Information Security Policy

CourtCorrect Ltd.

Document Name	Information Security Policy
Document Number	13-ISMS
Effective Date	08/07/2026
Policy Owner	Chief Executive Officer (CEO)
Approved By	ISMS Management Board
Classification	Public — Approved for External Release

1. Purpose

This Information Security Policy is the highest-level information security document of CourtCorrect Ltd. It establishes the organisation's overall direction, principles, and commitment to protecting the confidentiality, integrity, and availability of information across all of CourtCorrect Ltd.'s operations, systems, and services.

This document is the apex policy of the CourtCorrect Ltd. Information Security Management System (ISMS). It sets the mandate under which all subordinate topic-specific policies, procedures, and controls are established, and it is the policy required by Clause 5.2 of ISO/IEC 27001:2022 and Annex A control 5.1 (Policies for information security). The way in which the ISMS is operated and maintained to give effect to this policy is described in 02-ISMS ISMS Manual.

2. Scope

This policy applies to all information and information systems owned, operated, or processed by CourtCorrect Ltd., and to all individuals who access them, including all employees, contractors, temporary staff, interns, and third parties acting on behalf of the organisation.

CourtCorrect Ltd. operates a cloud-first, AI-based platform for consumer complaint resolution, hosted on Amazon Web Services (AWS) and OVHCloud, and operates from its registered office at 33 Percy Street, London W1T 2DF. The precise boundaries of the ISMS — including the services, locations, assets, and technologies in scope — are defined in **01-ISMS Scope of the ISMS**.

This policy covers information in all forms (electronic, physical, and verbal) throughout its lifecycle, and applies regardless of location, device, or medium.

3. Policy Statement and Leadership Commitment

CourtCorrect Ltd. is committed to protecting the information entrusted to it by its customers, consumers, employees, and partners. Because our platform processes personal data relating to individuals' consumer complaints, information security and data protection are fundamental to our purpose, our regulatory standing, and the trust our customers place in us.

Top management, led by the CEO, is accountable for information security and commits to:

- Establishing, implementing, maintaining, and continually improving the ISMS in accordance with ISO/IEC 27001:2022;
- Ensuring this policy and the information security objectives are established and are compatible with the strategic direction and purpose of the organisation;
- Integrating the ISMS requirements into the organisation's business processes;
- Providing the resources, tooling, and competent personnel needed for an effective ISMS;
- Communicating the importance of effective information security and of conforming to the ISMS requirements;
- Directing and supporting personnel to contribute to the effectiveness of the ISMS, and promoting continual improvement.

This commitment is exercised through the ISMS Management Board, which owns and approves this policy on behalf of top management.

4. Information Security Principles

CourtCorrect Ltd. protects information against loss of the following core properties:

- **Confidentiality —** information is accessible only to those authorised to have access.
- **Integrity —** the accuracy and completeness of information and processing methods are safeguarded.
- **Availability —** authorised users have reliable access to information and associated assets when required.

In upholding these properties, CourtCorrect Ltd. applies the following principles:

- Security is risk-based: controls are selected and prioritised on the basis of assessed risk to the organisation and to data subjects;
- Least privilege and need-to-know govern access to information and systems;
- Security and privacy are considered by design and by default in the development and operation of our AI platform;
- Personal data is processed lawfully, fairly, and transparently, in line with the UK GDPR and the Data Protection Act 2018;
- Everyone who handles CourtCorrect Ltd. information is responsible for protecting it.

5. Information Security Objectives

This policy provides the framework for setting and reviewing information security objectives. Objectives are established, measured, and reviewed by the ISMS Management Board and are documented in **10-ISMS Information Security Objectives Plan**. At the highest level, CourtCorrect Ltd. sets the following standing objectives:

- Protect the confidentiality, integrity, and availability of company, customer, consumer, and employee information;
- Comply with all applicable legal, regulatory, and contractual requirements relating to information security and data protection;
- Achieve and maintain certification to ISO/IEC 27001:2022;
- Prevent, detect, and respond effectively to information security incidents and personal data breaches;

- Build and maintain a culture of security awareness across the organisation.

