

Information Security Policy

Interactive Pty Ltd and its subsidiaries (Interactive) are a leading provider of Cloud, Cyber and Systems services. Interactive's purpose is to keep technology human, its vision is to be our customer's trusted technology partner, and this is achieved through our mission to provide exceptional service delivery through our dedicated team.

Information Security is defined as the protection of confidentiality, integrity and availability of information. To protect the organisation and support its vision as a trusted technology partner, Interactive has established and maintains an efficient and effective Information Security Management System (ISMS). Our ISMS is planned, developed, communicated and integrated into all the functions of the company. Interactive's ISMS policy is communicated to all interested parties including our customers and contractors.

ISMS Objectives

Interactive is committed to:

- Managing information security using a risk management framework with a criteria for evaluating the risk, based on the impact on confidentiality, integrity and availability, and to implement appropriate controls based on the risk outcomes.
- Complying with applicable legal, regulatory requirements and contractual security obligations, including mandatory reporting and notification requirements.
- Ensuring the ISMS is certified against the ISO/IEC 27001 standard.
- Continually improving the ISMS through the establishment and regular review of measurable security objectives at relevant functions and levels of the organisation.
- Ensuring continuity of business operations in the event of a crisis or disaster through the formulation, maintenance and periodic testing of business continuity plans.
- Requiring contractors and third parties working on our behalf to ensure that the confidentiality, integrity and availability requirements of all business systems are met.
- Reporting and investigating suspected or actual information security breaches in an efficient and timely manner.
- Promote security awareness and provide appropriate information security education and training for our staff, applicable contractors and third parties.
- Ensuring that security is integrated into the development lifecycle, from initial design to deployment and maintenance.
- Ensuring procedures are in place for handling of policy exemptions or exceptions.

Scope

The ISMS scope includes information security controls for Interactive's services as described in corresponding Statements of Work and the following supporting business areas:

- Service Desk – Providing 24/7 virtualised call logging services
- Technology – Supporting internal IT systems and applications
- People and Culture – Providing recruitment, training, employee benefits and performance management
- Interactive Repair Centre – Supporting Hardware Maintenance by repairing devices
- Legal – providing internal legal services
- Procurement – providing supply chain management services


Out of Scope

The ISMS scope does not include the security controls which customers are responsible for, including customer tenancies in the Cloud environments.

The security controls for the business processes, staff, information systems or physical security of third-party activities are out of scope because these activities are not under the direct management of Interactive. (Assurance of third-party activities is in scope, performed through contractual agreements and security reviews).


Security controls which third party public cloud providers are responsible for are outside of scope, however the Cloud and managed service; Infrastructure-as-a-Service core services are in scope. EraseIT operates under its own ISMS and is outside of Interactive's ISMS scope.

Signed by:


9690B1111938406...

Brendan Fleiter
Chief Executive Officer

Signed by:


6C21AFB645E5479...

Fred Thiele
Chief Information Security Officer



Document History & Approval

| Date | Description | Author | Approver/s |
|--------------|---|--|---|
| 25 July 2024 | Updated to include: <ul style="list-style-type: none"> • data breach notification requirements • secure development lifecycle controls. | Head of Risk & Compliance, Melanie Nguyen, | Chief Information Security Officer, Fred Thiele Chief Executive Officer, Brendan Fleiter |