Memorandum of Understanding for the Safeguard of Elector Information

[Prescribed authority name:]

1. **I**, [name], [Agency Head/CEO] of the [Prescribed Authority] (‘**the Authority**’), in respect of the [Prescribed Authority], as a prescribed authority for the purposes of the *Commonwealth Electoral Act 1918* (Cth) (‘**Electoral Act**’), understand and agree that the Australian Electoral Commission (**‘AEC’**) may give a copy of a Roll (or an extract of a Roll) (‘**Elector** **Information**’) to the Authority under item 4 of the table in subsection 90B(4) of the Electoral Act subject to compliance with this Memorandum of Understanding (‘**MOU**’).
2. **Provision of Elector Information**
	1. For the purpose of the MOU the Elector Information that may be provided to the Authority, on request by the Authority and payment of the fee in accordance with clause 10 is limited to:
		1. surname and given names;
		2. real place of living (Note: Address information cannot be provided in relation to silent electors and is not available for itinerant and eligible overseas electors).
	2. If the AEC wishes, Elector Information may also include information about the:
		1. sex of; or
		2. date of birth of; or
		3. occupation of

a person included on the electoral Roll.

* 1. Notwithstanding this MOU, the Electoral Commission or delegate may exercise its discretion to not give the Authority Elector Information at any time.
1. **Use of Elector Information**
	1. The Authority must ensure that Elector Information is not used for any purpose other than the permitted purpose as specified in relation to the Authority in Schedule 1 of the *Electoral and Referendum Regulation 2016* (‘**the Regulation**’).
	2. The permitted purpose(s) (as applicable) under item 4 of the table in subsection 90B(4) of the Electoral Act for the Authority is/are (as applicable):
		1. insert each permitted purpose prescribed in the table in Schedule 1 of the Regulationwith respect to the Authority.
	3. The Authority must ensure that Elector Information:
		1. is stored and communicated securely in accordance with clause 3 below;
		2. is not accessed by any:
			* 1. person (other than as permitted in clause 4 below); or
				2. Authority that is not the relevant Authority prescribed in column 2 of the table in Schedule 1 of the Regulation in respect of the Authority;
		3. that persons permitted to access the Elector Information are aware of the conditions and penalties specified in sub-clause 4.5 below; and
		4. is destroyed, deleted or returned in accordance with clause 5 below.
2. **Data security, confidentiality and protection of Elector Information**
	1. The Authority acknowledges that it is an ‘APP entity’ as defined by the *Privacy Act 1988* (Cth) (‘**the Privacy Act**’) and as such will, at all times, comply with the requirements of that Act.
	2. The Authority acknowledges that Elector Information received under item 4 of the table in subsection 90B(4) of the Electoral Act includes confidential and personal information and agrees to:
		1. take all reasonable steps to ensure that the Elector Information supplied is protected against loss, and against unauthorised access, use, modification, disclosure or other misuse;
		2. not disseminate any publications or information otherwise released from data compilations in a manner that is likely to enable the identification of a particular person;
		3. ensure that access to Elector Information is in accordance with clause 4 of this MOU; and
		4. ensure that all Elector Information is stored within a system with adequate controls on access in accordance with sub-clause 3.7 of this MOU.
	3. The Authority must notify the AEC of all unauthorised access, use, modification or disclosure of Elector Information irrespective of whether a report is made to the Office of the Australian Information Commissioner (OAIC). This notice must be in writing and provided as soon as the Authority is aware of the unauthorised use or disclosure.
	4. In accordance with the mandatory Notifiable Data Breach scheme (NDB Scheme) under Part IIIC of the Privacy Act, if the Authority becomes aware, or has reasonable grounds to suspect, a data breach has occurred, involving Elector Information that is personal information that is likely to result in serious harm to any individual affected, the Authority must:
		1. undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected; and
		2. notify the AEC of any Eligible Data Breach (as that term is defined in the Privacy Act), in writing as soon as practicable; and
		3. if the assessment determines that the breach constitutes an Eligible Data Breach, notify the OAIC; and
		4. notify all affected individuals in accordance with the NDB Scheme.
	5. When reporting an Eligible Data Breach, the Authority will provide the AEC with full details of the reported breach and copies of any reports or communications between the Authority and the OAIC relevant to the reported data breach.
	6. If the Authority receives a complaint alleging interference with the privacy of an individual by the Authority arising out of operations within the permitted purpose for the use of the Elector Information the Authority will:
		1. immediately notify the AEC in writing of the nature of that complaint and such details of that complaint as are necessary to minimise any (or further) interference; and
		2. keep the AEC informed as to the progress of that complaint as it relates to the Authority’s actions in connection with that allegation of interference.

