Duo Security is now part of Cisco.

Duo and CITC's Cloud Computing Regulatory Framework

Duo Security, part of Cisco, combines security expertise with a user-centered philosophy to provide two-factor authentication (2FA), endpoint remediation and secure single sign-on (SSO) tools for the modern era. As a cloud service provider (CSP) with customers in the Kingdom of Saudi Arabia, Duo is required to comply with business continuity, disaster recovery and risk management related rules and guidelines identified as mandatory by the CITC.

Duo complies with applicable provisions in the CITC Cloud Computing Regulatory Framework for data classified as Level 1 and as Level 2. Outlined below are Cloud Computing Regulatory Framework requirements which help demonstrate Duo's compliance.

How Duo Meets Cloud Computing Regulatory Framework Compliance Requirements

Cloud Contracts and Minimum Mandatory Content

Applicable law for the interpretation of the cloud contract and the resolution of any disputes, it being understood that, if this is other than the law of the Kingdom, it may not override any of the provisions of this Regulatory Framework or any other mandatory rules of the Kingdom that may not be overridden through choice of law provisions.

Adopt internal rules and policies on business continuity, disaster recovery and risk management, and provide to their cloud customers or the CSPs they cooperate with, upon their request, a summary of these rules and policies.

Transfer and Location of Customer Content

Cloud customers are informed about their customer content being transferred, stored and processed outside the Kingdom.

Learn more by reading **Duo's Privacy Data Sheet**.

Reporting of Security Breaches

Inform cloud customers of any security breach or information leakage and if either affects, or is likely to affect, cloud customers' cloud content, customer data or any cloud service.

Inform the Commission of any security breach or information leakage, and if either affects, or is likely to affect the customer content or customer data of a significant number of cloud customers or of a significant number of persons in the Kingdom due to their reliance on cloud customers' services that are affected.

Protection of Customer Data

Do not provide or authorise another party to provide to any third-party customer content or customer data, or process or use customer content or customer data for purposes other than those allowed under the cloud computing agreement with the cloud customer concerned.

Grant cloud customers the right and the technical capability to access, verify, correct or delete their customer data.

To find out more about Duo or its compliance with CITC's Cloud Computing Regulatory Framework for data classified as Level 1 and Level 2, contact **sales@duo.com.**