

Bermuda PIPA Checklist

18 checks to help your business handle personal information with care and confidence.

ORGANISATION

REVIEWED BY

DATE

A Lead & communicate

- **01 Give privacy a clear owner**
Name a privacy officer, publish contact details and keep your privacy programme active.
- **02 Build an information inventory**
Record the personal information you use, its purpose, storage locations and recipients.
- **03 Confirm the basis for each use**
Document the applicable PIPA condition and secure consent when it is required.
- **04 Tell people what to expect**
Make privacy notices clear about uses, disclosures, rights and how to contact you.
- **05 Make rights requests manageable**
Manage access, correction, blocking and erasure requests within applicable deadlines and exceptions.

B Handle information responsibly

- **06 Keep collection and use focused**
Collect what you need, use it fairly and stay within permitted purposes.
- **07 Check the quality of your records**
Keep records accurate and current enough for their intended use.
- **08 Set a defensible retention schedule**
Set retention periods, honour legal requirements and securely dispose of unneeded records.
- **09 Handle higher-risk information**
Apply relevant rules for sensitive information and for children, including online services.

C Secure day-to-day operations

- **10 Match safeguards to the risk**
Choose controls to match sensitivity, context and the likelihood and severity of harm.
- **11 Limit who can get in**
Use named accounts, minimum permissions and appropriate multifactor authentication.
- **12 Maintain secure systems**
Patch systems, use secure settings and maintain endpoint protection.
- **13 Protect every stage of handling**
Secure stored, shared and transmitted information, and its disposal. Include paper records.
- **14 Practise safe information handling**
Train staff in safe handling, threat awareness and prompt incident reporting.

D Plan, respond & improve

- **15 Review suppliers and transfers**
Assess suppliers and overseas recipients; ensure transfers meet PIPA protection requirements.
- **16 Prove that recovery works**
Keep protected backups and test that essential information can be restored.
- **17 Prepare for breach notifications**
If a breach is likely to adversely affect someone, notify the Commissioner, then affected individuals, without undue delay.
- **18 Review controls and record progress**
Reassess safeguards regularly. Record decisions, testing and improvements.

Using this checklist: Treat it as a starting point for your privacy programme, not proof of compliance. Controls such as MFA, patching and restore tests are practical ways to manage risk; PIPA does not prescribe these technologies individually.

Reference: Bermuda Personal Information Protection Act 2016 and PrivCom guidance.
Explore the official guidance: privacy.bm/guide-to-pipa