Codecov
Incident Response Workflow

April 19, 2017

1.0 Purpose

The purpose of the policy is to outline the security incident response workflow.

Codecov's intention for publishing an incident response workflow is to focus significant attention on data security and data security breaches, and how Codecov's established culture of openness, trust and integrity should respond to such activity.

Codecov's security team is committed to protecting Codecov's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of Codecov's data has occurred must immediately provide a description of what occurred via e-mail to security@codecov.io.

This e-mail address is monitored by Codecov's security team. Codecov will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the security team will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle protected or sensitive data.

3.0 Policy for confirmed theft, data breach, or exposure of data

As soon as a theft, data breach, or exposure containing protected or sensitive data is identified, the process of removing all access to that resource will begin.

The CEO will form and chair an incident response team to handle the breach or exposure. The incident response team will include Codecov's security team, and may include forensic investigators and legal advisors.

The security team will analyze the breach or exposure to determine the root cause. Once the breach or exposure is dealt with appropriately, the security team will work with other internal teams to conduct and produce a thorough internal post-mortem document, describing the timeline of technical and procedural steps taken, and what procedures will be put in place to prevent similar incidents in the future.

The CEO will decide how to communicate the breach to internal employees, the public, and those directly affected.