**Privacy Impact Assessment and Report**

*Microsoft Sentinel – Security Information and Event Management Tool*

How to conduct a Privacy Impact Assessment

*Instructions and tips for completing the report are provided in blue italicised text. Please delete any blue text as you complete each section.*

A Privacy Impact Assesment (PIA) process involves the following steps:

1. Conduct a threshold assessment
2. Plan the PIA
3. Describe the project
4. Identify and consult with stakeholders
5. Map the personal information flow
6. Identify the privacy risks
7. Identify options to address the privacy risks
8. Respond and review

1. Conduct a Threshold Assessment

A Privacy Threshold Assessment was conducted which indicated that a PIA was necessary as this project will be:

- Using personal information to make decisions or take action against individuals
- Collecting personal information in a way that might be perceived as being intrusive
- Using personal information for research or statistics
- A new or amended process for verifying an individual’s identity
- Using de-identified information that could be matched with another dataset (or publicly available information) and enable individuals to be identified

2. Plan the PIA

This project involves the implementation of Microsoft Sentinel as our Security information and event management tool. This will involve pulling existing logs from the following systems into a central location:

- M365 including Azure Active Directory, Outlook, SharePoint
- Datto
- Sophos
- Meraki.

The purpose of this project is to enhance our Essential Eight Maturity, to allow us to monitor events taking place on our systems whether by internal or external users and to enable us to report on internal user activity as requested by Management or People and Culture.

Privacy will be considered throughout the project:

- **At collection** – internal users agree to the ICT Acceptable Use policy on
commencement of employment which outlines how the data collected across the system can be used

- **Storage** – Microsoft Sentinel is part of our M365 E5 licensing procured through the Volume Servicing Agreement for Whole of Government. All data is stored within our Azure tenancy which is hosted within Australia.

- **Access**
  - Access to the logs is restricted to the ICT team and the third party provider, PCG Cyber who are providing a security monitoring service as part of their contract. They are covered by an AgriFutures Australia Service Provider Agreement.
  - Data can be requested by members of the Leadership Team and the People and Culture team for performance issues.
  - Data can be requested by the Manager, Legal Services if required as part of an investigation.

- **Type of Data captured**
  - Staff user information including Name, Position, Email Address, who they report to and who reports to them, internal phone number, work mobile phone if applicable.
  - User access details – roles and group members
  - IP addresses and geolocational data
  - Logins
  - Browser data, including search histories
  - Activities – i.e. accessing particular files, deleting documents or emails, forwarding/sharing documents or emails.

- **Disclosure**
  - Data will be available to the ICT team and PCG Cyber in the form of dashboards, alerts and log data to monitor activity within the AgriFutures network and systems.
  - Data may also be provided in the above formats internally to members of the Leadership Team, the People and Culture Team, the Manager Legal Services, The Privacy Officer to aid in performance management or investigations
  - Data may be required to be provided to law enforcement, the Australian Cyber Security Centre or other Agencies as entitled under law.

Privacy will be considered throughout the life cycle of the project and as any additional changes are made to the system in future

3. Describe the project

**Project:** Microsoft Sentinel – Security Information and Event Management Tool

**Description of the project:** Sentinel is being implemented within AgriFutures in order to provide us with the ability to monitor and act on the most up to date ICT security information from within our owned ICT Infrastructure. It is also a critical component of our Essential Eight Compliance.

While we currently have access to all of this information in our current platforms, investigating an issue or suspicious activity can require pulling multiple logs from different administrative portals. Sentinel will provide a centralised view which will improve monitoring and awareness.

**Roles and responsibilities:**
Nicole Legovich, Senior Manager, Corporate (Information Systems and Business Improvements) will be leading the project with assistance from Andrew Roden, Coordinator, Corporate (Information Systems and Business Improvements). Access will also be provided for Kristy Middlebrook, Data Coordinator and Erin Hemphill, Manager, Corporate (Information Systems and Business Improvements).

PCG Cyber will be providing technical staff to assist with the implementation of the new system and monitor the alerts.

