NOTE TO USER

These clauses are intended for use in Australian Government services contracts, including ICT contracts, where the services involve access, transmission or storage of Australian Government information in circumstances where there may be cyber-security risks involved.

The clauses set out the Australian Government's generally preferred position, but entities should consider the particular risks involved for the services, and may agree to change these provisions depending on its assessment of those risks and/or may include clauses to cover any additional mitigating strategies which are necessary or desirable to address those risks.

Generic terms have been identified below and should be replaced appropriately when inserting the clauses into your contract. The generic terms are:

- **Contractor**
- **Customer** (if this term is not used in the contractual arrangement, replace with the defined term for the Australian Government entity as defined in the contractual arrangement.)
- **Contract** (this term may need to be replaced with "Agreement" or "Deed", depending on the defined term for the contractual arrangement. The clause assumes that this term, when used in a deed of standing offer, includes any contract made under that deed; including through placement of an Official Order, Work Order or similar process).
- **Services** (this term is not used in the contractual arrangement, replace with the defined term for the activities to be undertaken by the contractor as defined in the contractual arrangement.)
- If "Notify", "Personnel" or "Subcontractors" are not defined terms in the contractual arrangement, replace these to "notify", "personnel" and "subcontractors".

X. CYBER-SECURITY

X.1 The purpose of clauses X.1, X.2 and X.3 is to set out the Contractor's obligations in respect of information and materials of the Customer:

(a) in respect of which the Contractor has custody or control for purposes connected with this Contract; or

(b) which are accessed, transmitted or stored using or on the Contractor's information systems or equipment under this Contract

(Customer Data).

X.2 The Contractor must:

(a) do all things that a reasonable and prudent entity would do to ensure that all Customer Data is protected at all times from unauthorised access or use by a third party or misuse, damage or destruction by any person;

(b) provide protective measures for the Customer Data that are no less rigorous than accepted industry standards and commensurate with the consequences and probability of unauthorised access to, or use, misuse or loss of, the Customer Data;
(c) without limiting clauses X.2(a) or X.2(b), comply with all security regulations or procedures or directions as are specified in the Contract or given by the Customer from time to time regarding any aspect of security of, or access to, the Customer's information, material or premises; and

(d) unless the Contract or the Customer in writing expressly states that it is not required, develop for acceptance by the Customer a Commonwealth Data Protection Plan (CDPP) that sets out how the Contractor and the Customer will deal with and discharge their obligations in respect of Customer Data (including personal information) during the provision of the Services. The CDPP must:

(i) be consistent with the requirements of the Contract (including clauses X.2(a) and X.2(b));

(ii) be consistent with the requirements of the Privacy Act 1988 (Cth);

(iii) specifically deal with cybercrime risks, including unauthorised access;

(iv) be consistent with the Australian Government’s Protective Security Policy Framework (PSPF) and Information Security Manual (ISM); and

(v) set out the steps and processes that the Contractor and the Customer will follow to protect the Customer Data from unauthorised access, use, misuse, destruction or loss,

and once accepted, the CDPP will form part of the Contract and the Contractor must comply with it unless the Customer otherwise agrees in writing.

X.3 If the Contractor becomes aware of any actual or suspected:

(i) action taken through the use of computer networks that result in an actual or potentially adverse effect on the Contractor’s information system and/or Customer Data residing on that system (Cyber Incident); or

(ii) any other unauthorised access or use by a third party or misuse, damage or destruction by any person (Other Incident),

the Contractor must:

(iii) Notify the Customer in writing immediately (and no longer than 12 hours after becoming aware of the Cyber Incident or Other Incident); and

(iv) comply with any directions issued by the Customer in connection with the Cyber Incident or Other Incident, including in relation to:

(A) notifying the Australian Cyber Security Centre, or any other relevant body, as required by the Customer;

(B) obtaining evidence about how, when and by whom the Contractor’s information system and/or the Customer Data has or may have been compromised, providing it to the Customer on request, and preserving and protecting that evidence for a period of up to 12 months;

(C) implementing any mitigation strategies to reduce the impact of the
Cyber Incident or Other Incident or the likelihood or impact of any future similar incident; and

(D) preserving and protecting Customer Data (including as necessary reverting to any backup or alternative site or taking other action to recover Customer Data).

X.4 The Contractor must, if specified in the Contract, take out and maintain insurance to protect against the risks of a Cyber Incident, and comply with the provisions of <<Insert reference to general insurance clause>> in respect of that insurance.

X.5 The Contractor must ensure that:

(a) all subcontracts and other supply chain arrangements, which may allow or cause access to Customer Data, contain no provisions that are inconsistent with clauses X.1, X.2, X.3 or X.4 or X.5; and

(b) all Personnel and any Subcontractors who have access to Customer Data comply with clauses X.2 and X.3.