Data Security Requirements

Document History & Approval

Date	Description	Author	Approver
3 October 2024	As referred to in the Master Procurement Agreement and/or Statement of Works	Melanie Nguyen, Head of Risk & Compliance	Fred Thiele, Chief Information Security Officer

Document Distribution

Document Title	Document Location
Data Security Requirements	https://www.interactive.com.au/policies-and-procedures/

- Please note that printed versions of this document are considered 'uncontrolled', please refer to the Document Location above to ensure that the latest version is being used.

Table of Contents

1. Background

In addition to the Supplier's obligations under the Master Procurement Agreement and any Order, if the Supplier is providing ICT Services to Interactive, the Supplier must comply with these Data Security Requirements.

2. Definitions

Unless otherwise defined, capitalised terms defined in the Master Procurement Agreement have the same meaning in these Data Security Requirements.

Cloud Services means services provided under an Order to Interactive over the internet or using a telecommunications network, and using servers or other information technology infrastructure controlled by the Supplier or a third party, which may include the provision of platform as a service or infrastructure as a service.

Data Centre Services means the provision of space, racks, and associated facilities within a data centre for the location of Interactive hardware or End Customer hardware.

Developed Software means any software developed, customised, or modified by the Supplier in performing the Software Development Services.

End Customer has the meaning given to it in the Master Procurement Agreement.

End Customer Data has the meaning given to it in the Master Procurement Agreement.

ICT Services(s) means the services (or any of them) specified in the Order, which may include:

a) Cloud Services;

b) Data Centre Services;

c) Maintenance and Support Services;

d) Managed Services; and

e) Software Development Services.

Interactive Data has the meaning given to it in the Master Procurement Agreement.

Maintenance and Support Services mean the maintenance and support services to be provided by the Supplier in respect of Software as specified in the Order.

Managed Services mean services where the Supplier agrees either to manage all or part of Interactive's information technology or infrastructure, or otherwise as specified in the Order.

Security Threat means a computer program, code, device, product or component that is designed to or has the potential to threaten the confidentiality, security, integrity, and or/availability of a system.

Software Development Services mean the development or customisation of software by the Supplier under a relevant Order.

Software means Developed Software, Supplier Software, or Third Party Software.

Supplier Software means any software in which the intellectual property rights are owned by, or licensed to the Supplier.

Third Party Software means programs or applications created by companies other than the Supplier, which the Supplier provides or licenses to Interactive.

Vulnerabilities means a weakness or weaknesses in a system, network, or third party-application that can be exploited to gain unauthorised access, disrupt operations, or cause harm, and includes (but is not limited to the following): software bugs, misconfigurations, and inadequate security controls.

3. Security Controls

The Supplier has and must continue to have in place (for the Term of the Agreement) appropriate physical, technical, personnel, and organisational measures (including without limitation): incident response plans, and processes ("**Security Controls**") to protect Interactive's Data and End Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Interactive may request to view the Supplier's Security Controls to ensure that the Security Controls adequately manage risks that threaten the confidentiality, integrity and/or availability of Interactive's Data and/or End Customer Data.

The Supplier must take all necessary steps to ensure all persons employed, engaged, or subcontracted by the Supplier in connection with the Agreement are made aware of the Data Security Requirements within this document and that all staff who have or may have access to Interactive's Data or End Customer Data have undergone appropriate background checks and security awareness training.

The Supplier must promptly inform Interactive of any actual or suspected Security Threats and/or Vulnerabilities which may adversely affect Interactive Data or End Customer Data, the availability of systems or infrastructure, and the steps taken to avoid their introduction.

4. Audit

The Supplier must, on a regular basis, and at least once per calendar year, conduct systematic and organised testing of its Security Controls (including its processes, policies, and capabilities, access to necessary skill sets, and preventative, detective and responsive security mechanisms, and penetration testing/technical assurance). Such testing must be conducted by appropriately skilled functionally independent specialists, and upon request, Supplier must provide to Interactive a copy of or an opportunity to inspect the audit report.

5. Software Services

If the Supplier is providing Software Development Services, the Supplier must:

- adopt a secure by design approach, coding and testing practices (including but not limited to acceptance testing for the quality and accuracy of the Deliverables);
- use separate environments for the purposes of development, testing, and production;
- protect Interactive Data and End Customer Data throughout the lifecycle of development;
- complete sufficient testing to guard against the presence of known or suspected vulnerabilities, malicious content, (both intentional and unintentional) upon delivery, including (without limitation):penetration testing and vulnerability scans, and provide evidence that such testing has been completed; and
- warrant that any Software provided by the Supplier does not contain any exploitable known vulnerabilities, or malicious code such as back door, time bomb, or any such terms that are capable of performing:
    - any disruptions or providing unauthorised access to a computer system or device; or
    - damaging, destroying, or preventing access to any data or file without Interactive's consent.

6. Developed Software

The Supplier must promptly provide the source code and associated documentation for any Developed Software upon request to Interactive. The Supplier must ensure that all source code for any software which forms part of the Developed Software and its associated documentation:

- is of a high quality including as to design, implementation, and presentation;
- has been designed and written in accordance with best industry practice; and
- is adequately commented throughout the code to enable other programmers having commercially available computer programming skills to read, understand, and modify the source code.

7. Escrow

In respect of any Supplier Software, Third Party Software, or Developed Software, the Supplier (if required by Interactive) must procure that the source code for any Software is placed in escrow on such terms as reasonably required by Interactive.

8. Open Source

The Supplier must not supply Interactive with any open source Software unless it has clearly identified the Software as being or compromising open source software in the relevant Order and Interactive has approved the supply of that open source Software and any relevant licence terms. Any open source Software supplied by the Supplier will be considered Supplier Software for the purpose of the Agreement and without limitation, is subject to the same warranties and indemnities set out in the Agreement in respect of such Software.