User Awareness Training Program

Synthetic Users

Version: 1.2

Effective Date: January 2025

Last Updated: January 2026

Document Owner: CTO — Artur Ventura

Review Frequency: Annually (every January)

Classification: Internal – Confidential

CRA Reference: 2.2.1

Change History

Version	Date	Author	Changes
1.1	January 2025	CTO / Security Lead	Initial release
1.2	January 2026	Artur Ventura, CTO	Added AI/GenAI Awareness module (Section 4a); confirmed quiz platform as Google Forms; updated last review date to January 2026. Per JPMC SCA CRA 2.2.1.

Objective

To educate and reinforce security awareness among all employees, ensuring they understand and adhere to best practices for data protection, compliance, and cybersecurity. This plan is tailored to meet the stringent requirements of our banking sector clients, including JPMC.

1. Kick-Off Meeting (January)

Audience: All employees

Purpose: Introduce the annual security awareness program, outline the importance of security in our industry, and explain the expectations for the year.

Content:

- Overview of the program
- Key security policies and procedures
- Importance of data protection and compliance, especially for banking clients
- Introduction to the year's AI/GenAI security focus topics

Format: All-hands meeting (virtual or in-person) with senior leadership and security officers

2. Monthly Security Focus Emails (February – November)

Audience: All employees

Purpose: Provide continuous education on specific security topics to keep security awareness top-of-mind.

Content schedule:

Month	Topic
February	Phishing and Social Engineering
March	Password Management and Multi-Factor Authentication (MFA)
April	Data Encryption and Secure Data Handling
May	Mobile Device Security and Remote Work Best Practices
June	Physical Security and Secure Workspace Guidelines
July	Data Privacy Regulations (GDPR, CCPA, JPMC contractual obligations)
August	Secure Software Development and Coding Practices
September	Incident Response Procedures
October	Insider Threat Awareness
November	Compliance and Audit Readiness

Format: Concise, engaging emails with links to further reading, videos, and quizzes

3. Quarterly Interactive Training Sessions (March, June, September, December)

Audience: All employees

Purpose: Engage employees in interactive, scenario-based training sessions that reinforce key security concepts.

Quarter	Month	Topic
Q1	March	Phishing Simulation and Response (with live phishing test)
Q2	June	Data Protection and Encryption Best Practices
Q3	September	Secure Remote Work and Device Management

Q4	December	Incident Reporting and Response Simulation

Format: Virtual or in-person workshops with interactive elements, including role-playing scenarios and group discussions

---

4. Annual Security Awareness Quiz (November)

Audience: All employees

Purpose: Assess employees' understanding of key security concepts covered throughout the year.

Content: Questions covering all monthly focus topics, interactive scenarios, and policy-specific questions.

Platform: Google Forms — delivered via company email with completion tracked by the Security Lead. Completion is mandatory for all employees. Results are reviewed by the CTO and retained for annual compliance reporting.

Completion tracking: Participation rate and individual results are recorded and retained as evidence of annual security training.

4a. AI/GenAI Security Awareness Module (Annual — Q2)

Audience: All employees, with additional depth for engineering, product, and customer-facing roles

Purpose: Ensure all employees understand the unique security risks associated with AI/GenAI systems and their responsibilities when interacting with or building AI-powered features.

Content:

- **Prompt injection awareness** — What prompt injection attacks are, how they target LLM-based systems, and how to recognize and report suspicious inputs
- **AI output handling** — Not treating AI-generated content as authoritative without verification; understanding hallucination risk
- **Data minimization in AI prompts** — Not including sensitive customer data, PII, or confidential information in prompts sent to external LLM providers
- **Model provider data boundaries** — Understanding which data leaves Synthetic Users' infrastructure when using third-party LLM APIs and what protections are in place
- **Reporting AI/GenAI incidents** — How to report unexpected model behavior, data exposure concerns, or suspected misuse via the standard incident reporting process

Format: Asynchronous self-paced module with a 5-question comprehension check; facilitated by the CTO. Completion tracked in Google Forms alongside the November quiz.

---

5. Specialized Training for High-Risk Roles (Ongoing)

Audience: Employees in roles with elevated security responsibilities (IT, DevOps, HR, Finance, AI/ML engineering)

Purpose: Provide deeper, role-specific training to those handling sensitive data or systems.

Content:

- Advanced threat detection and response
- Secure coding practices and code reviews
- Handling of sensitive customer data
- Compliance with banking sector-specific regulations
- AI/GenAI model security and adversarial testing (for engineering roles)

Format: Instructor-led training

---

6. Security Awareness Week (October)

Audience: All employees

Purpose: Intensify focus on security awareness through a series of events, coinciding with National Cybersecurity Awareness Month.

Content:

- Daily webinars on various security topics
- Interactive challenges (capture the flag, security puzzles)
- Rewards and recognition for top performers in security challenges

Format: In-person or virtual events

7. Policy Acknowledgment and Refresher Training (December)

Audience: All employees

Purpose: Ensure all employees are up-to-date on company security policies and have acknowledged their understanding.

Content:

- Review of updated security policies and procedures
- Mandatory refresher training on key policies (acceptable use, data handling)
- Digital acknowledgment form to be signed by all employees

Format: In-person or virtual events with digital acknowledgment via Google Forms

8. Program Evaluation and Feedback (December)

Audience: All employees and management

Purpose: Evaluate the effectiveness of the security awareness program and gather feedback for improvement.

Content:

- Anonymous employee surveys
- Review of quiz and training participation data
- Feedback session with management and key stakeholders

Format: Online surveys (Google Forms), data analysis, and roundtable discussion

9. Related Documents

- Incident Response Plan — Incident reporting procedures covered in training
- SDLC AI/GenAI Addendum — AI/GenAI security practices referenced in Module 4a
- Third-Party Risk Management Policy — LLM provider data handling
- Employee Code of Conduct — Baseline security obligations for all employees