AI Security Quick Reference Guide

Understanding Shadow AI Risks in Credit Unions

What is Shadow AI?

Shadow AI refers to the use of artificial intelligence tools and applications by employees without explicit organizational approval, oversight, or security controls. This includes personal use of consumer AI tools like ChatGPT, Claude, Gemini, and Copilot for work-related tasks.

Critical Statistics: The Scale of Shadow AI

Statistic	Source
38% of employees share sensitive work info with AI tools without employer knowledge	*CybSafe × NCA 2024*
50% of employees are Shadow AI users; 46% unwilling to stop even if banned	*Software AG 2024 (6,000 workers)*
71% of office workers use AI tools without IT approval	*2025 Enterprise Research*
485% increase in corporate data put into AI tools (Mar 2023-Mar 2024)	*Cyberhaven Labs*
46% of organizations experienced internal data leaks through generative AI	*Cisco 2025*
Financial services firms are **300x** more likely to be targeted by cyberattack	*IBM Security*

Red Flags: Signs of Shadow AI in Your Credit Union

- Employees copying large amounts of member data to clipboard
- Unusual network traffic to AI service domains (openai.com, anthropic.com, etc.)
- Staff productivity increases without clear explanation of new tools
- Documents or communications with AI-characteristic phrasing
- Browser extensions for AI assistants installed on workstations
- Requests to IT for access to AI tools or questions about AI policies
- Personal devices being used more frequently for work tasks

Member Data at Risk

When employees use unsanctioned AI tools, the following sensitive data may be exposed:

- **Personal Identifiable Information (PII):** Names, SSNs, dates of birth, addresses
- **Financial Data:** Account numbers, balances, transaction history
- **Authentication Credentials:** PINs, security questions, login information
- **Loan Information:** Credit scores, application details, income data
- **Internal Documents:** Policies, procedures, strategic plans
- **Communication Records:** Member correspondence, complaint details

Immediate Action Checklist

Take these steps within the next 30 days:

1. **Conduct an AI Usage Audit**
   - Deploy anonymous employee surveys about AI tool usage
   - Review network traffic logs for AI service domains
   - Inventory browser extensions across workstations
2. **Establish Interim Policies**
   - Communicate clear expectations about AI tool usage
   - Prohibit member data input into consumer AI tools
   - Require disclosure of AI tool usage in work products
3. **Implement Technical Controls**
   - Block or monitor access to consumer AI platforms
   - Deploy Data Loss Prevention (DLP) tools for AI traffic
   - Enable clipboard monitoring for sensitive data patterns
4. **Train Your Team**
   - Educate staff on risks of unauthorized AI usage
   - Provide approved alternatives for legitimate use cases
   - Establish reporting channels for AI-related concerns

⚠ CRITICAL REMINDER

NCUA reported 892 cyber incidents affecting credit unions (Sept 2023-May 2024). 73% involved third-party service providers, including AI vendors.

Questions? Contact your Information Security team immediately if you suspect unauthorized AI usage.