FISMA

Summary

Regulation: Federal Information Security Management Act

Abbreviation: FISMA

Governs these parties: US federal agencies that provide services or receive grant money

Enforced by: the Department of Homeland Security

Details

FISMA aims to reduce the potential risk of unauthorized data use, and to develop, document, and implement an information security and protection program disclosure. The governed federal agencies need to comply with the information security standards guidelines, and mandatory required standards developed by NIST.

The rest of this document is designed to help our community understand FISMA better by outlining the following information.

How it Relates to Cybersecurity

In order to comply with FISMA, federal agencies need to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of and maintain an information system inventory, categorize information systems, maintain a system security plan, utilize security controls, conduct risk assessments, control certification, and accreditation and ensure continuous monitoring.

How Coro Handles Compliance for You

At Coro, we've done the research thoroughly and regularly track updates to the regulation in order to ensure that you are implementing best practices in the areas we cover when we're protecting your systems.

The following table outlines the requirements described by FISMA that Coro implements in conjunction with Microsoft 365 or Google Workspace.