

**PROTOCOL ON BIOSECURITY DATA AND INFORMATION SHARING  
BETWEEN THE  
COMMONWEALTH, STATE AND TERRITORY BIOSECURITY AGENCIES**

**1. Introduction**

- 1.1. Australia's biosecurity system underpins Australia's agricultural production, agricultural exports and the inbound tourism industry. It also protects human health and social amenity to maintain Australia's biodiverse natural environments.
- 1.2. The national biosecurity system does not exist as a single physical or legal entity. It is built on 'shared responsibility'—the cooperation, investment and actions by all. For governments, the sharing of responsibility occurs through a cooperative partnership under the Intergovernmental Agreement on Biosecurity (IGAB).
- 1.3. The IGAB has created a framework for governments to coordinate and identify priority areas of reform and action to build a more effective national biosecurity system. The National Biosecurity Committee is formally established under the IGAB and provides advice to the Agriculture Senior Officials Committee on national biosecurity and progress in implementing the IGAB along with recommendations from subsequent reviews.
- 1.4. Under IGAB Australian governments have agreed to take a collaborative approach to collecting, collating, analysing, storing and sharing biosecurity information to improve decision making and enhance operational efficiency.
- 1.5. This data sharing protocol (the protocol) expands upon the agreement established by the IGAB by providing greater guidance around the two-way sharing of data and information to support the management of biosecurity risks and the export of Australian agricultural products.
- 1.6. Multilateral sharing of data and information (between Commonwealth and jurisdictional agencies) including that of a sensitive nature is needed to prevent, mitigate and manage the impact of potential or actual biosecurity risks, and those events and issues that may impact the export of Australian agricultural products.

**2. Purpose**

- 2.1. The intent of this protocol is to encourage a culture of responsibility to share data and information except where there are legal or other significant impediments. Parties are responsible for ensuring that it is lawful to share data and information according to the laws that apply in their jurisdiction. This protocol applies to sharing sensitive data, unless otherwise prohibited by law, or where sharing would compromise legal investigations.
- 2.2. The protocol draws on five core principles (Appendix 1) that define the basis for sharing data and information:
  - 2.2.1. data and information should be shared to the extent possible according to circumstances
  - 2.2.2. sharing data and information is essential
  - 2.2.3. data and information are governed
  - 2.2.4. data and information are reliable
  - 2.2.5. data and information are shared securely.
- 2.3. This protocol is a voluntary agreement with the intent that all Parties cooperate with and assist each other in the exchange of data and information.
- 2.4. This protocol does not create any enforceable rights or impose any legally binding obligations on any Party.

### 3. Scope.

3.1. The protocol applies to the sharing of non-sensitive and sensitive data and information, including sensitive data and information where such disclosure is not prohibited by law or where disclosure would not compromise an investigation, to support the management of:

- 3.1.1. potential or actual biosecurity risks that threaten or contravene measures to manage biosecurity at the domestic or international border; and
- 3.1.2. the export of Australian agricultural products.

### 4. Parties

4.1. This protocol is made between the following Parties or subsequent agencies with similar responsibilities:

- Australian Capital Territory - Environment, Planning and Sustainable Development Directorate
- Australian Government - Department of Agriculture and Water Resources
- New South Wales - Department of Primary Industries
- Northern Territory - Department of Primary Industry and Resources
- Queensland - Department of Agriculture and Fisheries
- South Australia - Primary Industries and Regions
- Tasmania - Department of Primary Industries, Parks, Water and Environment
- Victoria - Department of Economic Development, Jobs, Transport and Resources
- Western Australia - Department of Primary Industries and Regional Development

### 5. Data and information quality

- 5.1. All data and information shared under this protocol should be reliable (to the extent possible according to circumstance). The reliability and confidence level of the data should be made explicit when sharing the data.
- 5.2. All data and information shared should be clearly marked with its authoritative source.
- 5.3. Where possible, the data and information should be of a high quality and meet agreed standards. This includes an understanding of the quality of the data according to the circumstances under which it is provided.

