** and **HIERARCHY SECURITY**. This prevents sensitive grievances or legal discovery data from being visible to IT staff or cross-departmental peers.

Phase 3: Data Loss Prevention (DLP)

- [ ] **Connector Classification**
  Group connectors into 'Business' and 'Non-Business' categories in the Power Platform Admin Center.

- [ ] **Cross-Tenant Isolation**
  Enable tenant isolation to prevent data from being exfiltrated to external Power Platform environments.