3343-POLCY-S01-Information Security Policy-Version 01.08		
Reviewed by: **Katee Houston** Approved by: **Gareth Burton**	Effective from; **07/07/2026**	Next Review Due; **07/07/2028**

Classification

Classification	
Public	✓
Internal	
Restricted	
Confidential	
Commercial – In Confidence	

Policy Statement

The purpose of this policy is to set out the company's 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 and contractors, who interact with information which is held by EA Technology Ltd. and the information systems used to store and process it. All employees are expected to apply and adhere to this policy in their daily activities.

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 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 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 appropriate, 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 employee or contractor is responsible for complying with the Information Security Policy and any subsidiary policies and procedures appropriately. It is essential that all employees adhere to the ISMS, as a single lapse can create the opportunity for a security incident 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.

- EA Technology Ltd. will manage all security incidents in accordance with the Incident Response Policy and Procedure, which governs incident classification, defined roles and responsibilities, escalation paths, and ensures lessons are learned and improvements made.

- 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.

- EA Technology Ltd. will classify and handle information in accordance with the Data Classification and Control Policy, defining handling, labelling, and sharing requirements for each classification level.

- EA Technology Ltd. will ensure that third-party suppliers and contractors with access to information assets are assessed for security risk and are contractually obligated to meet EA Technology Ltd.'s information security requirements.

- All employees and contractors of EA Technology Ltd. who handle personal identifiable information must ensure the correct protection and handling. Access to EA Technology Ltd. information systems will follow the principle of least privilege and require strong authentication, including multi-factor authentication where appropriate.

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

- Management will ensure employees and contractors receive information security training, including but not limited to general awareness and phishing awareness, to support the effectiveness of the ISMS.

- EA Technology Ltd. will manage the risks associated with the processing and handling of information in accordance with a documented Information Security Risk Management methodology, defining risk identification, analysis, evaluation, treatment, acceptance, and monitoring, in alignment with ISO 27001 and 27005.

- EA Technology Ltd. will maintain business continuity and disaster recovery capabilities to ensure the availability of critical information systems, in accordance with the Business Continuity Plan and supporting procedures.

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
Auditing Information Security Manager to develop an audit plan and ensure it is conducted in accordance with the annual plan
Management Review Deliver Management Review meetings and advise Senior Management on a quarterly basis
Risk Assessment Maintain an accurate risk assessment by Risk Owners on an annual basis
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
Improvements Information Security Manager is to ensure any improvements (corrective/improvement actions) in relation to ISO 27001 are implemented within the agreed time phase.
Technical Compliance Information Security Manager will monitor that the technical compliance reviews are being conducted within the agreed timeframe · 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.

Information Security Manager has direct responsibility for strategic planning, maintaining the policies and providing advice and guidance for ISMS implementation. In addition, ensuring compliance with any legislation, regulations and industry International 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.

Data Protection Officer ensures the organisation processes, personal data of staff, customers, providers or any other individuals in compliance with the applicable data protection rules (GDPR).

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

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.

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 organisational 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 storing company information

Policy Review

This document will be reviewed **biannually** 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 and contractors are required to familiarise themselves with *any* information security supporting or related documents to adhere to them in the working environment.

Gareth Burton

CEO, EA Technology Ltd.

Date: 07/07/2026

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
V01.06	17/04/2024	Katee Houston	Robert Davis	No updates made
V01.07	20/08/2025	Katee Houston	Robert Davis	Changes to the objectives wording Job titles changed within 'Responsibility' section Changed to biannual reviews
V01.08	07/07/2026	Katee Houston	Gareth Burton	Strengthened wording on risk management, incident response, third parties, BCP, training, data classification and access control. Standardised terminology Sign off from GB