### 6. Classification of data and information

- 6.1. The classification levels assigned to data and information will determine what data and information is shared, who data and information is shared with and how the data and information is shared.
- 6.2. The originator sharing the data will determine the sensitivity of data based on the Public, For Official Use Only or Sensitive classifications definitions (refer to clauses 6.3, 6.4 and 6.5 below).
- 6.3. **Public** - The Public classification can be used on data and information that can be made publicly available where its compromise will cause no foreseeable damage to organisations or individuals. Data and information under this classification will be routinely shared amongst jurisdictions in the spirit of the principles that underpin this protocol.
- 6.4. **For Official Use Only (FOUO)** - For Official Use Only should be used on data and information where its disclosure may cause limited damage to the government, organisations or individuals. Data and information shared under this classification will only be shared via an appropriate mechanism with members within the trusted network.
- 6.5. **Sensitive** - The sensitive classification should be used where the disclosure of data and information is limited under legislation or may cause serious damage to the government, organisations or individuals. Data and information shared under this classification will only be shared via an appropriate secure mechanism with members within the trusted network.

## 7. Governance

- 7.1. Parties to this protocol undertake that data and information shared under the protocol will be shared by default.
- 7.2. The Parties agree that when sharing data and information, including sensitive material, they will assign owners and stewards that provide necessary oversight and management of these assets.
- 7.3. Sensitive information will be shared with fewer (trusted) people and will be subject to greater controls. Information that is not sensitive will be shared with a broader audience and subject to fewer controls. Guidelines for sharing sensitive data within the trusted network are outlined in clause 8.2.
- 7.4. Using the classifications described in under clause 6, data and information should be appropriately marked before being shared.
- 7.5. Public data and information can be transferred between Parties via email. Sensitive and for official use only data and information (refer to clause 6) will be transferred via an appropriate secure mechanism to the trusted information network within in each Party (refer to clause 8).
- 7.6. Parties should ensure that accessibility of shared data will be managed with appropriate permissions and common rules as appropriate for its classification.

## 8. Roles and responsibilities

- 8.1. **Agriculture Senior Officials' Committee** – is responsible for endorsing the protocol and facilitating its operation through the cooperative actions of the Council.
- 8.2. **National Biosecurity Committee** – is responsible for reviewing the protocol to maintain its currency and for the operation of the protocol within and between agencies.
- 8.3. **Trusted Information Network** – comprises senior or expert positions and roles that are the recipients of sensitive and for official use only data and information under this protocol. The trusted network will be:
  - 8.3.1. Responsible for ensuring that sensitive and for official use only data and information is shared under the protocol, unless otherwise prohibited by law, or where sharing would compromise legal investigations
  - 8.3.2. Responsible for conveying any restrictions applying to the on sharing of sensitive and for official use only information when sharing information under the protocol
  - 8.3.3. Accountable for the use, storage and access to sensitive and for official use only data and information shared under the protocol
  - 8.3.4. Accountable for the quality of any data and information supplied through the network and for adherence to relevant information management requirements including accessibility and security.
- 8.4. **Specific Points of Contact** – Parties to this agreement will appoint Specific Points of Contact (SPOC) with responsibility for:
  - 8.4.1. Managing data and information requests under the protocol as appropriate. [Trusted network members may request sensitive and for official use only directly from other network members]
  - 8.4.2. Notifying relevant officers within their own agencies when a data request is made agencies or when sensitive or for official use only information is shared as appropriate
  - 8.4.3. Maintaining a register of shared data and information categories
  - 8.4.4. Reporting potential or confirmed data breaches (refer to clause 12)
  - 8.4.5. Responding to queries about the protocol within their Party.
- 8.5. Parties are responsible for sharing, enabling access to and using data and information securely, in accordance with this protocol.

8.6. Further guidance to support the protocol are in the attached appendices.

## **9. On-sharing of data and information**

9.1. All public data and information may be on-shared.

9.2. Parties will not disclose or on-share any sensitive or for official use only data and information it has received unless it has received written agreement from the originating Party sharing the data, or the disclosure is required and authorised by law (for example, under subpoena, Freedom of Information or Ministerial requests). In such circumstances authorised by law, the originating Party will be notified prior to the data and information being shared.

## **10. Data and information use, retention and deletion**

10.1. **Record ownership** the originating Party remains the primary information owner with responsibilities for its quality, reliability etc. of the data and information that is shared.

