Australian Business Lawyers & Advisors

Cyber Security Checklist

For Australian businesses, the potential reputational and financial risks associated with cyber security and data breach incidents are serious and very real. Regulators are closely monitoring data protection and privacy law compliance on a global basis, and so are tech-savvy customers. Protecting your business and preventing loss of valuable data such as your intellectual property, confidential information and customer data is critical. Cyber security is no longer just an IT issue, but must be proactively managed by organisations and their boards across all areas of their business.

How would your business stack up if you were facing a cyber security threat or under scrutiny by regulators?

Complete this checklist to see if your business is prepared.

Cyber Security and Data Privacy Audits

- ☐ Have you recently conducted a cyber security and data privacy audit?
- ☐ Do you know exactly how and when you collect data, the types of data you collect, current and proposed uses, location of data (electronic and hard copy), who has access to data, whether you transfer data overseas (including to third party service providers or hosts)?
- ☐ Have you reviewed your IT systems from a cyber security and organisational privacy by design perspective to ensure they are compliant with applicable laws and consistent with company policies?

Tip: If your last cyber security or data privacy Audit was pre-2018, you should consider completing another audit or takes steps to update existing systems, policies and procedures to ensure compliance with new notifiable data breach laws and the GDPR. If your business has never done a focused data privacy and cyber security Audit, we highly recommend you do so to ensure you identify critical gaps in compliance and practical steps for rectification to protect your business and minimise unnecessary risk.

Privacy Policy

- ☐ Do you have an up-to-date, compliant privacy policy?
- ☐ Does your privacy policy cover the list of compulsory items set out in the Australian Privacy Principles?
- ☐ Has your business recently changed its products, services, systems, processes, structure or otherwise evolved and grown?
- ☐ If yes, have you checked your privacy policy to ensure it accurately covers all current purposes and necessary consents for any new uses of data collected for the purpose of providing products or other services?

Tip: You should regularly review your privacy policy to ensure you comply with the requirements under the Privacy Act's Australian Privacy Principles (APPs) to have an up-to-date, compliant policy that covers the mandatory APP items and accurately reflects your business's collection and treatment or uses of customer data.

Data Breach Response Plan

- ☐ Do you have a Data Breach Response Plan?
- ☐ Does your board and staff know what to do to meet mandatory reporting and other legal obligations in the event of a cyber security or data breach incident?
- ☐ Do you regularly test your Data Breach Response Plan?
- ☐ Have you run a hypothetical "breach" scenario to check staff knowledge and compliance?
- ☐ Do you have technical and legal experts readily available to respond and advise in the event of a breach?

Tip: *It is critical to have a Data Breach Response Plan in place so you know what to do in the likely event your organisation suffers a cyber security or data breach incident, and can assess and respond quickly, including notification of regulators (if necessary).*

Education & Training

- ☐ Do you have effective cyber security and data privacy training across all levels in your organisation?
- ☐ Do you include cyber security and data privacy modules in your new staff inductions?
- ☐ Do all staff know who within the organisation to contact in the event of a suspected cyber security or data breach incident?

Tip: *Your staff deal with valuable and sensitive personal data every day, and with human error one of the most common causes of data breaches and cyber security incidents, comprehensive organisational training is the best way to minimise your privacy compliance and cyber security risks.*

Cyber Security Technology Review

- ☐ Has your IT team or IT service providers recently reviewed whether your IT systems and devices, including data servers, cloud storage and other hosting services have up-to-date technical and physical security against threats, including appropriate anti-virus software?
- ☐ Are all computers protected by a properly configured firewall?
- ☐ Do you have policies in place to ensure safe and proper use of internet and email?
- ☐ Are staff prevented from installing software without prior approval?
- ☐ Do wireless networks have appropriate encryption?
- ☐ Do you have controls in place to ensure authorised access only (e.g. individual logins and two factor authentications)?
- ☐ Do you have sufficient password obligations and strength levels?

Tip: *Talk to your IT team or IT service providers and make sure someone with appropriate expertise can confidently answer these questions.*

Business Critical Digital Assets

- ☐ Do you know what data and IT systems your business needs to keep operating in the event of a malicious cyber security breach?
- ☐ Do you know where your business critical information and data is located (e.g. on internal computer systems, Australian based data centres, international data centres or cloud based servers)?
- ☐ Do you know who has access to it?
- ☐ Do you understand the risks associated with data held by your third party suppliers, and whether their security measures (and their contractual obligations) are adequate?
- ☐ What backup measures and disaster recovery plans do you have in place?

