|  |  |
| --- | --- |
| **MICROSOFT 365 ADMIN REFERENCE SHEET**  Where to find governance, protection & enablement reports in your M365 tenant | **🔒 GOVERN** │ **PROTECT** │ **ENABLE 🚀**  Three Locks™ Framework | AI Governance Workshop |
|  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **GOVERN**  Own it. Track it. Report on it. |  | **PROTECT**  Lock down data. Detect risk. |  | **ENABLE**  Deploy safely. Measure adoption. |
|  |  |  |  |  |
| 📂 **SharePoint — Site Usage & Sharing Reports**  📍 admin.microsoft.com → SharePoint Admin → Active Sites  Inactive sites, site permissions, storage per site; flag oversharing risks |  | 🔒 **Microsoft Purview — Data Loss Prevention**  📍 compliance.microsoft.com → Data Loss Prevention  Active DLP policies, policy matches, and incident reports; configure data-tier-based rules |  | ✅ **Microsoft 365 Apps Usage Report**  📍 admin.microsoft.com → Reports → Usage → Microsoft 365 Apps  Which M365 apps are actively used vs. licensed; identify underutilized Copilot seats |
|  |  |  |  |  |
| 🔐 **SharePoint — Data Access Governance**  📍 SharePoint Admin Center → Reports → Data Access Governance  Site permissions, sensitivity labels, sharing reports, site policy comparisons |  | 🏷 **Sensitivity Labels (MIP) — Label Usage Report**  📍 compliance.microsoft.com → Information Protection → Label Activity  Which labels are applied, by whom, and to what content; catch mislabeled or unlabeled files |  | 🤖 **Microsoft Copilot Usage Report**  📍 admin.microsoft.com → Reports → Usage → Microsoft 365 Copilot  Copilot adoption by user, app, and activity type; track engagement and feature usage |
|  |  |  |  |  |
| 🔑 **Azure AD / Entra ID — Roles & Admins**  📍 entra.microsoft.com → Roles & Admins  All global admins, privileged roles, and custom role assignments across your tenant |  | 🌐 **Defender for Cloud Apps — Block Unsanctioned AI**  📍 security.microsoft.com → Cloud Apps → Discovered apps  Filter Category = Generative AI > Select tool & mark as ‘unsanctioned’. |  | ⚙ **Microsoft Copilot Settings & Controls**  📍 admin.microsoft.com → Settings → Microsoft 365 Copilot  Enable/disable Copilot per license group; configure data access scope and plugin controls |
|  |  |  |  |  |
| 📋 **Microsoft Purview Compliance Portal**  📍 compliance.microsoft.com → Policies  Central hub for all compliance policies: DLP, retention, communication compliance, insider risk |  | 🌐**Defender for Endpoint – Setup for Blocking**  📍 security.microsoft.com → Settings → Endpoints  1. Settings > Endpoints > Advanced Features. 2. Toggle Network protection to ‘On’ 3. Go to Settings >Cloud apps > Cloud Discovery 4. Enable MS Defender for Endpoint integration. |  | 🛡 **Azure AD / Entra — Conditional Access Policies**  📍 entra.microsoft.com → Protection → Conditional Access  Enforce MFA, device compliance, and location rules before granting access to AI tools |
|  |  |  |  |  |
| 🌐 **Defender for Cloud Apps — Shadow AI Discovery**  📍 security.microsoft.com → Cloud Apps → Cloud App Discovery  Detect unsanctioned AI tools being used on your network; see usage volume and risk scores |  | 👁 **Entra ID — Sign-In Logs & Risky Sign-Ins**  📍 entra.microsoft.com → Monitoring → Sign-In Logs  All user sign-ins; filter by app, location, risk level; detect unauthorized AI tool access |  | 📲 **App Governance — OAuth App Activity**  📍 security.microsoft.com → Cloud Apps → App Governance  All third-party OAuth apps connected to your tenant; revoke unapproved AI integrations |
|  |  |  |  |  |
| 🗂 **Microsoft 365 Groups & Teams Governance**  📍 admin.microsoft.com → Teams & Groups  See all M365 Groups, Teams, and ownership; identify unowned or ungoverned groups |  | 🚨 **Microsoft Defender — Alerts & Incidents**  📍 security.microsoft.com → Incidents & Alerts  Security incidents across M365; filter for data exfiltration, unusual file access, DLP triggers |  | 🎓 **Viva Learning — Training Completion**  📍 admin.microsoft.com → Viva → Viva Learning → Reports  Track AI governance training completion rates by department; export for compliance records |
|  |  |  |  |  |
| 🧾 **Audit Log — Admin Activity**  📍 compliance.microsoft.com → Audit → Audit Search  Full log of admin-level changes: policy edits, role changes, app grants, DLP modifications |  | 📊 **Purview — Insider Risk Management**  📍 compliance.microsoft.com → Insider Risk Management  Detect risky user behaviors: mass downloads, sharing to personal accounts, AI data exfiltration |  | 📈 **Adoption Score & Microsoft 365 Usage Analytics**  📍 admin.microsoft.com → Reports → Adoption Score  Measure how effectively your org uses M365; identify teams ready for AI enablement |
|  |  |  |  |  |
|  |  |  |  | 🔗 **Teams App Permission Policies**  📍 admin.teams.microsoft.com → Teams Apps → Permission Policies  Control which third-party AI apps can be installed in Teams; create allowlists by user group |

|  |
| --- |
| **💡 TIP:** All reports above require appropriate admin roles (Global Admin, Security Admin, Compliance Admin, or Reports Reader). Assign the least-privileged role that meets the need. Access paths are current as of Microsoft's 2025 admin portal layout and may shift with product updates. |