10.2. **Receiving Parties** may analyse, edit and alter the data and information received under the protocol unless specifically advised not to. Receiving Parties are responsible for managing access permissions to sensitive and for official use only data and information.

10.3. **Storage, retention and deletion** – Parties will ensure that they store, process and delete all data and information in accordance with information management policies and principles and relevant legislation.

10.4. Data and information should be securely destroyed in alignment with the relevant department's corporate records management policy. Parties who have received data and information that is due for deletion should advise the originating Party of this intent.

## **11. Data breaches**

11.1. Under this protocol, a data breach may arise when the following events occur or are suspected to occur affecting data and information shared under this agreement:

- 11.1.1. Loss or unauthorised access, modification, use or disclosure or other misuse.
- 11.1.2. Malicious actions, such as theft or hacking.
- 11.1.3. Internal errors that cause accidental loss or disclosure.

## **12. Responding to data breaches**

12.1. When a Party discovers or suspects that data breach has occurred (refer to Clause 11.1) the process set out in Appendix 2 will be followed. The Party will notify the originating Party of the breach or suspected breach as soon as practicable.

## **13. Review of the protocol**

13.1. It is recognised as policy develops and data and information sharing arrangements mature that this protocol will need be reviewed and amended to ensure that it remains fit for purpose.

13.2. The protocol will be reviewed annually after its implementation. The National Biosecurity Committee will be responsible for initiating this review and the protocol will be amended with mutual agreement of the majority of Parties.

13.3. The protocol may also be amended at the instigation of a Party and with the mutual agreement of the majority of Parties.

## **14. Signatories**

14.1. By signing this protocol, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for data and information and the process of sharing itself are sufficient to meet the purpose of the protocol.

## **List of Appendices**

Appendix 1 Data sharing principles

Appendix 2 Managing data and information breaches

**Data and information sharing principles**

*Principle 1 – data and information should be shared*

Information should be shared unless there are legal or significant impediments. Parties are responsible for ensuring that it is lawful to share information according to the laws that apply in their jurisdiction. This includes sharing sensitive data, unless otherwise prohibited by law, or where sharing would compromise legal investigations.

*Principle 2 – sharing data and information is essential*

All managers of biosecurity risks and facilitators of agricultural exports need to share data and information to effectively manage those risks, to operate at an optimal level and to facilitate sound decision making and delivery of regulatory functions. There should be a clear and common understanding of what information is to be shared, when it will be shared, with whom it will be shared and why it will be shared.

*Principle 3 – data and information are governed*

Data and information, including sensitive material, should have assigned owners and stewards that provide necessary oversight and management of these assets, are accountable for their quality and for adherence to relevant information management requirements including accessibility.

Sensitive material received from other Parties should be held and managed with appropriate security, including determining access.

*Principle 4 – data and information are reliable*

Data and information should be reliable and the confidence level of the data should be made explicit. It should have an authoritative source and be fit for purpose to meet business needs. This includes that there is an understanding of the quality of the data according to the circumstances under which it is provided. Where possible, it should be of a high quality and meet agreed standards.

*Principle 5 – data and information are shared securely*

The mechanism for sharing data and information should be appropriate to ensure the security of its transfer appropriate to its classification. Accessibility of shared data will be managed through agreed access permissions and establishing common rules as appropriate for its security.

## Managing Data Breaches

### Purpose

This Data Breach Response Plan<sup>1</sup> (Response Plan) sets out the procedure to be followed in the event that Parties who have received data and information under the data sharing protocol experience or suspect that a data breach has occurred that has a *sensitive* or *for official use only* classification.

In the event that those Parties sharing data and information under the protocol have a data breach response plan, they should follow their internal processes and ensure that the originating Party, whose data and information has been breached has been advised.

### What is a data breach?

For the purposes of this Response Plan, a data breach occurs when shared information and data classified as *sensitive* or *for official use only* has been lost, subjected to unauthorised access, unauthorised modification, unauthorised disclosure or other misuse or interference.

Data breaches may arise from:

- loss or unauthorised access, modification, use or disclosure or other misuse;
- malicious actions, such as theft or hacking; and
- internal errors that cause accidental loss or disclosure.

