

 AI

THE AI SECURITY PLAYBOOK: 6 Essentials Every Sales Organization Needs

A practical guide to minimizing risk and maximizing trust when using AI in your business.

As AI becomes an essential part of the sales toolkit, it's critical to protect your business and client relationships. These six foundational steps will help your team use AI tools responsibly and securely.

 01

Establish Clear AI Sales Usage Policy

WHAT IT IS: Internal guidance outlining how AI tools should, and should not, be used.

WHY IT MATTERS: Sets clear expectations and helps your sales team avoid risk, confusion, or misuse.

PUT IT INTO PRACTICE:

- Define acceptable vs. unacceptable use cases.
- Specify what types of data can be entered into AI tools.
- Include rules for public AI vs. approved vendor tools.
- Address client confidentiality, IP protection, and ethical concerns.

 02

Limit Access to Tools and Data

WHAT IT IS: Restricting AI tools and sensitive data to only those who need them.

WHY IT MATTERS: Reduces accidental misuse or unauthorized access.

PUT IT INTO PRACTICE:

- Use single sign-on (SSO) and multi-factor authentication.
- Set user permissions based on roles.
- Keep a record of who has access to which tools.
- Reassess access during role changes or offboarding.



03

Encrypt Sensitive Data

WHAT IT IS: Securing data while utilizing AI platforms using encryption.

WHY IT MATTERS: Prevents exposure of confidential or client data when interacting with AI tools.

PUT IT INTO PRACTICE:

- Use platforms with built-in encryption for data in transit and at rest.
- Avoid entering sensitive information (e.g., PII, financials) into tools that don't meet your data standards.
- Understand how each AI vendor stores, protects, and deletes your data.



05

Train and Educate Your Teams

WHAT IT IS: Teaching your employees how to use AI tools responsibly and securely.

WHY IT MATTERS: Builds confidence and reduces risk of costly errors or misuse.

PUT IT INTO PRACTICE:

- Include AI usage training in onboarding.
- Offer regular refreshers as tools and policies evolve.
- Tailor training to specific roles and responsibilities.
- Share examples of good vs. poor prompt practices.



04

Monitor and Audit AI Use

WHAT IT IS: Keeping track of how AI tools are used, by whom, and for what purpose.

WHY IT MATTERS: Enables accountability, policy enforcement, and early detection of misuse.

PUT IT INTO PRACTICE:

- Enable logging and user activity tracking.
- Conduct periodic audits of usage.
- Create alerts or checks for high-risk behaviors.
- Document audit results for compliance purposes.



06

Vet and Manage Vendors Carefully

WHAT IT IS: Evaluating AI vendors for data security, privacy, and compliance.

WHY IT MATTERS: Ensures your tools meet your internal standards—and don't introduce risk.

PUT IT INTO PRACTICE:

- Review vendor certifications (SOC 2, ISO 27001, etc.).
- Ask if your data is stored, used for model training, or shared.
- Select vendors that allow you to retain control over your data.
- Keep a list of approved tools and who is using them.

If you need help creating your AI sales policy or selecting the right AI tools, contact us for guidance and additional resources.



**SALES
XCELERATION®**