Roles and Permissions for Data Loss Prevention

Role Name	Built-In Role	Can Create/Edit DLP Policies	Can View DLP Reports	Typical Use Case
Compliance Administrator	✅ Yes	✅ Yes	✅ Yes	Full DLP access – create, manage, and monitor DLP across Microsoft 365
Compliance Data Administrator	✅ Yes	✅ Yes	✅ Yes	Access and manage sensitive data in SharePoint, Exchange, OneDrive
Information Protection Admin	✅ Yes	✅ Yes	✅ Yes	Manage DLP, sensitivity labels, and classification settings
Information Protection Reader	✅ Yes	❌ No	✅ Yes	Read-only access to DLP alerts, label activity, and reports
Security Administrator	✅ Yes	⚠️ Limited*	✅ Yes	Focused on security configuration, some DLP access if scoped
Security Reader	✅ Yes	❌ No	✅ Yes	Can monitor and investigate DLP alerts, but not modify policies
Global Administrator	✅ Yes	✅ Yes	✅ Yes	Has all permissions; not recommended for routine DLP tasks
Custom Role (Scoped Admin)	🚫 No	✅ (If configured)	✅ (If configured)	Use for delegated DLP management in specific regions or departments

*Security Administrator can manage alerts and see reports, but cannot create/edit DLP policies unless granted additional roles like Compliance Administrator.