***Storage of Elector Information***

* 1. The Elector Information must be stored and communicated securely and the Authority must ensure that the Elector Information:
		1. is not copied (except when uploading the Elector Information in accordance with sub-clause 2.3 or as part of standard system redundancy and backup process);
		2. is uploaded to a computer facility that is owned and operated solely by the Authority or is operated and maintained by a third party under contract with the Authority. Any terms of the relevant contract must mirror section 95B of the Privacy Act;
		3. is stored on a computer facility in such a way as to restrict access to the Elector Information, including any standard system redundancy and backup copies, to permitted persons in accordance with clause 4;
		4. where there is a need to communicate the Elector Information for use in accordance with this MOU, the Elector Information must be encrypted using a Commonwealth Government approved protocol; and
		5. is kept by the Authority in accordance with the Australian Government Protective Security Policy Framework consistently with the Authority’s obligations under the *Privacy Act 1988* (Cth).
	2. The Authority must not transmit, hold or process the Elector Information outside Australia.
	3. The Authority must disclose in writing to the AEC all third-party vendors that have access to their IT systems that stores Elector Information and notify the AEC within one month of any contractual change of third-party vendor.
	4. The Authority must disclose in writing to the AEC any system that stores Elector Information which is managed by a third-party vendor.
	5. Clause 3 will survive the expiration or termination of this MOU.
1. **Access to Elector Information**
	1. The Elector Information must only be accessed and used for a permitted purpose by:
		1. the Authority’s employees employed under the *Public Service Act 1999* (Cth) or another Act authorising the employment of persons on behalf of the Commonwealth or the Authority (as the case requires), who work in a team that has been authorised by the Authority to access Elector Information based on a genuine need for the performance of duties; or
		2. those persons who provide services to the Authority under a contract (‘**Contract Staff**’) who have executed a Deed Poll under sub-clause 4.2 and who work in a team that has been authorised by the Authority to access Elector Information based on a genuine need for the performance of duties. This definition of Contract Staff includes staff at a third party vendor that manages any system which stores Elector Information.
	2. The Authority must require all of the Authority’s Contract Staff, who may access, use or disclose Elector Information as part of their employment duties to execute a Deed Poll provided by the AEC as to the Permitted Purpose of Elector Information before accessing the Elector Information as part of their duties. The Authority must inform the AEC if an Authority Contract Staff member who has executed a Deed Poll is no longer accessing, using or disclosing Elector Information.
	3. The Authority must require all of the Authority’s employees and Contract Staff, who may access, use or disclose Elector Information as part of their employment duties to undertake training which outlines the sensitivity of the data and their legislative requirements as referenced in this MOU.
	4. The Authority must capture and log all records of training attendance, including the dates that the training was undertaken.
	5. The Authority must ensure that its employees and Contract Staff are made aware that:
		1. the use of Elector Information for purposes other than a permitted purpose may constitute a breach of section 91A of the Electoral Act, which carry penalties of up to 100 penalty units. The value of a penalty unit is set by section 4AA of the *Crimes Act 1914* (Cth) and is currently $222;
		2. the use of Elector Information for a commercial purpose may constitute a breach of section 91B of the Electoral Act, which carries penalties of up to 1,000 penalty units;
		3. an offence under Division 478 of the *Criminal Code Act 1995* (Cth) (‘**the Criminal Code’**) may be committed by:
			1. unauthorised access to, or modification of Elector Information for a purpose that is not a permitted purpose. If a person is found guilty of an offence under 478.1 of the Criminal Code, a court may impose a maximum penalty of up to 2 years imprisonment;
			2. unauthorised impairment of the reliability, security or operation of the data held on the disk or other medium containing the Elector Information. If a person is found guilty of an offence under 478.2 of the Criminal Code, a court may impose maximum penalty of up to 2 years imprisonment;
			3. possession or control of Elector Information with intent to commit a computer offence. If a person is found guilty of an offence under 478.3 of the Criminal Code, a court may impose maximum penalty of up to 3 years imprisonment; or
			4. producing, supplying or obtaining the Elector Information with the intent to commit a computer offence. If a person is found guilty of an offence under 478.4 of the Criminal Code, a court may impose maximum penalty of up to 3 years imprisonment.
		4. the Elector Information must remain in the Authority’s power, possession or control and must be securely stored at all times.
	6. The Authority must undertake an annual review of user access rights to ensure user access rights to the data are commensurate with roles and responsibilities.
	7. The Authority must log all access to and undertake the monitoring of audit logs, to monitor for the ongoing appropriate use/access to the Elector Information.
	8. The Authority must retain the inputs (e.g. user listings or audit logs that were reviewed) and outputs (e.g. actions undertaken after the review) of both forms of review outlined above and provide these inputs and outputs to the AEC where required and upon request by the AEC.
2. **Destruction of Elector Information**
	1. On the earlier of:
		1. the expiration of the periodending six months after the receipt of the Elector Information by the Authority, or
		2. the receipt of an updated version of the Electoral Information (or earlier if the Authority decides that it no longer requires the Elector Information).

