dryvIQ

AI-Ready Data Checklist

Whether you're preparing for agentic AI, generative AI, copilots, or other data-driven initiatives, use our checklist to ensure your data is relevant, organized, cleansed, secured, and ready for what's next.

Is Your Platform Built to Support AI-Ready Data?

○ Assess your storage systems for AI readiness: Does your current platform easily integrate with AI & analytics technologies?

○ Migrate unstructured data from legacy storage systems to modern, AI-capable platforms.

○ Set up continuous sync to ensure your data stays current and accessible.

Is Your Data Ready for AI Initiatives?

○ Define your AI goals and target high-impact GenAI use cases.

○ Implement an intelligent data management platform to curate use-case-specific data sets to train your AI models with the right data.

○ Automatically eliminate outdated, duplicate, or irrelevant files to eliminate hallucinations and boost AI accuracy.

○ Regularly audit your content to keep data clean, usable, and AI-ready for future initiatives.

Is Content Organized for Efficiency?

○ Shore up data governance to ensure all data is easy to find, protect, and manage.

○ Automate unstructured data classification based on file contents, and apply rich metadata.

○ Automatically organize files into correct taxonomies and move them to new locations to fuel your data initiatives.

○ Customize entity recognition and document classification to match your business needs as they evolve.

Has Your Sensitive Data been Cleansed?

○ Prevent sensitive data like PII, IP, or other non-public info from being used in AI training by enforcing classification-based controls.

○ Apply redaction, encryption, and anonymization to protect sensitive info while preserving high-value insights for AI and data-driven initiatives.

○ Automate compliance processes to safeguard sensitive data as AI use grows.

Are Your Security Measures Robust Enough for AI-Driven Operations?

○ Enforce strict access controls and continuously audit sharing permissions to ensure only authorized users have access to sensitive data.

○ Apply security labels and policies (like MPIP or Box Shield) in real time to safeguard content automatically.

○ Quarantine exposed or high-risk files immediately and block unauthorized sharing to prevent data breaches.

○ Regularly review and update security policies to stay ahead of evolving threats and maintain trust in your AI-ready data.