6. Commitment to Satisfy Applicable Requirements

CourtCorrect Ltd. is committed to satisfying all applicable requirements related to information security, including legal, statutory, regulatory, and contractual obligations. These requirements — including the UK GDPR, the Data Protection Act 2018, and customer contractual commitments — are identified, recorded, and maintained in **12-ISMS Relevant Laws, Regulations, and Contractual Requirements**. Compliance is monitored on a continuous basis, supported by the Vanta trust management platform.

7. Commitment to Continual Improvement

CourtCorrect Ltd. is committed to the continual improvement of the suitability, adequacy, and effectiveness of its ISMS. Improvement is driven through risk assessment, internal and external audit, management review, incident learning, and the tracking of corrective actions, as described in **08-ISMS Procedure for Management Review** and **09-ISMS Procedure for Corrective Action and Continual Improvement**.

8. Governance, Roles, and Responsibilities

Overall accountability for information security rests with the CEO and top management. Day-to-day direction of the ISMS is delegated to the Information Security Management Leader, with governance and approval provided by the ISMS Management Board. All personnel and relevant third parties have a responsibility to comply with this policy and its subordinate policies. Detailed roles, responsibilities, and authorities are defined in **03-ISMS Roles, Responsibilities, and Authorities**.

Policy approvals, policy exception approvals, corrective-action closure, and liaison with auditors and the certification body are exercised by the ISMS Governance Lead (Head of Legal and Compliance), who established the ISMS and leads the certification programme. Day-to-day operation and maintenance of the ISMS is carried out by the ISMS Operations Coordinator under the direction of the Information Security Management Leader, as defined in 03-ISMS Roles, Responsibilities, and Authorities.

9. Information Security Policy Framework

This Information Security Policy sits at the top of a structured hierarchy of documented information. It is given effect by the ISMS management framework, by a set of topic-specific policies that address specific areas of information security, and by the procedures and registers that provide operational detail and evidence. The following framework provides a single, consolidated view of CourtCorrect Ltd.'s information security posture.

9.1 Policy Hierarchy

Tier	Document set	Purpose
Tier 1 — Apex policy	13-ISMS Information Security Policy (this document)	Establishes overall direction, principles, and top-management commitment. Mandated by Clause 5.2 and Annex A 5.1.
Tier 2 — ISMS	00–12 ISMS documents, including	Define how the ISMS is governed,

Tier	Document set	Purpose
management framework	02-ISMS ISMS Manual	planned, operated, evaluated, and improved (ISO/IEC 27001 Clauses 4–10).
Tier 3 — Topic-specific policies	Operational information security policies (see 9.2)	Set mandatory requirements for specific control areas, implementing Annex A controls.
Tier 4 — Procedures, registers, and records	Procedures, plans, registers, and logs referenced by the policies	Provide operational detail and the evidence base for the ISMS (Clause 7.5.3).

9.2 Topic-Specific Policies

The following topic-specific policies are approved under the authority of this Information Security Policy and are mandatory for all in-scope personnel. Each is maintained, versioned, and communicated in accordance with the ISMS, and the definitive list of current versions is held in 00-ISMS Master List of Documents:

Topic-specific policy	Primary focus
Acceptable Use Policy	Acceptable use of information, systems, and devices
Access Control Policy	Identity, authentication, and access management
AI Model Governance and Risk Process	Governance and risk management of AI models
AI Safety Policy	Safe and responsible operation of AI systems
Asset Management Policy	Identification and handling of information assets
Change Management Policy	Controlled change to systems and services
Cryptography Policy	Encryption and key management
Data Protection and Handling Policy	Lawful and secure processing of personal data
Data Retention and Disposal Policy	Retention periods and secure disposal
Disaster Recovery and Business Continuity Plan	Resilience, recovery, and continuity
DSAR Procedure	Handling of data subject access requests
Human Resource Security Policy	Personnel security across the employment lifecycle
Incident Management Policy	Detection, response, and reporting of incidents
Operations Security Policy	Secure operation of systems and networks
Physical Security Policy	Protection of premises and physical assets
Systems Development Lifecycle Policy	Secure development and deployment
Third-Party Supplier Process	Security of suppliers and the supply chain

CourtCorrect Ltd. also maintains corporate governance policies (including the Code of Conduct, Whistleblower Policy, Anti-Bribery, Corruption and Sanctions Policy, Health and Safety Policy, Diversity and Inclusion Policy, and ESG Policy) which operate alongside the ISMS and support the control environment where relevant.

10. Risk Management

CourtCorrect Ltd. operates a consistent, risk-based approach to identifying, assessing, and treating information security risks. Risks are assessed against the confidentiality, integrity, and availability of information and the potential impact on data subjects, and are treated through the selection of appropriate controls. The methodology and criteria are defined in **04-ISMS Risk Assessment and Risk Treatment Process**, and the applicability of controls is recorded in **11-ISMS Statement of Applicability**.

11. Compliance, Monitoring, and Enforcement

Compliance with this policy and its subordinate policies is mandatory. Compliance is monitored through continuous control monitoring (via Vanta), internal audit, and management review. Failure to comply may expose CourtCorrect Ltd. and its customers to risk and may constitute a serious breach of trust.

Any breach of this policy may result in disciplinary action, up to and including termination of employment or contract, and, where applicable, legal action. The disciplinary process for information security breaches is applied in accordance with the Human Resource Security Policy and Annex A control 6.4.

12. Communication, Availability, and Awareness

This policy is documented, approved by top management, and published to all personnel via the company’s document repository. It is communicated to all in-scope personnel on joining and at least annually, and personnel are required to acknowledge it. Because it is classified for external release, this policy is also made available to relevant interested parties, including customers, on request. Awareness and communication activities are managed in accordance with **06-ISMS Information Security Communication Plan**.

13. Review

This policy is reviewed by the ISMS Management Board at planned intervals of at least once every twelve months, and additionally whenever significant changes occur (for example, material changes to the business, technology, regulatory environment, or risk profile), to ensure its continuing suitability, adequacy, and effectiveness.

14. Approval

This Information Security Policy has been approved and is endorsed by the top management of CourtCorrect Ltd. It is issued under the authority of the CEO and approved by the ISMS Management Board.

15. ISO/IEC 27001:2022 Coverage

This document provides evidence of compliance with the following requirements of the ISO/IEC 27001:2022 standard:

Clause / Control	Requirement Name	Application in Document 13-ISMS
Clause 5.1	Leadership and commitment	Satisfied by the documented commitment of top management in Sections 3, 7, and 14.
Clause 5.2	Policy	Satisfied in full: this is the information security policy established by top management, appropriate to the organisation's purpose (Sec. 2–3), containing the objectives framework (Sec. 5), a commitment to satisfy applicable requirements (Sec. 6) and to continual improvement (Sec. 7), and made documented, communicated, and available to interested parties (Sec. 12).
Clause 6.2	Information security objectives	Framework for objectives set in Section 5; detailed objectives maintained in 10-ISMS.
Annex A 5.1	Policies for information security	Satisfied by the definition, approval, publication, communication, acknowledgement, and planned review of this policy and the topic-specific policies mapped in Section 9.
Annex A 6.4	Disciplinary process	Addressed by the enforcement and disciplinary provisions in Section 11.

16. Version History

Version	Date	Description	Prepared by	Approved by
1.0	01/07/2026	Initial creation of the standalone Information Security Policy as the apex ISMS document, established to satisfy ISO/IEC 27001:2022 Clause 5.2 and Annex A 5.1 and to address the non-conformity raised at pre-certification assessment regarding the absence of a unified information security policy.	Angelica Naiko (Head of Legal and Compliance)	ISMS Management Board
1.1	08/07/2026	Updated Section 8 to reflect the ISMS role structure: ISMS Governance Lead authorities and ISMS Operations Coordinator for day-to-day operation (June 2026 internal audit finding).	Angelica Naiko (Head of Legal and Compliance)	ISMS Management Board