The Authority must ensure that any medium containing the Elector Information provided by the AEC, including all copies of the Elector Information (as distinct from information about an individual that is merged in the Authority’s records for the relevant permitted purpose) is:

* + 1. securely deleted and destroyed in accordance with the destruction instructions provided by the AEC, or
		2. delivered to the AEC by registered mail.
	1. Within two weeks of the occurrence of an event specified in sub-clause 5.1, and at the direction of the AEC, the Authority must provide to the AEC a Certificate of Destruction (using the template provided) that attests to the:
		1. deletion of the Elector Information earlier uploaded to the computer facility; and
		2. destruction or return by registered mail of the discs or other medium provided by the AEC that contain the Elector Information provided before the receipt of the new Elector Information from the AEC (as the case requires).
	2. The Authority acknowledges that the provision of Elector Information remains at the discretion of the AEC and any request for access to such information by the Authority may be refused. The Authority may not be provided the next provision of Elector Information if the AEC is not satisfied that destruction has occurred.
1. **Security Incidents**
	1. For the purposes of this MOU a ‘**Security Incident**’ is any event that indicates that the security of an information system, service or network has been, or may have been, compromised.
	2. The Authority must immediately advise the AEC’s Elector and Roll Section (via email to rps@aec.gov.au) of any Security Incident involving Elector Information.
2. **Organisational Change**
	1. The Authority will advise the AEC of any proposed changes to organisational structure, or business process that may impact on the way Elector Information is accessed or used. This includes, but is not limited to, any new contractual arrangements which may facilitate a wider use of the Elector Information.
3. **Annual assurance statement**
	1. The Authority must provide the AEC with an annual statement of assurance before 30 June each year that the Elector Information has been used in accordance with the MOU.
	2. Where the Authority fails to provide such assurance, no further Elector Information will be provided until the AEC is fully satisfied that the Authority is operating in strict conformance with the MOU.
4. **Audits of the Management of the Elector Information**
	1. Where the AEC has concerns that the conditions of the MOU have not or are not being met it may request the Authority undertake an audit of its compliance with the provisions of this MOU. The audit must be undertaken at the expense of the Authority and be undertaken by an auditor approved by the AEC Information Technology Security Advisor and the Assistant Commissioner responsible for Assurance at the AEC.
	2. The audit must be prepared pursuant to the provisions of the Standard on Assurance Engagements (ASAE 3150) issued by the Auditing and Assurance Standards Board.
	3. The Authority must provide a copy of the audit report to the AEC within one (1) month of the audit report being available.
	4. If an issue identified in an audit report has not been addressed to the AEC’s satisfaction within 30 business days after receipt of the audit report, the Electoral Commission or delegate may exercise its discretion to not give the Authority further Elector Information. The AEC may also direct the Authority to destroy Elector information that it holds in accordance with clause 5 where an audit report identifies non-compliance with the MOU.