### Interaction of the Response Plan with other laws and policies

Assessing and responding to a data breach may involve the consideration of a number of overlapping policies and legal requirements that the Party operates within.

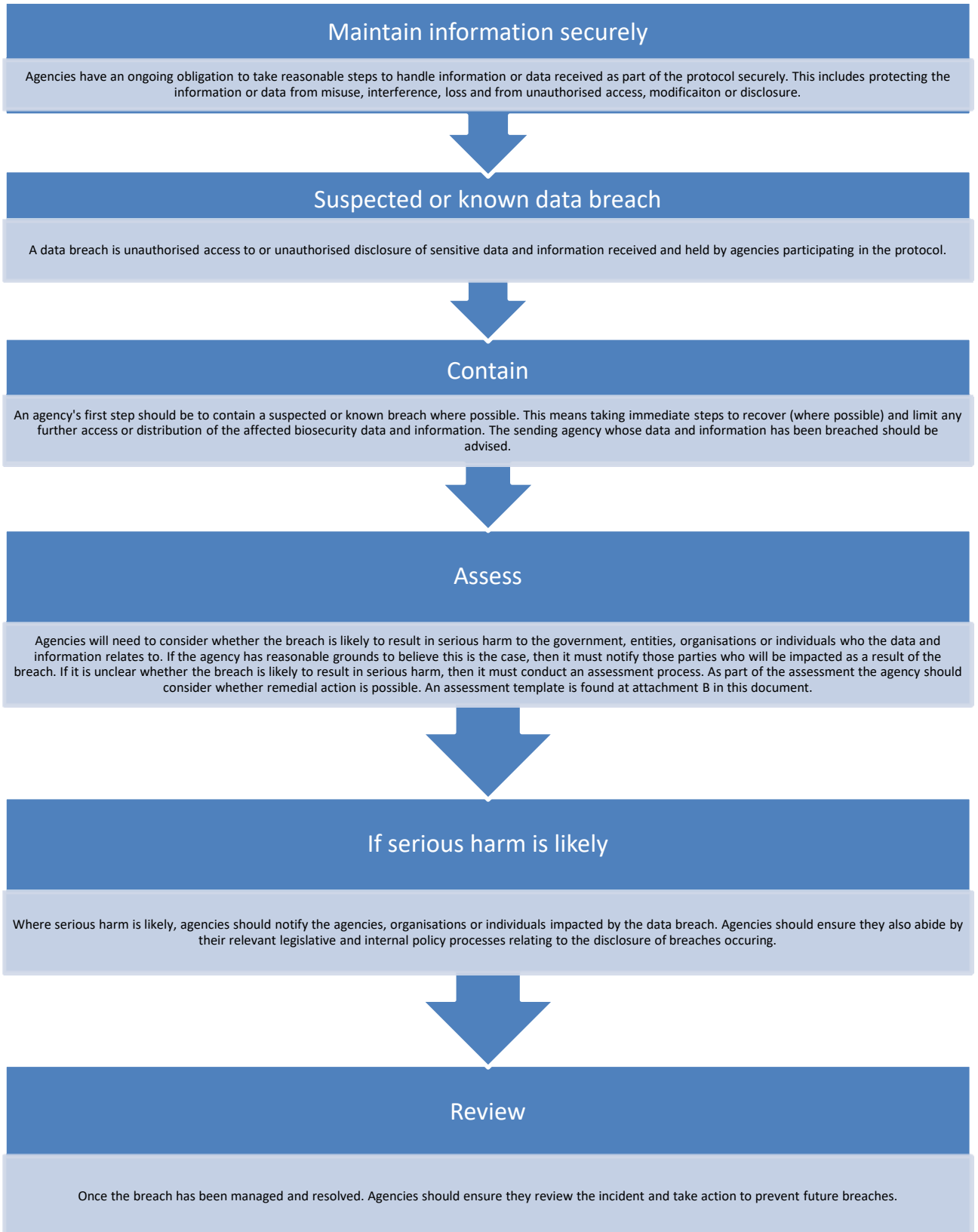
### Responding to data breaches

Parties who do not have an internal data breach response plan should follow the process set out below at Attachment A where a data breach relating to *sensitive* and *for official use only* data and information has occurred.

