Microsoft Security

AI-Ready in Four Steps: A Data Preparation Guide

Data drives AI, but it also introduces challenges like data oversharing, data leakage, and noncompliant usage that can compromise security.

Top data challenges

1. Data oversharing
Users may gain unauthorized access to sensitive data via AI apps due to a lack of labeling policies or appropriate access controls.

2. Data leakage
Users may inadvertently leak sensitive data to unsanctioned AI apps. Sanctioned apps expose data if AI-generated responses don't inherit the data protection controls of the referenced files.

3. Noncompliant usage
Users may generate high-risk content or content that doesn't abide by ethical standards with AI apps.

Four steps to take before diving into AI

Step 1: Know your data.

Identify where your data resides and understand how it will travel through your AI systems.

30% of decision-makers report lacking full visibility into their business-critical data[1]

Checklist

- **Identify sensitive data:** Locate where sensitive data resides and assess how it is accessed and used throughout your organization.
- **Classify data:** Apply predefined or custom classifications to ensure sensitive data is accurately labeled for proper management and protection.
- **Enable user labeling:** Empower users to manually label sensitive files within their applications to enhance real-time data protection and control.

Mitigating key data challenges

1. **Data oversharing**
Labeling sensitive data ensures only authorized users have access, reducing oversharing.
2. **Data leakage**
Clear labeling and access controls minimize the risk of data leaking to unauthorized AI applications.
3. **Noncompliant usage**
Classifying data helps enforce compliance, preventing inappropriate use within AI apps.

Step 2: Protect your data.

Establish clear guidelines to help ensure that sensitive data is properly safeguarded against unauthorized access.

87% of security leaders report having experienced a data breach in the past 12 months[2]

Checklist

- **Set access and protection levels:** Apply rights management, encryption, and watermarks based on sensitivity.
- **Enable user and admin labeling:** Ensure consistent data classification by allowing both manual and automated labeling.
- **Ensure secure collaboration:** Use sensitivity labels to control sharing and maintain alignment with protection policies.

Mitigating key data challenges

1. **Data oversharing**
Sensitivity labels and permissions control access, ensuring users interact only with data they are authorized to view.
2. **Data leakage**
Labeling sensitive data adds protections like encryption, reducing the risk of leakage to unsanctioned apps.
3. **Noncompliant usage**
Applying rights management and encryption safeguards sensitive information from misuse.

Step 3: Govern your data.

Implement governance policies to maintain control and ensure compliance with evolving AI regulations.

55% of leaders admit they don't fully understand AI regulations[3]

Checklist

- **Clean up data and permissions:** Regularly review and update access to ensure authorized control.
- **Apply content management policies:** Govern data retention and deletion across platforms and delete outdated data.
- **Monitor AI interactions:** Track AI usage and detect noncompliant activities.
- **Prepare for regulatory standards:** Stay informed on new AI regulations, such as the European Union Artificial Intelligence Act (EU AI Act) and the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF).
- **Commit to responsible AI:** Adopt AI governance frameworks to align with data protection standards.

Mitigating key data challenges

1. **Data oversharing**
Governance policies allow you to audit and update access, preventing unintentional data sharing.
2. **Data leakage**
Monitoring AI usage and enforcing access controls helps prevent unauthorized data transfers.
3. **Noncompliant usage**
Auditing and monitoring ensure compliance, reducing the risk of unethical content creation.

Step 4: Prevent data loss.

Establish Data Loss Prevention (DLP) policies to secure AI-generated content and mitigate the risks of data exfiltration across multiple channels.

>80% of organizations rate theft or loss of personal data and intellectual property as high-impact insider risks[4]

Checklist

- **Implement DLP policies:** Prevent unintentional sharing or loss of business-critical data.
- **Extend DLP across platforms:** Ensure protection covers devices, browsers, file shares, and messaging platforms.
- **Control access to AI-generated data:** Restrict access based on user roles and responsibilities.
- **Apply data security to AI prompts and responses:** Use encryption, watermarking, and labeling for AI data.
- **Restrict sensitive data in AI prompts:** Limit high-risk users from sharing sensitive data in AI tools.

Mitigating key data challenges

1. **Data oversharing**
DLP policies monitor and restrict data sharing across channels to prevent unauthorized access.
2. **Data leakage**
DLP safeguards sensitive data by controlling transfers to unsanctioned applications.
3. **Noncompliant usage**
DLP restricts sensitive data in AI prompts, reducing the risk of misuse in high-risk activities.

Help keep your organization's data safe

To get the most out of AI and ensure data security, start with a comprehensive plan to understand your data, safeguard it, govern its use, and prevent data loss.

For additional insights, download the e-book: Strengthen your organizations digital security: Protect your data and build trust

For more information on how to keep your organization's data safe, explore our Security Program for nonprofit organizations.

@msftnonprofits

facebook.com/msftnonprofits

linkedin.com/showcase/microsoft-for-nonprofits

[1] Microsoft, Survey of 510 US compliance decision-makers commissioned from agency Vital Findings, March 2023
[2] "Rethinking Security from the Inside Out," Microsoft, page 7, March 2024
[3] "12 Trends Shaping the Future of Digital Business," Gartner, Inc., 2022
[4] "Portal26 Research Report: State of Generative AI 2023," Portal 26 and CensusWide, page 5, November 2023