Tip: *Many businesses are heavily reliant on data and digital assets, which means a cyber attack can be crippling. Make sure you are across where your data is located and have backup measures and have business continuity plans in place.*

GDPR

- ☐ If your business is online or international, have you considered if the GDPR applies to your business?
- ☐ If so, does your privacy policy comply with the stricter requirements under the GDPR?
- ☐ Do you have systems and processes in place to ensure your business can implement the additional GDPR obligations?

Tip: *Given the high penalties and international reach under the GDPR, it is worth seeking advice on whether the GDPR applies to your business and how your compliance stacks up. The GDPR obligations are much stricter than Australian privacy laws and require businesses to take additional steps to protect consumer data rights and control over their data.*

Overseas transfers and IT service agreements

- ☐ Have you reviewed your IT service provider contracts?
- ☐ Do you know if all data is stored locally or transferred overseas to cloud or third party data centres?
- ☐ Do your third party providers have obligations to promptly assist you with any investigation into a potential cyber security or data breach incident?
- ☐ Do you have appropriate indemnities and obligations to comply with Australian privacy laws and standards included in those contracts?
- ☐ Are your service providers required to cooperate and assist you with data breach notifications, including where the data breach is their fault?
- ☐ When the cause is unclear, who is obliged to prepare and submit any notification?
- ☐ Do your contracts align with your data breach response plan and privacy policy?

Tip: *Under the Australian Privacy Act, organisations remain responsible for data privacy breaches by overseas contractors and service providers. Make sure your contracts with IT service providers, hosting services and data centres have appropriate privacy law compliance and data breach obligations and that you understand where your service providers transfer and store your data.*

Data retention, de-identification and destruction

- ☐ Does your organisation have a comprehensive data retention, de-identification and destruction policy (both for hard copy and electronic data)?
- ☐ Do you know what data retention laws apply to your business?
- ☐ How does your organisation and IT systems address data retention periods, de-identification or destruction of data after retention periods expire, and any overlapping data retention laws and other legal obligations to retain data for lawful purposes?

Tip: *There may be multiple applicable regulatory regimes depending upon your business, industry, sector, professional obligations and permitted purposes under your privacy policy, including some which may overlap. Insufficient data retention, destruction or de-identification practices put your business at a higher risk in the event of a data breach, as there is often more data held than is permitted to be retained, which the regulator has frowned upon recently.*

Board Oversight

- ☐ How does your organisation report cyber security and data breach incidents to the Board, if at all?
- ☐ Is there sufficient funding for cyber security and data privacy compliance measures?
- ☐ With human error the most common cause of cyber security and data breach incidents, are staff encouraged to disclose cyber security and data breach incidents to management and the board as part of the organisation's culture?
- ☐ Does the board often discuss cyber security trends and management of customer data?
- ☐ Do you consider cyber risks and data privacy as part of your strategic planning process?
- ☐ Have you considered cyber insurance as part of your cyber and data risk management strategy?
- ☐ Alternatively, have you reviewed your business insurance to check if you're already covered (and if so, for what exactly)?

Tip: *Cyber security and data privacy compliance should be firmly on your board's agenda. Resource allocation and effective use of risk committees (and expert advice where required), can better position your organisation in the likely event of a cyber security or data breach incident, both in the eyes of the regulator and most importantly, your customers.*

If there have been any boxes in this checklist which you could not confidently tick, your business should act swiftly to address any gaps.

ABLA can assist you with a range of cyber security and data privacy legal services, including:

- Cyber security, data protection and privacy audits
- Advice on eligible data breaches and cyber security incidents
- Data breach response plans
- Privacy policies
- Data retention, de-identification and destruction policies
- IT contracting

Get in contact with our team of cyber security and data privacy legal experts for a confidential discussion today. With a range of fixed fee services and exceptional value hourly rates, Australian Business Lawyers & Advisors can help your business feel more confident.

dataprotection@ablawyers.com.au

1300 565 846

ablawyers.com.au