eGoldHub

USE CASE

Achieving 100% Read and Accept Rates for Cybersecurity Policies

AT A GLANCE

Challenges

- No centralized method to distribute cybersecurity policies
- Lack of acknowledgement tracking for audits
- Manual tracking was inconsistent and incomplete

Benefits

- Automated reminders for outstanding acknowledgements
- Centralized dashboard showing distribution and acknowledgement status
- Clear reporting to support audit readiness

CHALLENGES

A mid-sized financial services firm faced growing cybersecurity pressures. Every year, auditors requested proof that employees had reviewed and accepted updated security policies—acceptable use, password standards, phishing procedures, encryption rules, and more.

But IT had no centralized method to distribute or track acceptance. Some policies were emailed, others posted on internal drives, and acknowledgment was sporadic at best. During a SOC 2 audit, gaps in policy acknowledgement records were identified.

SOLUTIONS

With eGoldHub, cybersecurity policies and related trainings are centrally distributed and tracked.

Policies and trainings are assigned by group, and acknowledgements are required.

Administrators can see who has received content, who has acknowledged it, and who remains outstanding.

Automated reminder emails are sent for incomplete acknowledgements, reducing manual follow-up and improving audit readiness.

BENEFITS

Benefit One
Improves visibility into required policy distribution and acknowledgement.

Benefit Two
Simplifies SOC 2, ISO 27001, and other regulatory audits.

Benefit Three
Reduces administrative workload by eliminating manual tracking.

INDUSTRIES MOST AFFECTED

Financial services & fintech

Healthcare & medical systems

Government & public sector

SaaS & technology

Manufacturing & critical infrastructure

Education & research institutions

A-LIGN
ISO 27001
CERTIFIED