SherpaTech
INSURANCE SPECIALISTS FOR TECH & IT

DATA BREACH CHECKLIST

Our Data Breach Checklist has been created as a framework in the event of a Cyber Incident. We encourage you to fill out your key contacts and distribute these to your staff. So in the case of a cyber incident, they know how to escalate and who to alert. This checklist has been created as a guide and may need to be amended to best suit your organisation. Other documents may also need to be created in support of the actions below.

Please fill out the following information below:

KEY CONTACTS	NAME	EMAIL	PHONE NO.
IT Service Provider	_____	_____	_____
Insurer 24/7 Response Team	_____	_____	_____
Insurance Broker	_____	_____	_____
Chief Technology Officer / Head of IT	_____	_____	_____
Chief Risk Officer / Head of Compliance	_____	_____	_____

Note: an eligible data breach occurs when the following criteria are met:

- There is unauthorised access to, or disclosure of, personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.

The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.

Source: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme

1. CONFIRM BREACH	INFORMATION OR LINK	COMPLETED
List the date, time, duration, and location of the breach		Y N N/A
The type of personal information involved in the breach		Y N N/A
How the breach was discovered and by whom		Y N N/A
List the suspected cause and extent of the breach		Y N N/A
Make a list of the affected individuals, or possible affected individuals		Y N N/A
Identify if there is risk of serious harm to the affected individuals		Y N N/A
List the risk of other harms		Y N N/A

2. CONTAIN BREACH	INFORMATION OR LINK	COMPLETED
To prevent further damage where possible		Y N N/A

3. INFORM YOUR BROKER & INSURER	INFORMATION OR LINK	COMPLETED
Note that Data Breach teams operate 24/7, are funded by the insurer and are aligned to advise and reduce exposure and cost.		Y N N/A

4. IDENTIFY OBLIGATIONS	INFORMATION OR LINK	COMPLETED
To your Customers, Stakeholders & Suppliers		Y N N/A
To the regulators (local and offshore e.g., GDPR). Regarding the local regulator, consider, does the breach or suspected breach indicate a systemic problem in Office of Australian Information Commissioner (OAIC) processes or procedures?		Y N N/A

Consider, could there be media or stakeholder attention as a result of the breach or suspected breach?		Y N N/A
Consider the Australian Cyber Security Centre (ACSC), police/law enforcement, or other agencies or organisations that may be affected by the breach, or can assist in containing the breach, or can assist individuals affected by breach, or where the OAIC is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.		Y N N/A

5. BUILD AN ACTION PLAN & EXECUTE	INFORMATION OR LINK	COMPLETED
Including actions, resourcing, timing, and oversight		Y N N/A
Project execution		Y N N/A
Consider ownership at the highest level of the organisation		Y N N/A
Consider bringing in specialists as needed.		Y N N/A

6. PREVENT FURTHER BREACHES	INFORMATION OR LINK	COMPLETED
Finalising the cause of the breach		Y N N/A
Implementing a strategy to identify and address any weaknesses in data handling		Y N N/A
Updating data breach response plan if necessary		Y N N/A
Making appropriate changes to policies and procedures		Y N N/A
Revising staff training practices if necessary		Y N N/A
Considering an audit to ensure necessary outcomes are brought into effect		Y N N/A
Preserving evidence to determine the cause of the breach or allowing the OAIC to take corrective action		Y N N/A