**Scope:** Sentinel will pull logs from the M365 environment, including Azure Active Directory, Outlook and SharePoint; Meraki; Sophos; Datto.

**Privacy elements:**
- Staff user information including Name, Position, Email Address, who they report to and who reports to them, internal phone number, work mobile phone if applicable.
- User access details – roles and group members
- IP addresses and geolocational data
- Logins
- Browser data, including search histories
- Activities – i.e. accessing particular files, deleting documents or emails, forwarding/sharing documents or emails.

**Benefits:** The SIEM will enable AgriFutures to monitor events taking place on our information and communication systems.

The purpose of this project is to enhance our Essential Eight Maturity, to allow us to monitor to events taking place on our systems whether by internal or external users and to enable us to report on internal user activity as requested by Management or People and Culture.

4. Identify and consult with stakeholders

The ICT team, comprising of Nicole Legovich, Gerard McTaggart, Andrew Roden, Kristy Middlebrook and Erin Hemphill formed the assessment committee for this project.

CompNow (MSP) were consulted for input and this was a recommendation by the internal audit on Cyber Security.

5. Map the personal information flow
6. Identify the privacy impacts

- Users are made aware that their activities are monitored as part of the ICT acceptable use policy.
- All data is stored within Australia in our Azure instance.
- PCG Cyber have been contracted using our Service Provider Agreement and are thus bound by its terms.
- Data will be used to monitor the security of the systems.
- Data will only be visible to ICT team and PCG Cyber.
- Specific user data will only be provided to the Leadership Team on request.

7. Identify options to address the privacy risks

The ICT acceptable use policy clearly outlines what is considered acceptable in relation to AgriFutures Australia's ICT systems and infrastructure. Staff are required to agree to this on commencement of employment and again on a yearly basis. Any use of the information gathered in the SIEM has been addressed in the policy.

All efforts have been made to secure the data.

Dealing with Risk

The risk is identified as Significant (Major/Unlikely). Should the SIEM be breached, all of our internal user data would be accessible and it would be likely that they would gain access to the whole of our M365 instance. However, the likelihood of this occurring is unlikely given the level of protection offered by Microsoft.

Privacy Risk Assessment Matrix (Relative Severity of Risk)
8. Respond and review

This PIA will be revisited should anything change with this project or additional logs be integrated with the system. Given that this project was a recommendation in order to improve our Essential Eight Compliance, we are confident proceeding.

Document Information

<table>
<thead>
<tr>
<th>Date PIA completed:</th>
<th>31/10/2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td>Draft Completed</td>
</tr>
<tr>
<td>Prepared by:</td>
<td>Nicole Legovich</td>
</tr>
<tr>
<td>Position:</td>
<td>Senior Manager, Corporate (Information Systems and Business Improvements)</td>
</tr>
<tr>
<td>Email:</td>
<td><a href="mailto:Nicole.legovich@agrifutures.com.au">Nicole.legovich@agrifutures.com.au</a></td>
</tr>
</tbody>
</table>

Endorsement and approval

Project manager:

**I recommend** the project proceeds as proposed in this document.

<table>
<thead>
<tr>
<th>Name:</th>
<th>Nicole Legovich</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position:</td>
<td>Senior Manager, Corporate (Information Systems and Business Improvements)</td>
</tr>
</tbody>
</table>
The following officer (General Manager) has endorsed this document:

<table>
<thead>
<tr>
<th>Name</th>
<th>Louise Heaslip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>GM, Corporate</td>
</tr>
<tr>
<td>Signature</td>
<td>[Signature]</td>
</tr>
<tr>
<td>Date</td>
<td>16/11/2022</td>
</tr>
</tbody>
</table>

Privacy officer:

I agree to the project proceeding as proposed in this document.

<table>
<thead>
<tr>
<th>Name</th>
<th>Jessica Grant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>Manager, Governance and Compliance (Privacy Officer)</td>
</tr>
<tr>
<td>Signature</td>
<td>[Signature]</td>
</tr>
<tr>
<td>Date</td>
<td>09.11.2022</td>
</tr>
</tbody>
</table>