DATA BREACH POLICY – NO LIMIT

1. Introduction

This guide provides guidance for No Limit when responding to a data breach.

A Data Breach occurs when data falls into the hands of someone that is not authorised to view it. This can happen many ways, including lost or stolen mobile phones and computers, Internet site or server being hacked, paper records stolen or not destructed correctly, etc.

2. Personal vs Corporate Data

This document will envelope both personal and corporate data. It is a mandatory requirement under the Privacy Act 1988 (Cth) that a breach of personal data is reported to the relevant government agency.

It is requirement of No Limit that a data breach of any type is reported to No Limit management.

If a breach of personal data occurs No Limit's management will immediately forward the details onto the relevant authorities.

3. How do data breaches occur?

Data breaches occur in many ways. Some examples include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased
- databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organisation
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person.

4. Preventing data breaches

It is an obligation under Privacy Act that No Limit takes precautions to prevent data breaches.

As data breaches can happen without a breach in security or computer systems it is expected that all No Limit staff are adequately trained and are aware of how they use data, especially personal data.

All staff are to be aware of the following aspects of data: -

- the sensitivity (having regard to the affected individual(s)) of the personal information held
- the harm that is likely to result to individuals if there is a data breach involving their personal information
- the potential for harm (in terms of reputational or other damage) to No Limit if their information holdings are breached, and
- how the No Limit stores, processes and transmits the personal information (for example, paper-based or electronic records, or by using a third-party service provider).

- Secure destruction of data, including paper documents, hard drives, usb drives, old mobile phones etc.

Remember that in the modern world the firewall is every employee, not just the computers or servers.

5. Risk Assessment of systems

If a No Limit system maintains data, a risk assessment must be performed on the data: -

- Identifying the security risks to personal information held by the organisation and the consequences of a breach of security.
- Identifying the security risks to corporate information held by the organisation and the consequences of a breach of security
- Identifying the legal obligation to storing personal or corporate data.
- Identifying the business continuity impact to the business if there is a breach of this data.
- Identifying the standard required to hold the data, for example, Cloud Security Council recommendations for Cloud providers.

6. Notification of Personal Data being held

If No Limit is holding Personal details on any system it must be fully disclosed to the owner of the information under the Privacy Act. Please see the No Limit Privacy Policy for more details.

7. Identifying a data breach

Identification of a data breach is managed in many ways.

7.1 Stolen Device, e.g. phone, laptop, USB drive, etc

If an IT device is stolen or lost it must be reported IMMEDIATELY.

7.2 Hacked System or security violation

If anyone believes an IT system has been compromised it must be brought to the attention of No Limit management. They must begin an investigation and identify if a data breach has occurred.

7.3 Suspicious behaviour.

If any No Limit employee notices unusual behaviour they are to contact their supervisor immediately who will escalate the event to the correct person. For example, this can be an employee copying company data onto a personal device, or printing company documents for their personal use.

7.4 Information left on printers

If an employee sees a document containing sensitive information left on a printer, they must report it to their supervisor so the owner of the document can be contacted for further action.

8. Responding to the Data Breach

Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

8.1 Contain the breach

Take whatever steps possible to immediately contain the breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach.

For example, if it is detected that a customer's bank account has been compromised, can the affected account be immediately frozen and the funds transferred to a new account?

8.2 Initiate a preliminary assessment

Move quickly to appoint someone to lead the initial assessment. This person should have sufficient authority to conduct the initial investigation, gather any necessary information and make initial recommendations. If necessary, a more detailed evaluation may subsequently be required.

Determine whether there is a need to assemble a team that could include representatives from appropriate parts of the agency or organisation.

Consider the following preliminary questions:

What personal information does the breach involve? What was the cause of the breach?

What is the extent of the breach?

What are the harms (to affected individuals) that could potentially be caused by the breach? How can the breach be contained?

8.3 Consider who needs to be notified immediately

Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.

In some cases it may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals).

Escalate the matter internally as appropriate.

It may also be appropriate to report such breaches to relevant internal investigation units.

If the breach appears to involve theft or other criminal activity, it will generally be appropriate to notify the police.

If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the OAIC. The OAIC may be able to provide guidance and assistance.

Where a law enforcement agency is investigating the breach, consult the investigating agency before making details of the breach public.

Be careful not to destroy evidence that may be valuable in determining the cause or would allow the agency or organisation to take appropriate corrective action.

Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made

8.4 Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, agencies and organisations should assess the risks associated with the breach.

Consider the following factors in assessing the risks: The type of personal information involved.

The context of the affected information and the breach. The cause and extent of the breach.

The risk of serious harm to the affected individuals. The risk of other harms.

8.5 Notification

The Data Breach Committee should consider the particular circumstances of the breach, and:

- decide whether to notify affected individuals, and, if so
- consider when and how notification should occur, who should make the notification, and who should be notified
- consider what information should be included in the notification, and
- consider who else (other than the affected individuals) should be notified

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

In general, notifying the OAIC, or other authorities or regulators should not be a substitute for notifying affected individuals. However, in some circumstances it may be appropriate to notify these third parties:

- OAIC - The OAIC strongly encourages agencies and organisations to report serious data breaches to the OAIC. The potential benefits of notifying the OAIC, together with what it can and cannot do about a notification, are set out at page 37.
- Police — If theft or other crime is suspected. The Australian Federal Police should also be contacted if the breach may constitute a threat to national security.
- Insurers or others — If required by contractual obligations.
- Credit card companies, financial institutions or credit reporting agencies — If their assistance is necessary for contacting individuals or assisting with mitigating harm.
- Professional or other regulatory bodies — If professional or regulatory standards require notification of these bodies. For example, other regulatory bodies, such as the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority have their own requirements in the event of a breach.
- Other internal or external parties not already notified — No Limit should consider the potential impact that the breach and notification to individuals may have on third parties, and take action accordingly. For example, third parties may be affected if individuals cancel their credit cards, or if financial institutions issue new cards.
- Union or other employee representatives.

9. Contacts

Office of the Australian Information Commissioner (OAIC)

Telephone 1300 363 99