3343-POLCY-S01-Information Security Policy-Version 01.05		
Reviewed by: **Katee Houston** Approved by: **Robert Davis**	Effective from; **01/03/2023**	Next Review Due; **01/03/2024**

Classification

Classification	
Public	✓
Internal	
Restricted	
Confidential	
Commercial – In Confidence	

Policy Statement

The purpose of this policy is to set out the companies aims and objectives for the Information Security Management System. Information Security is defined as the preservation of confidentiality, integrity, and availability of information.

This policy provides the overarching approach to the Information Security Management System at EA Technology Ltd. and is the master policy document of the Information Security framework, with all policies relating and remaining consistent with this policy.

Information Security Policy

Scope

This policy is applicable and to be communicated to all employees, temporary/contractors, (clients and authorised third parties where required), who interact with information which is held by EA Technology Ltd. and the information systems used to store and process it. All employees should be applying the scope daily.

Information Security Policy

The following information security principles provide governance for the security and management of the information at EA Technology Ltd.

EA Technology Ltd. will ensure that-

- The Information Security Policy delivers an overarching policy for EA Technology Ltd. ISMS, which will be communicated to all employees, temporary employees and contractors at EA Technology Ltd. and is made available to all interested parties.

- EA Technology Ltd. has established a framework of controls and policies to the principles and requirements of all relevant industry International Standards, Legislation/Regulations and company risks to protect the Confidentiality, Integrity and Availability of asset information, but also, providing a framework of Information Security Best Practice, that will enable EA Technology Ltd. to achieve a security strategy that encompasses the interdependent elements of protective security;
  1) Physical - Buildings, estates and property;
  2) Personnel – Employees, temporary employees and contractors;
  3) Information – hard copy, electronic and information processing systems.

- Such policies and procedures that guide the Information Security will be regularly reviewed and updated as appropriately, through continuous improvement as defined in Clause 10 in ISO/IEC 27001.

- Information assets (both in hard copy and electronic format) both belonging to and entrusted to EA Technology Ltd. are to be protected.

- Every associate of EA Technology Ltd., whether an employee, temporary employee or contractor, are responsible for complying to the Information Security Policy and, any subsidiary policies and procedures appropriately. It is crucial all employees adhere to the ISMS as it only takes one opportunity for a potential 'incident/event' to arise.

- Any security breaches of EA Technology Ltd. Information system, that could lead to the potential loss of *Confidentiality, Integrity* and/or *Availability*, must be reported and investigated appropriately.

- Employees, temporary employees and contractors of EA Technology Ltd. who are responsible for information, must ensure the classification of information and handling of information adheres to its classification as agreed by EA Technology Ltd., with relevant legislation and regulations, such as GDPR, plus, any requirements applied to EA Technology Ltd. by our stakeholders or third-party suppliers.

- All employees, temporary employees and contractors of EA Technology Ltd. who handle personal identifiable information must ensure the correct protection and handling.

- Management are responsible for implementing effective processes within ISMS, to protect EA Technology Ltd. information assets, whilst monitoring controls and compliance.

- Management will ensure to properly brief EA Technology Ltd. employees, temporary employee and contractors of their responsibilities and contribution to the effectiveness of the ISMS; whilst providing training, motivation, monitoring and on-going awareness.

- EA Technology Ltd. will manage the risks associated with the processing and handling of information, digital continuity and records management in respect of all information specifically data held electronically.

Information Security Objectives

The Information Security Objectives will be reviewed and updated quarterly during the Management Review.

Certification

Maintain ISO 27001 certification for EA Technology

Governance

ISO Compliance Officer to develop an audit plan and ensure it is conducted on a monthly basis

Governance

Deliver Management Review meetings and advise Senior Management on a quarterly basis

Risk Assessment

Maintain an accurate risk assessment by Risk Owners reviewing *at least* twice a year

Incidents

The IT department to investigate security incidents within *1 day* of reporting

Employee Training

Deliver/monitor staff training regarding information security on an annual basis – specifically ensuring that any training is completed within *6* weeks

Improvements

ISO Compliance Officer is to ensure any improvements (corrective/improvement actions) in relation to ISO 27001 are implemented within the allocated documented time phase.

Technical Compliance

The ISO Compliance officer will monitor that the technical compliance reviews are being conducted and during the agreed time phase

· Vulnerability scans / Penetration testing
· Access control review (both physical and electronic)
· Access control review (drives)
· Event logs (non-privilege accounts)
· Event logs (privilege accounts)
· Capacity Reports
· Software installation review
· USB data review

Responsibilities

CEO & Board of Directors has responsibility to support the ISMS framework and to approve/review the Information Security Policy.

ISO Compliance Officer has direct responsibility for strategic planning, maintaining the policies and providing advice and guidance for ISMS implementation. In addition, ensuring compliance to any legislation, regulations and industry International Standards.

All Managers are responsible for ensuring the compliance of their associates, plus, providing associates understand their responsibilities regarding ISMS. Managers must also provide motivation, monitoring and on-going awareness training.

Head of Data responsible for IT infrastructure, such as, all ongoing activities that serve to provide appropriate access and protect Confidentiality, Integrity and Availability in compliance with the ISMS policies and standards.

Information Security Committee reviews the ISMS and the Information Security Policy on a regular basis. This will include assessing for any opportunities for continuous improvements and the need to change any aspects of the ISMS.

Risk Owners

[Definition] - *person or entity with the accountability and authority to manage a risk.*

Management levels, who coordinate efforts to mitigate and manage risk with the help of various individuals who own part of the risk. For example, risk identification, assessment, managing, monitoring and updating.

Asset Owners

[Definition] – *person or entity with responsibilities regarding organizational assets*

Management level, who is responsible for and will ensure the correct protection controls are in place for their dedicated asset. For example, ensuring a secure locked door is in place for a room containing a server containing company information

Data Protection Officer

To ensure that organisation processes, personal data of staff, customers, providers or any other individuals in compliance with the applicable data protection rules (GDPR).

All employees must follow EA Technology Ltd. written policies and procedures, plus, thoroughly understand their responsibilities to ISMS and how their roles contribute towards achieving a secure and effective ISMS.

Policy Review

This document will be reviewed **annually** or, if changes are *essential* to be made to the Information Security Policy. The reviews will be made to ensure that the Information Security Policy remains appropriate, up-to-date and relevant in the light of any changes to legislation/regulations or EA Technology Ltd.

Supporting Policies, Procedures and Guidelines

Supporting procedures and guidelines have been established to help reinforce the requirements of ISMS.

EA Technology Ltd. employees, temporary employees and contractors are required to familiarise themselves with *any* Information security supporting or related documents to adhere to them in the working environment.

Robert Davis

CEO, EA Technology Ltd.

Signed: …Robert Davis…

Date: …01/03/2023…

History Review

Version	Date	Revision Author	Approved by	Summary of Change
V01.00.00	20/10/20	Katee Houston	Robert Davis	New Policy
V01.00.01	11/01/21	Katee Houston	Robert Davis	Update to the Responsibility section
V01.02	27/05/2021	Cheryl Ashdown	Katee Houston	Versioning updated to Management System format
V01.03	17/8/2021	Katee Houston	Robert Davis	Removed the introduction information to the document. Classification categories updated to reflect the new category. Updated the header review title. Legislation and Regulations removed from this document.
V01.04	03/02/2022	Katee Houston	Robert Davis	Updated the Security Objective now ISO 27001 certification has been achieved, plus training metric. Plus, software installation has been added to the security objectives.
V01.05	01/03/2023	Katee Houston	Robert Davis	No updates made