	5. The Authority must report to the AEC, the results of internal and external audit/assurance activities undertaken in relation to systems and processes, as relevant to the management of the Elector Information. This includes independent assurances that third-party vendors are subject to, such as ISO-37000 compliance audits, to ensure their IT systems are secure.
	6. The AEC may, on no less than ten (10) working days notice undertake inspections and/or audits of the Authority no more than once a year, at the Authority’s cost to check the Authority’s compliance with its requirements outlined in this MOU, or any Certificate of Destruction or Deed Poll signed by or required to be signed by the Authority. The Authority agrees to provide the AEC or its agents with reasonable access to their sites to facilitate inspections and/or audits.
5. **Financial arrangements**
	1. The Authority understands that the AEC is entitled to recoup the costs incurred by the AEC in providing Elector Information to the Authority in accordance with subsection 90B(9) of the Electoral Act.
	2. The Authority must pay the service fee and receipt of the payment must be confirmed in order for the AEC to provide Elector Information.
6. **Review and termination of the agreement**
	1. This MOU will commence upon execution and expire five years from the date of execution.
	2. The AEC may at any time review and vary the terms and conditions of this MOU and require the execution of a new MOU.
	3. The AEC may at any time by written notice, terminate this MOU.
	4. Upon receipt of a notice of termination from the AEC, the Authority must:
		1. securely destroy or deliver to the AEC the Elector Information which is in the Authority’s power, possession or control; and
		2. provide the AEC with a statutory declaration confirming that the secure destruction of the Elector Information or the secure delivery of the Elector Information to the AEC is complete and in accordance with this clause.
	5. Any notice under this MOU is only effective if it is in writing, signed by the person giving the notice and either delivered by hand, sent by pre-paid post, or transmitted electronically by electronic mail.
	6. A notice:
		1. must be sent to the relevant address under sub-clause 11.7 using one of the means specified in the following sub-clauses:
7. by hand or courier;
8. by post; or
9. electronic transmission; and
	* 1. subject to sub-clause 11.6(c) is delivered on a business day if delivery occurs before 5 p.m. or otherwise on the next business day; and
		2. is taken to have been delivered on a business day:
10. by post, on the date that it should arrive in the ordinary course of the post from the date of posting for the method of postage used by the person giving the notice; or
11. by electronic transmission on the day and at the hour of transmission, unless the sender receives a notice of failure of the transmission.
	1. For the purposes of sub-clause 11.5 the relevant address is for a notice to:

(a)     the AEC to be directed to the attention of the Elector and Roll Services Section at:

(i)      street address:

10 Mort Street

Canberra ACT 2600

(ii)     postal address:

Locked Bag 4007

Canberra ACT 2601

(iii)    email: rps@aec.gov.au

until otherwise notified by the AEC to the Authority; and

(b)     the Authority to be directed to the attention of [name] at:

(i)      street address:

(ii)     postal address:

(iii)     email:

Until otherwise notified by the Authority to the AEC.

1. **Execution**

Executed on 2021

|  |  |  |
| --- | --- | --- |
| 1. Signed by [name], [Agency Head/CEO], who is duly authorised to make this agreement on behalf of the Authority in the presence of:
2.
3. (Signature of witness)
4.
5. (Name of witness)
 | **))))))))))** |  1. (Signature)
 |