SAMPLE FRAMEWORK FOR DATA BREACH PREPAREDNESS AND RESPONSE

DATA BREACH POLICY

Management Overview

At 1300 InTech, we recognise that the risk of data breaches—whether through cyberattacks, accidental disclosures, or system vulnerabilities—poses significant operational, financial, and reputational threats to our clients and their business. This Data Breach Policy Guide outlines a comprehensive, proactive, and systematic approach to preventing, detecting, managing, and recovering from data breach incidents.

This policy serves to:

- Protect sensitive client and company data.
- Ensure compliance with relevant legal obligations (e.g., Australian Privacy Act, Notifiable Data Breaches Scheme)
- Support staff and client trust through transparent, prompt, and professional incident response.
- Maintain ongoing cyber hygiene and organisational readiness.

This document lays out a simple six-step framework, plus Additional Recommendations, a useful Data Breach Response Checklist and a handy Data Breach Response Handout for Staff, Contractors and Client teams. We recommend regular reviews (quarterly) and, of course, after any major incident.

If you don't have a plan, and you don't know where to start, this is the document for you.

1. Prepare

1.1 Create Incident Response Plan (IRP)

- Maintain a documented IRP that outlines specific steps for detecting, containing, investigating, and resolving security incidents.
- Assign clear responsibilities and escalation paths, including an incident response team and data breach response lead.

1.2 Classify Data and Inventory

- Maintain a centralised and regularly updated inventory of all sensitive, personal, financial, and business-critical data.
- Classify data by sensitivity to ensure appropriate protections are in place.

In 2024, Australia saw a significant increase in data breaches, with **1,113 incidents** reported to the Office of the Australian Information Commissioner (OAIC).

1.3 Establish Identity and Access Controls

- Enforce Multi-Factor Authentication (2FA) for all systems and accounts.
- Use enterprise-grade Password Management Software.
- Implement Least Privilege Access Controls: Users only access data necessary for their role.

1.4 Begin Logging & Monitoring

- Enable detailed system and user activity logging across endpoints, servers, and cloud services.
- Retain logs for a minimum of 12 months to support forensic investigations.

1.5 Start Staff Training & Awareness

- Deploy iSAT Security Awareness Training regularly for all staff, especially those with email and data access.
- Test awareness via simulated phishing and other social engineering exercises.

2. Strengthen Security Stack

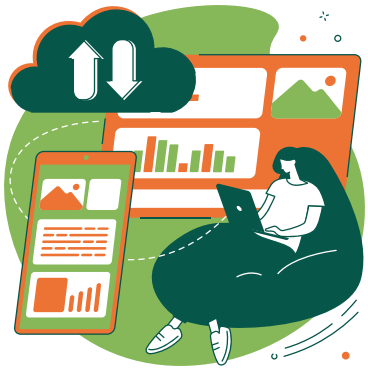
2.1 Endpoint and Identity Protection

- Deploy Detection Protection for all Users and Endpoints, incorporating:

  - ITDR (Identity Threat Detection & Response)
  - EDR (Endpoint Detection & Response)
  - SIEM (Security Information & Event Management)

2.2 Backup and Disaster Recovery

- Establish managed, encrypted, off-site backups of all critical data and systems.
- Test backup recovery quarterly.
- Document and verify backup integrity using checksums or hash verification.



2.3 Policy Management

- Use a Policy Management System to distribute, track, and enforce policies.
- Ensure all new hires are onboarded with relevant IT and security policies from day one.
- Implement version control policies and maintain an audit trail of employee acknowledgments.

3. Detect and Contain

3.1 Threat Detection

- Utilise SIEM tools and real-time threat intelligence feeds to detect anomalies.
- Establish alert thresholds for unusual data access, login locations, and failed access attempts.

3.2 Containment Procedures

- Immediately isolate compromised systems from the network.
- Disable affected user accounts and change relevant credentials.

3.3 Evidence Preservation

- Secure logs, memory dumps, and disk images.
- Avoid rebooting or altering affected systems until a forensic snapshot is taken.

4. Notify

4.1 Internal Escalation

- Immediately report incidents to the IT Manager and the 1300 InTech Incident Response Team.

4.2 Legal and Regulatory Compliance

- Assess the breach under the Privacy Act 1988 (C'wth) and the Notifiable Data Breaches (NDB) Scheme to determine if reporting is mandatory.
- Notify the Office of the Australian Information Commissioner (OAIC) within 72 hours if applicable.

A 2023 Mastercard study found that **33% of small businesses** affected by cyberattacks suffered **financial losses** as a result.

4.3 External Stakeholder Communication

- Prepare coordinated and approved communication for:

  - Affected individuals
  - Clients and partners
  - Media (if necessary)

4.4 Public Messaging

- Ensure messaging is transparent, timely, and does not speculate.
- Provide a dedicated point of contact for breach-related enquiries.

Australia recorded **47 million data breaches in 2024**, making it the 11th most affected country globally, according to cybersecurity firm Surfshark.

5. Remediate

5.1 Fix Identified Vulnerabilities

- Apply software patches or firmware updates.
- Reset passwords and enforce new security controls if needed.
- Review and update firewall and network security rules.

5.2 Investigate and Audit

- Assess the breach under the Privacy Act 1988 (C'wth) and the Notifiable Data Breaches (NDB) Scheme to determine if reporting is mandatory.
- Notify the Office of the Australian Information Commissioner (OAIC) within 72 hours if applicable.

