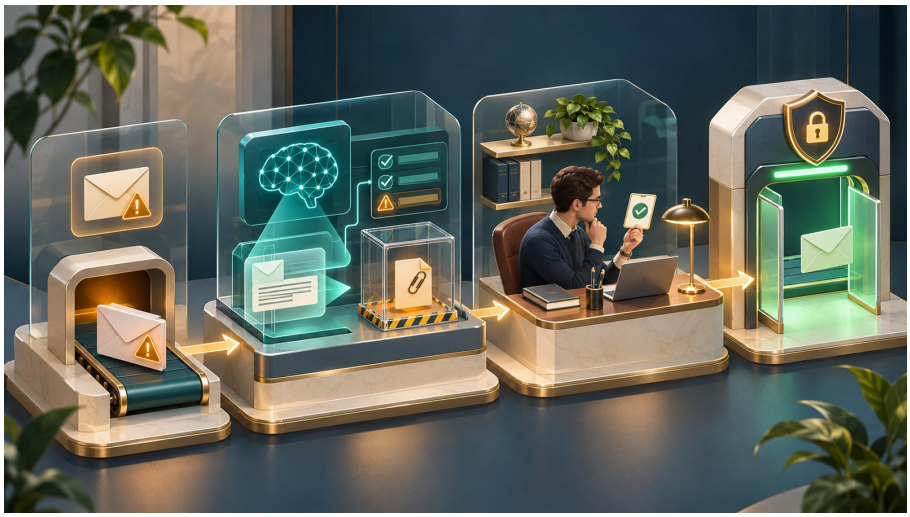
AIT TECHNOLOGY | BUSINESS IMPLEMENTATION SERIES

Forms and procedure records

Using AI in cybersecurity: a controlled operating manual



AI-generated editorial illustration; fictional people and systems.

Tailored to your business

AIT Technology can customise these procedures and build bespoke software, AI workflows and integrations. Scope, testing, pricing and support are agreed before implementation.

Version 1.0 | 18 November 2026 | UK business context

Starting framework: approve company-specific scope and owners before adoption. No certification, guaranteed compliance or emergency response service is implied.

FORM 01 | AI-assisted suspicious-email triage

Owner: Security analyst | Start: Reported suspicious message.

Use with the matching manual procedure. Save locally in an approved location. Do not enter passwords, API keys or recovery codes. Refer to restricted evidence rather than pasting sensitive data.

Company / case reference

Owner / deputy / date and time zone

Scope / trigger / affected systems or workflow

Verified facts / evidence references / uncertainties

Actions / results / timestamps (reference extra pages if needed)

Approval / authority / reporting decision and reasons

Completion checks / handoff / outstanding risks

Next action / responsible person / deadline / review date

Status (record explicitly): Open / Paused / Awaiting approval / Completed

FORM 02 | AI-assisted alert correlation

Owner: Security operations lead | Start: Multiple related security alerts.

Use with the matching manual procedure. Save locally in an approved location. Do not enter passwords, API keys or recovery codes. Refer to restricted evidence rather than pasting sensitive data.

Company / case reference

Owner / deputy / date and time zone

Scope / trigger / affected systems or workflow

Verified facts / evidence references / uncertainties

Actions / results / timestamps (reference extra pages if needed)

Approval / authority / reporting decision and reasons

Completion checks / handoff / outstanding risks

Next action / responsible person / deadline / review date

Status (record explicitly): Open / Paused / Awaiting approval / Completed

FORM 03 | Approve a response action

Owner: Authorised incident lead + business owner where needed | Start: AI suggests account/device/network containment.

Use with the matching manual procedure. Save locally in an approved location. Do not enter passwords, API keys or recovery codes. Refer to restricted evidence rather than pasting sensitive data.

Company / case reference

Owner / deputy / date and time zone

Scope / trigger / affected systems or workflow

Verified facts / evidence references / uncertainties

Actions / results / timestamps (reference extra pages if needed)

Approval / authority / reporting decision and reasons

Completion checks / handoff / outstanding risks

Next action / responsible person / deadline / review date

Status (record explicitly): Open / Paused / Awaiting approval / Completed

FORM 04 | Prompt-injection attempt

Owner: Security lead + AI service owner | Start: Evidence tries to redirect instructions, reveal secrets or invoke tools.

Use with the matching manual procedure. Save locally in an approved location. Do not enter passwords, API keys or recovery codes. Refer to restricted evidence rather than pasting sensitive data.

Company / case reference

Owner / deputy / date and time zone

Scope / trigger / affected systems or workflow

Verified facts / evidence references / uncertainties

Actions / results / timestamps (reference extra pages if needed)

Approval / authority / reporting decision and reasons

Completion checks / handoff / outstanding risks

Next action / responsible person / deadline / review date

Status (record explicitly): Open / Paused / Awaiting approval / Completed

FORM 05 | Incorrect AI incident summary

Owner: Incident lead | Start: Summary invents facts, omits impact or assigns blame.

Use with the matching manual procedure. Save locally in an approved location. Do not enter passwords, API keys or recovery codes. Refer to restricted evidence rather than pasting sensitive data.

Company / case reference

Owner / deputy / date and time zone

Scope / trigger / affected systems or workflow

Verified facts / evidence references / uncertainties

Actions / results / timestamps (reference extra pages if needed)

Approval / authority / reporting decision and reasons

Completion checks / handoff / outstanding risks

Next action / responsible person / deadline / review date

Status (record explicitly): Open / Paused / Awaiting approval / Completed

FORM 06 | Disable the AI component safely

Owner: AI/security service owner | Start: Boundary failure, unexpected spend, unsafe behaviour or provider outage.

Use with the matching manual procedure. Save locally in an approved location. Do not enter passwords, API keys or recovery codes. Refer to restricted evidence rather than pasting sensitive data.

Company / case reference

Owner / deputy / date and time zone

Scope / trigger / affected systems or workflow

Verified facts / evidence references / uncertainties

Actions / results / timestamps (reference extra pages if needed)

Approval / authority / reporting decision and reasons

Completion checks / handoff / outstanding risks

Next action / responsible person / deadline / review date

Status (record explicitly): Open / Paused / Awaiting approval / Completed