Fidesic

www.fidesic.com

2023

INCIDENT RESPONSE POLICY

Overview

Fidesic information security response is based on the recommended best practices from the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources.

This policy applies to all information systems and information system components of Fidesic. Specifically, it includes:

- Servers and other devices that provide centralized computing capabilities.
- Devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities

Monitoring and Event Alerts

Alerts are sent to the Fidesic Security Board and Infrastructure teams for review and response to any potential threats. These alert channels are available 24 hours a day, 365 days a year.

Incident Response

The Fidesic Security Board will analyze and respond to any event when Fidesic managed customer data has been improperly handled or accessed. Fidesic is required to report all events and accidents. This policy provides the Fidesic Security board authority for direction under incident prevention, identification, investigation, and resolution within all departments.

Required response for all incidents:

- Validating that an incident has occurred
- Communicating with relevant parties and notifications
- Preserving evidence
- Documenting an incident itself and related response activities
- Containing an incident
- Addressing the root cause of an incident
- Escalating an incident

If a security incident is discovered, Fidesic will begin a rapid and effective incident investigation, response and recovery process. A root cause analysis is performed to identify opportunities for measures to improve the overall security posture. Fidesic will follow a formal chain of procedures to collect information, maintain a custody of evidence, and complete a full investigation (this evidence may include legally admissible forensic data when necessary).

Notifications

If there is a confirmed security incident involving information and data stored that involves a Fidesic customer, Fidesic will promptly notify any affected customers of both the scope and potential impact of any such incident. Information about malicious attempts, suspected incidents, or incident history is confidential and not externally shared.