

SAMPLE

Incident Disclosure Readiness Kit

The opening of reporting-obligations-by-regime.docx, one of 28 files in the kit.

<https://solasai.net/products/incident-disclosure-kit/>

Solas AI | Incident Disclosure Readiness Kit solasai.net

Reporting Obligations by Regime

This template does not constitute legal advice. Consult qualified counsel for compliance decisions.

Purpose

This document is your single reference for incident reporting obligations across every major regulatory framework. When an incident occurs, use this to immediately identify who you must notify, when, what to include, and what happens if you miss the deadline.

Keep this document current. Regulations change. Review annually and after any regulatory update.

Quick-Reference Comparison Table

Framework	Who Must Report	Report To	Timeline	Key Trigger
SEC (8-K)	Public companies	SEC (EDGAR)	4 business days from materiality determination	Material cybersecurity incident
NIS2	Essential and important entities (EU)	National CSIRT / competent authority	24hr / 72hr / 30 days	Significant incident affecting service delivery
DORA	Financial entities (EU)	Competent authority (via ESA templates)	4hr / 72hr / 1 month	Major ICT-related incident
HIPAA	Covered entities and BAs	HHS OCR, individuals, media (if 500+)	60 days (individuals), annual (HHS <500)	Breach of unsecured PHI
GDPR	Data controllers	Supervisory authority	72 hours	Personal data breach likely to result in risk
CA (CCPA/CPRA)	Businesses with CA residents' data	CA AG, affected individuals	"Most expedient time possible"	Breach of unencrypted personal information

Framework	Who Must Report	Report To	Timeline	Key Trigger
NY (SHIELD Act)	Businesses with NY residents' data	NY AG, affected individuals	"Most expedient time possible"	Breach of private information
TX (TDPSA)	Businesses with TX residents' data	TX AG (if 250+), affected individuals	60 days	Breach of sensitive personal information
FL (FIPA)	Businesses with FL residents' data	FL Dept. of Legal Affairs (if 500+), individuals	30 days	Breach of personal information
IL (PIPA)	Businesses with IL residents' data	IL AG, affected individuals	"Most expedient time possible"	Breach of personal information
PCI DSS	Merchants and service providers	Acquiring bank, card brands	Immediately upon discovery	Compromise of cardholder data
GLBA	Financial institutions	Primary federal regulator, FTC	"As soon as possible" (within 36 hrs for FTC Safeguards)	Security event affecting customer information
CIRCI	Critical infrastructure entities	CISA	72 hours (incidents) / 24 hours (ransom payments)	Covered cyber incident or ransom payment
DFARS 252.204-7012	DoD contractors handling CUI	DoD via DIBNet	72 hours	Cyber incident affecting covered contractor information systems

SEC — Form 8-K (Item 1.05)

Applicability

All public companies registered with the SEC (domestic registrants). Foreign private issuers report on Form 6-K.

Who Must Report

The registrant (public company) itself. The obligation rests with the company, not individual officers, though officers sign the filing.

Report To

- SEC via EDGAR filing system
- Item 1.05 of Form 8-K

Timeline

- **4 business days** from the date the registrant **determines** the incident is material
- The SEC has stated companies may not unreasonably delay the materiality determination to avoid the disclosure deadline
- A registrant may delay filing if the U.S. Attorney General determines disclosure poses a substantial risk to national security or public safety (requires written notification to SEC)

Required Content

- ☐ Nature and scope of the incident
- ☐ Date of discovery and whether the incident is ongoing
- ☐ Whether any data was stolen, altered, accessed, or used for any unauthorized purpose
- ☐ Effect of the incident on the registrant's operations
- ☐ Whether the registrant has remediated or is currently remediating the incident
- ☐ Material impact or reasonably likely material impact on financial condition and results of operations

What NOT to Include (per SEC guidance)

- Specific technical details about the incident response
- Information about planned remediation that could reveal vulnerability information
- Details that would impede an ongoing law enforcement investigation

Penalties for Non-Compliance

- SEC enforcement action
- Civil penalties
- Securities fraud claims from investors
- Shareholder derivative lawsuits
- Reputational damage from late/inadequate disclosure

Common Mistakes

- Delaying materiality determination to buy time
- Providing boilerplate language instead of incident-specific information
- Failing to update the 8-K as material new information emerges (use 8-K/A)
- Disclosing too much technical detail or too little business impact
- Not coordinating disclosure timing with law enforcement

NIS2 Directive (EU)

Applicability

Essential entities (energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, space) and important entities (postal services, waste management, chemicals, food, manufacturing, digital providers, research).

The sample ends here. The full document runs about 3,804 words; the kit holds 28 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/incident-disclosure-kit/>, 14-day refund for any reason.