Using the template in Europe or the United States

The template is written for UK law and the UK Cyber Essentials scheme. To use it in the EU or the United States, check the things below. Financial firms, healthcare, makers of digital products and some other organisations have extra rules, listed under special cases.

European Union	What to change	Who to ask
Scope, Regulatory check	NIS2. Check whether the EU cyber security rules (NIS2) apply to you through your country's law. As a rule they cover medium-sized and large organisations in listed sectors, and some others whatever their size.	Your national cyber security authority
Reporting incidents and breaches	Deadlines. Under NIS2, a significant incident needs an early warning without undue delay and within 24 hours of becoming aware of it, a fuller notice within 72 hours and a final report within a month of that notice. Personal data breaches go to your data protection authority without undue delay and, where feasible, within 72 hours of becoming aware of them, unless unlikely to put people at risk, as in the UK.	Your national CSIRT and your data protection authority
Assessing risk, Testing, monitoring and review	Personal data. The EU GDPR asks for the same security as the UK GDPR. Change the references.	Your data protection authority
Reporting incidents, Acceptable use	UK names. Replace the Information Commission and Report Fraud with your data protection authority, your national CSIRT and the police. The offences in section 13 and Cyber Essentials are UK only.	Your legal advisers
Special cases	Banks, insurers and other financial firms have their own ICT rules (DORA). Makers of connected devices and software sold in the EU should check the Cyber Resilience Act, which applies in stages from 11 September 2026.	Your legal or regulatory advisers

United States	What to change	Who to ask
Scope, Regulatory check	Which rules apply. Check the federal and state rules for your sector and your data, including states whose residents' data you hold. Some states, such as New York, require reasonable security safeguards. The FTC can act where a business misleads people about its security.	Your legal advisers
Reporting incidents and breaches	Breach notices. Every state has its own law on telling people about breaches of personal information. Check the ones that apply to you.	Your legal advisers
Reporting incidents, Who is responsible	Public companies. If you file Form 8-K with the SEC, a cyber incident you decide is material is generally disclosed within four business days of that decision.	Your securities lawyers
Reporting incidents and breaches	UK names. Replace the UK bodies with your own contacts. You can report cyber incidents to CISA and cyber crime to the FBI. The offences in section 13 and Cyber Essentials are UK only.	CISA, the FBI and your legal advisers
Special cases	Financial firms (the FTC Safeguards Rule; banks tell their regulator of certain incidents as soon as possible, within 36 hours of deciding they qualify), healthcare (the HIPAA Security Rule), federal contractors and critical infrastructure (check the status of CIRCIA) have rules of their own.	Your legal or regulatory advisers

Sources: the statements above were taken from official pages read on 4 October 2026. The pages are listed at policysight.com/templates/information-security. Version 1.0, next review April 2027.

This guide is a starting point, not legal or regulatory advice, and PolicySight Ltd is not a law firm. It is a list of things to check. It is not complete and law changes. Have your own advisers confirm what applies to you before you rely on it.