According to the IBM Data Breach Report In 2024, the cost of data breaches has grown significantly, with the average breach now costing $4.88 million—up 10% from 2023.

5.3 Post-Incident Report

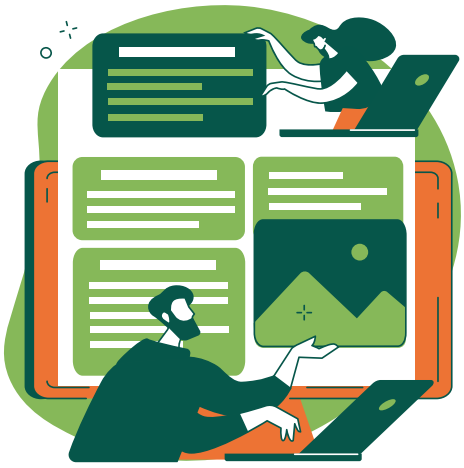
- Conduct a formal incident debrief.
- Update the Incident Response Plan and security stack based on lessons learned.

5.4 Continuous Monitoring

- Increase monitoring of affected systems and users.
- Watch for follow-up attacks, identity theft, or fraud attempts

The Australian Cyber Security Centre (ACSC) receives **cybercrime reports** on average every **6 minutes**.

6. Document



Maintain a full incident register including:

- Timeline of events (discovery to closure)
- Actions taken by each team/individual
- Evidence collected
- Communications with stakeholders
- Regulatory filings and legal consultations
- Final root cause analysis and remediation steps

According to the Australian Cyber Security Centre (ACSC), **over 87,400 cybercrime reports** were received during the 2023–24 financial year.

7. Other Recommendations

7.1 Data Loss Prevention (DLP)

- Deploy DLP tools to monitor, detect, and block unauthorised data transfers.

7.2 Device Encryption

- Enforce full-disk encryption on all devices and remote workstations.

7.3 Vendor and Third-party Risk

- Require vendors to adhere to minimum security standards and notify of breaches.
- Maintain up-to-date third-party risk assessments.

7.4 Cyber Insurance

- Review and maintain appropriate cyber insurance coverage.

7.5 Annual Penetration Testing

- Conduct external pen testing at least once a year and after major system changes.

According to Statista, in 2024, approximately **48%** of all data breach incidents worldwide involved the compromise of **customers' personally identifiable information (PII)**, making it the most frequently breached data type.

8. Review and Maintenance

- This policy shall be reviewed annually or after any security incident.
- Updates must be approved by senior management and communicated to all employees

According to the Australian Cyber Security Centre (ACSC), **62% of small businesses** have encountered a **cyber security incident**.

Breach Checklist

Data Breach Response Checklist

Use this when a potential breach occurs:

Initial Actions

- I've disconnected affected systems or accounts.
- I've secured or recovered any exposed data.
- I've notified IT/security team or manager.

Assessment

- Type of data involved (personal, financial, health, etc.)
- Who accessed the data (internal, external, unknown)?
- Risk of serious harm (identity theft, financial loss, etc.)
- Was the data encrypted or protected?

Notification Decision

- Internal review by breach response team
- Legal advice obtained if needed
- Affected individuals notified (if required)
- Regulator (Privacy Commissioner) notified (if required)
- Public notice posted (if individual contact is not possible)

Prevention

- Root cause identified
- Technical fix or policy update completed
- Staff training delivered or refreshed
- Vendor contracts reviewed

Staff Guidance

Data Breach Response Training Handout

Audience: Staff, contractors, and client teams

Purpose: Quick-reference guide to responding to data breaches effectively and legally.

What is Data Breach?

A data breach is when personal, sensitive, or confidential information is:

- Accessed by someone who shouldn't (e.g. hackers)
- Disclosed or shared without permission
- Lost or sent to the wrong person

Examples

- An email with personal info is sent to the wrong person
- A laptop with client files is lost or stolen
- Your system is hacked and personal data is accessed
- A third-party software you use is breached

Your 4- Step Response Plan

Step 1 - Contain

- Disconnect affected systems (Wi-Fi, logins, servers)
- Change passwords or remove access rights
- Recover or delete leaked data if possible

Step 2 - Evaluate

Ask yourself:

- What kind of data was involved?
- Who accessed it?
- Could it cause harm (financial, identity theft, distress)? Report to your manager or IT team ASAP

Step 3 - Notify

- If serious harm is likely, affected people must be told
- Some cases must also be reported to the Privacy Commissioner (This decision will be made by your data breach team/IT provider).

Step 4 - Prevent

- Review what went wrong.
- Updatesystems, training, or policies.
- Adjust third-party contracts if needed

How to Report A Breach?

A data breach is when personal, sensitive, or confidential information is:

- Internal staff: Email helpdesk@1300intech.com.au or call 1300 468 324.
- Clients: Use our breach reporting form or call your account manager.

Do’s and Don’ts

DO’S

- Report Immediately.
- Stay calm and follow the process.
- Record what happened.
- Ask for expert help if unsure.

DON’TS

- Ignore or cover up.
- Try to fix it all yourself.
- Delay timing is critical.
- Assume it’s “no big deal”.

In 2024, Infosecurity Magazine reported that nearly all data breaches—**95%**—were caused by **human error**.

1300intech.com.au
1300 468 324
Ringwood, Victoria 3134