BLUE STAR DIRECT
DATA BREACH POLICY

Document Control

Non-Disclosure Clause

The information contained in this document is of a proprietary and confidential nature and will not be copied, transmitted or shown in full or part to any person beyond whom it is intended, especially third party organisations and competitors of Blue Star DIRECT. By reading this document you are accepting the above terms and conditions.

Document Attributes

DOCUMENT TITLE	BLUE STAR DIRECT DATA BREACH POLICY
OWNER	GROUP GENERAL MANAGER, DIRECT
AUTHOR	NATIONAL PROCESS & COMPLIANCE MANAGER
DOCUMENT CLASSIFICATION	INTERNAL USE ONLY
AUTHORISED BY	GROUP GENERAL MANAGER, DIRECT

Version Control

VERSION NUMBER	DATE MODIFIED	MODIFIED BY	REASON FOR MODIFICATION
1.00			Original

References

DOCUMENTS	VERSION NUMBER
Blue Star DIRECT Information Security	V1.00
IVE Group Information Security Incident Management Policy	V1.00
Blue Star DIRECT Privacy Policy	V1.00
Blue Star DIRECT Information Classification, Retention & Disposal Policy	V2.00
Blue Star DIRECT Data Breach Incident Response Report	V1.00

Document Reviewers

NAME	DEPARTMENT/ROLE	DATE REVIWED
David Veness	Group General Manager, DIRECT	9 July 2018
Santo Losurdo	National IT Director	9 July 2018
Paul McMaster	GM, Business Systems & Technology, IVE Group	9 July 2018

1. BACKGROUND

For the purposes of this document, the terms 'data' and 'information' have been used interchangeably and should be taken to mean both data and information.

Blue Star DIRECT (BSD) creates, stores and maintains a vast amount of data, much of which is confidential personal customer information. The stored data is used for direct communication for our customers, including the business requirements, business rules, input data, processed information as well as electronic and printed output.

Information in Blue Star DIRECT is held in many forms such as campaign records, reports, personnel records, paper files, and computerised databases, applications and documents. It may be transmitted in many ways including by hand, by courier, post or electronically using shared communications lines. Information may be transmitted through systems controlled by Blue Star DIRECT or systems controlled by external parties. The principles underlying the need for information security applies to all information irrespective of the media on which it is held.

A data breach is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

In the event that Blue Star DIRECT experiences a data breach, or suspects that a data breach has occurred, it is important that procedures are in place to enable Blue Star DIRECT to contain, assess and respond in a timely manner. This will help minimise potential damage to individuals, our customers and the organisation.

2. SCOPE

This Policy applies to all employees (including contractors and agency personnel) within Blue Star DIRECT who access or deal with BSD Information, Customer Information and Customer Personally Identifiable Information, on behalf of all Blue Star DIRECT sites that are within our operational control and required to comply with the Privacy Act 1988.

3. POLICY

This policy sets out mandatory procedures that staff must apply in the event that Blue Star DIRECT experiences a data breach or suspects that a data breach has occurred.

Blue Star DIRECT policies that should be read in conjunction with this policy are:

- Blue Star DIRECT Information Security Policy
- IVE Group Information Security Incident Management Policy
- Blue Star DIRECT Privacy Policy

4. DEFINITIONS

4.1. DATA BREACHES

A data breach is an incident, in which information is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

4.2. INFORMATION SECURITY BREACH

An information security breach is any incident that results in unauthorised access of data, applications, services, networks and/or devices through bypassing their underlying security mechanisms (e.g. firewalls).

An information security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorised information technology perimeter. An information security breach may also be caused by any software attempts to undermine the confidentiality, integrity or availability of a system and may be the result of external intrusion. The method of intrusion needs to be identified to stop further access and mitigate damage to servers.

Some causes of an information security breach are:

- Databases containing personal information being illegally accessed by individuals outside of the organisation
- Abuse of privileges in a network environment
- Unauthorised changes to network profiles or access control lists.

Information Security breaches and Data Breaches are one and the same, however different processes may need to be followed to ensure a Data Breach is effectively managed with our customers.

Refer to the IVE Group Information Security Incident Management Policy for further details.

4.3. PERSONALLY IDENTIFIABLE INFORMATION

Personal information is defined under the Privacy Act as any information or opinion, about an identified individual or an individual who can be reasonably identified from the information.

The information will still be personal information whether it is true or not and regardless of whether there is a record of it.

Personally identifiable information can be in any format. The definition is technology neutral and is not limited to information contained in records. Personal information might be contained in information that is shared verbally, captured digitally or recorded in writing.

For example:

- A recording of a call containing an individual's voice may be that individual's personal information where the recorded person can be reasonably identified (e.g. when the recording is linked to the customer's file).
- Images of individuals in photographs or video will be personal information where the person's identity is clear or can be reasonably worked out from the image.
- Contact information (e.g. name, home address, phone number, email address).
- Financial details (e.g. credit information, credit card number, transaction information, etc.);
- Government identifiers (e.g. Centrelink Reference Number, Medicare number);
- Tax File Number (TFN);
- Date of birth;
- Health or biometric information;
- Other sensitive information (such as sexual orientation, gender identity, racial or ethnic origin, criminal record, political opinions or religious views).