---

<sup>1</sup> The data breach response plan and process have been developed based upon the Office of Australian Information Commissioners *Data Breach and Preparation Response Guide*

## Attachment A – Data Breach Response Process



## Data Breach Assessment Template

This template should be used by Parties in assessing and reporting on information and data breaches under the protocol.

Description	Details
<b>Description of the breach</b>	<i>Provide a short description of the breach, including the date and time the breach was discovered and the duration and location of the breach.</i>
<b>Type of information/data involved</b>	<i>Insert and detail the type of information and data that was breached.</i>
<b>How the breach was identified</b>	<i>Insert details about how the breach was discovered and by whom.</i>
<b>Cause and extent of breach</b>	<i>Insert details about the cause and extent of the breach.</i>
<b>List of impacted agencies, companies and individuals</b>	<i>List the affected agencies, companies or individuals who are or may be impacted by the breach.</i>
<b>Is the breach likely to result in serious harm to any of the agencies/companies or individuals to whom the data relates?</b>	<p><i>Evaluate whether the breach is likely to result in serious harm to any of the agencies, companies or individuals to whom the information or data relates having regard to:</i></p> <ul style="list-style-type: none"> <li>- <i>The type of information involved</i></li> <li>- <i>The degree of sensitivity of the information</i></li> <li>- <i>The person or persons who have obtained or who could obtain the information</i></li> </ul>
<b>Remedial action taken</b>	<i>Insert details of any steps that have been taken to reduce any potential harm to the agencies, companies or individuals e.g. By recovering the information before it has been accessed or changing access controls on compromised systems</i>
<b>Is or will the remedial action result in reducing the severity of harm to the agency, companies or individuals impacted?</b>	<i>Insert details of whether the remedial action has resulted in making serious harm no longer likely.</i>
<b>Who will be notified of the breach?</b>	<i>Insert details of those agencies, organisations or individuals who will be notified of the breach.</i>
<b>Preliminary recommendations</b>	<i>Include any recommendations on actions that could be undertaken to contain or remediate the breach or prevent future breaches of a similar nature to inform the review of the data breach.</i>
<b>Names of team members as part of the breach response</b>	<i>Insert the names and roles of response team members.</i>
<b>Date</b>	<i>Insert date</i>



For Official Use Only


**Protocol Endorsement by Agriculture Senior Officials Committee (AGSOC)**

This is a non-binding, good faith agreement that supports the work under schedule 3 of the IGAB for Australian governments to take a collaborative approach to collecting, collating, analysing, storing and sharing biosecurity information to improve decision making and enhance operational efficiency.

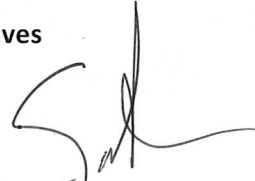
In signing this endorsement:

- AGSOC **AGREES** that the protocol is suitable for implementation with all participating parties.

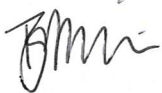
**AGSOC Representatives**



**Daryl Quinlivan**  
Commonwealth Department of Agriculture and  
Water Resources  
Date: 4/10/18



**Scott Hansen**  
New South Wales, Department of Primary  
Industries  
Date: 4/10/18



**Emily Phillips**  
Victoria, Department of Economic  
Development, Jobs, Transport and Resources  
Date: 4/10/18



**Beth Woods**  
Queensland, Department of Agriculture,  
Fisheries and Forestry  
Date: 04/10/2018



**Ralph Addis**  
Western Australia, Department of Primary  
Industries and Regional Development  
Date: 4/10/18



**Scott Ashby**  
South Australia, Primary Industries and Regions  
Date: 4/10/18



**John Whittington**  
Tasmania, Department of Primary Industries,  
Parks, Water and Environment  
Date: 4.10.18



**Alister Trier**  
Northern Territory, Department of Primary  
Industry and Resources  
Date: 4.10.2018



**Ian Walker**  
Australian Capital Territory. Environment,  
Planning and Sustainable Development  
Directorate  
Date: 10/10/18

**Martyn Dunne**  
New Zealand, Ministry for Primary Industries  
Date: