clearestate

Security & Compliance Overview

At ClearEstate, security and compliance are paramount to ensuring a safe and reliable user experience. Our commitment is to safeguard your data, eliminate vulnerabilities, and maintain uninterrupted access.

Compliance Certifications

ClearEstate leverages **Vanta** for real-time compliance and privacy standards, in order to enforce its **SOC2 Type II** certification.

Data Security

ClearEstate employs industry-standard technologies to protect consumer data from unauthorized access, disclosure, and loss. We conduct background checks on all employees, and they receive security training regularly.

Infrastructure & Network Security

Our platform is hosted on Google Cloud Platform (GCP), which features multiple layers of security, including electronic access cards, alarms, and biometrics. ClearEstate personnel do not have physical access to GCP data centers.

Third-Party Audits

GCP undergoes regular third-party audits and certifications, such as SSAE 5-compliant SOC certifications and ISO 27001 certification. ClearEstate also undergoes regular third-party audits and can provide its SOC-2 report upon request.

Intrusion Detection & Prevention

We employ intrusion detection and prevention systems (IDS/IPS) to detect and prevent unusual network patterns and suspicious behaviour.

Business Continuity & Disaster Recovery

ClearEstate maintains daily encrypted backups of data on GCP, enabling point-in-time recovery. In case of data loss, we can restore data from backups. We also have disaster recovery plans in place.

For more information, please visit the Security & Compliance page on our website or contact support@clearestate.com.

clearestate

Data Breach Procedures

We have procedures for detecting, responding to, and mitigating data breaches, including a kill switch and data auditing to revert changes made during a breach.

Data Flow & Encryption

Data is encrypted at rest and in transit using AES-256bit encryption. ClearEstate uses JWT authentication tokens for API access.

Data Retention & Removal

We retain consumer data for up to 7 years or as required by law. Data is removed upon termination or by request.

Application Security

We employ single sign-on (SSO), JSON Web Token authentication, and REST API authentication for enhanced security.

Email Security

ClearEstate uses SPF and DMARC to prevent email spoofing and phishing.

Audit Controls

We maintain audit logs of all user actions and activity, and admin controls ensure data safety.

Corporate Security

We protect against internal threats with secure workstations and access controls. Risk management and regular testing are integral to our security practices.

Contingency Planning

We have contingency plans for various scenarios, including risk management, disaster recovery, and communication.

Security Policies

ClearEstate maintains security policies that are regularly reviewed and updated. Consumers can request specific policy details.

Background Checks & Security Training

All employees undergo background checks and security training during onboarding.

Disclosure Policy

We have an incident handling and response process, including communication and documentation. Vulnerability disclosure is encouraged and taken seriously.

For more information, please visit the Security & Compliance page on our website or contact support@clearestate.com.