5. ELIGIBLE DATA BREACHES

The notifiable data breaches (NDB) scheme requires regulated entities to notify affected individuals and the Office of Australian Information Commission (OIAC) about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

When determining whether a data breach is likely to result in serious harm, an objective assessment needs to be conducted and a decision made from the viewpoint of a reasonable person.

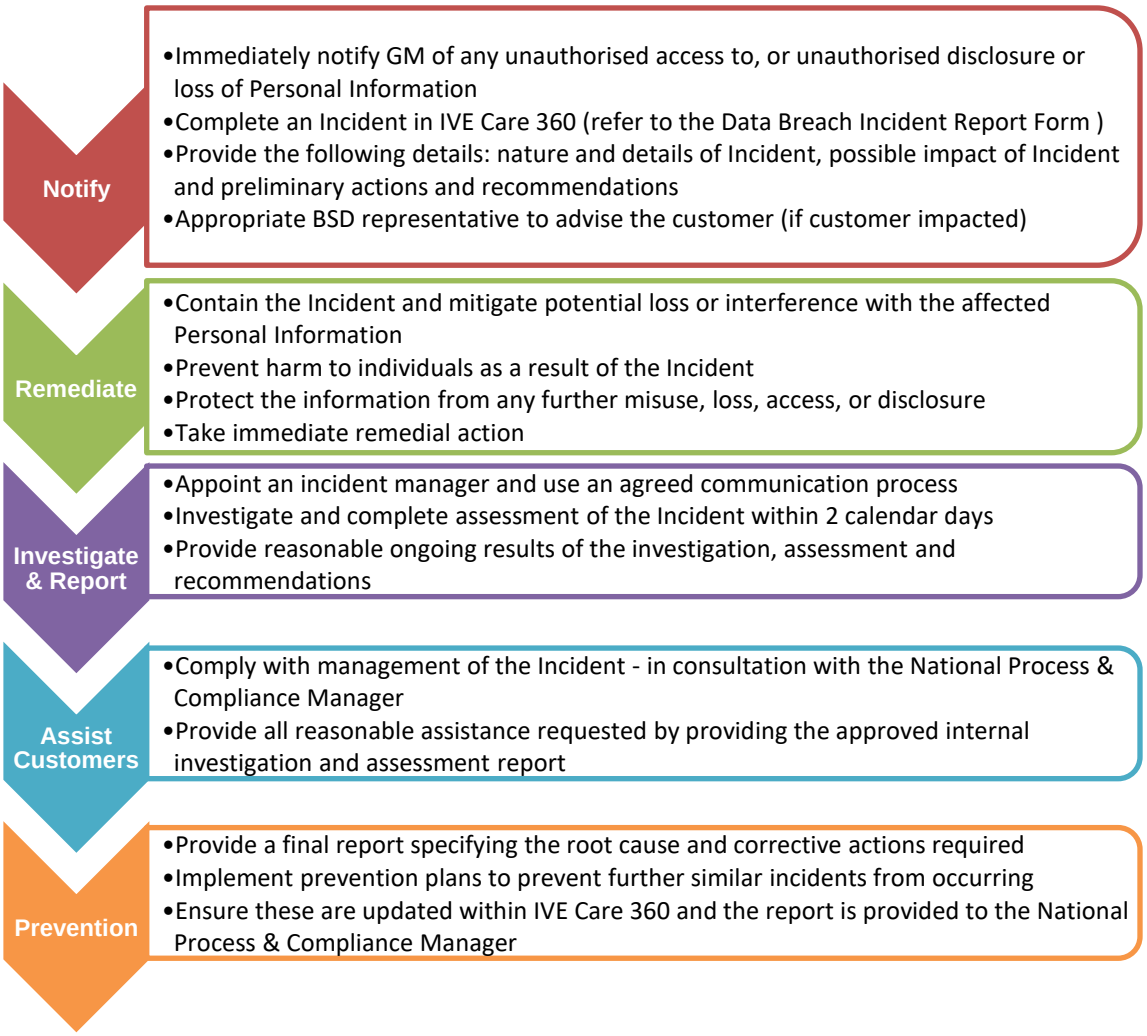
Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Commissioner. Reference: Identifying eligible data breaches (OAIC website).

In all instances, the final decision on whether an eligible data breach has occurred to should be made by the Group General Manager, DIRECT in consultation with the National Process and Compliance Manager and the National IT Director. In all cases, it is Blue Star DIRECT's intention to comply with the Privacy Act.

6. PROCESS FOR MANAGING DATA BREACHES

Notifiable Incidents are to be identified, notified, managed and remediated in accordance with this Policy.

The five key steps to follow when managing Notifiable Incidents are set out below:



7. NOTIFICATION

It is the responsibility of all BSD employees to act accordingly when identifying a potential breach either internally or when notified by a customer. Immediately notify your manager if you become aware of any unauthorised access to, or unauthorised disclosure of personal information or loss of personal information, you also must complete an Incident form (through IVE Care 360). Refer to the Data Beach Incident Report Form.

If you consider that something is 'not right' or has potential to cause a customer concern/harm, immediately notify your manager.

7.1. NATURE AND DETAILS OF THE NOTIFIABLE INCIDENT

- The date of the Notifiable Incident
- The date detected or suspected of the Notifiable Incident
- Description of the Notifiable Incident
- The types of personal information affected (or suspected to be affected) and if not specifically known, explain the types of information that are held on the relevant system that may be affected.
- The root cause of the Notifiable Incident (if known) e.g. malicious or criminal attack, system fault, human error or any control deficiencies or gaps.
- Whether the personal information affected is protected by one or more security measures, e.g. it is encrypted, anonymised or otherwise not easily accessible to unauthorised parties.

7.2. POSSIBLE IMPACT OF NOTIFIABLE INCIDENT

- The number of individuals whose personal information is involved in the Notifiable Incident (if known).

7.3. PRELIMINARY ACTIONS AND RECOMMENDATIONS

- Any action taken to address the Notifiable Incident
- Any action taken to mitigate the harm an individual may suffer as a result of the Notifiable Incident
- Recommendations for any actions that may or will be taken by BSD and/or individuals who may be affected by the Notifiable Incident in order to mitigate its impact and prevent harm to affected individuals.

At the conclusion of the analysis stage (Section 7.1 – 7.3 above), the appropriate BSD representative is to contact the client and advise them of the status of the data breach.

8. REMEDIATE

Immediately after becoming aware of the data breach or suspected data breach, BSD will take all necessary and appropriate action to:

- Contain the data breach e.g. stop the unauthorised practice or recover the records.
- Mitigate potential loss or interference with the affected Personal Information
- Prevent harm to individuals as a result of the breach.
- Protect the information from any further misuse, loss, access or disclosure

- Take immediate remedial action to prevent the likelihood of harm occurring for any individuals whose personal information is involved in the data breach.

9. INVESTIGATE & REPORT

Immediately following notification BSD will:

- Appoint an Incident Manager to lead the initial assessment and be the primary contact point concerning the Notifiable Incident.
- Investigate and complete the Data Breach Incident Report form within IVE Care 360 (to the extent then known), within two (2) business days, including the possible impact of the Notifiable Incident and the likelihood of harm to any individuals to whom the impacted information relates.
- Identify and discuss the steps available to contain the breach e.g. stop the unauthorised practice or recover records and action any agreed steps as soon as practicable, and within the timeframe reasonably required.
- Assess whether further remedial steps can be taken to mitigate the harm an individual may suffer as a result of the Notifiable Incident.
- Provide reasonable ongoing updates on results of the investigation, assessment and recommendations provided in accordance with section 3.1 above and this section 3.3, at a frequency that reflects the severity of the Notifiable Incident, and until the remediation efforts are completed and the prevention plans (if applicable) implemented to the appropriate parties.
- Use agreed communication mechanisms or processes for providing those updates.

10. ASSISTING BLUE STAR DIRECT CUSTOMERS

Immediately following notification BSD will:

- Provide all reasonable assistance in conducting the investigation and assessment of the Notifiable Incident.
- Comply with reasonable directions in connection with management of the Notifiable Incident, including in relation to the prevention of future incidents.
- Determine whether the Notifiable Incident is likely to result in serious harm to affected individuals and therefore requires notification to the OAIC and affected individuals.
- Provide our customer, the control to process the assessing of and notifying affected individuals and the OAIC, and comply with directions concerning those notifications if that notification is required.
- Consult and take into account reasonable considerations before issuing any notifications or statements to the OAIC and affected individuals.

Note: Where a data breach involves more than one entity, the OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification. Refer to the following link on the OIAC website: Joint Entities

11. PREVENTION

Implement prevention once:

- A Notifiable Incident is contained.
- Risk of immediate harm is mitigated.
- Any required notifications to the OAIC and affected individuals are issued.

Provide a final report that specifies:

- The root cause of the data breach incident
- The corrective actions to be undertaken to prevent a repeat occurrence of the Notifiable Incident, which will be specified in prevention plan to the customer's reasonable satisfaction. The prevention plan could include, for example, a security audit to identify required uplifts to physical and technical security; changes to policies and procedures to reflect lessons learned from the incident and investigation; review of employee selection and training practices.
- Implement the prevention plan.

12. IMPLEMENTATION OF THIS POLICY

To enable BSD to assess its ability to respond to Notifiable Incidents in accordance with its responsibilities, BSD may undertake periodic reviews (at a reasonable frequency) to test and validate compliance. These reviews will predominantly focus on testing operational readiness and preparedness for responses to data breaches and mitigation strategies in place.