Information Security Incident Response Provisions Statement

General

The named Trellix account manager shall be the single point of contact (SPOC) for the customer. The SPOC shall be responsible for the handling of communications with the customer regarding all incidents. The account manager is the primary point of contact for all requests related to the service. Customers can report security issues to Trellix by contacting their account manager/customer service representative or by emailing the dedicated customer support center: trellixsoc.report@trellix.com.

Trellix Responsibilities

1. Management responsibilities and procedures have been established to ensure a quick, effective, and orderly response to information security incidents. The content of such is verified via annual ISO 27001 audits.
2. Employees and contractors using Trellix information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
3. Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.
4. Information security incidents shall be responded to in accordance with the documented procedures.
5. Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. This knowledge shall be anonymized and aggregated form.

6. Trellix shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

Trellix has implemented a business continuity plan (BCP) in relation to its data centers and facilities. An executive summary of the current BCP is available on request under NDA. Trellix reserves the right to update, amend, modify, or change the BCP from time to time.

Notification Procedures

1. Information security incidents shall be reported through appropriate management channels without undue delay.
2. The reporting of these incidents shall be done through secure communication channels adhering to SPF, DMARC, and DKIM standards and opportunistic TLS.
3. Trellix shall report information security incidents within 72 hours of confirming the information security incident impacting probable customers, or as specified by contract or regulation.
4. Reporting of these incidents shall include the following information:
    a. A description of the nature of the information security incident including where possible, the categories of records concerned
    b. The name and contact details of the contact point where more information can be obtained
    c. A description of the likely consequences of the information security incident
    d. A description of the measures taken or proposed to be taken by Trellix to address the information security incident, including, where appropriate, measures to mitigate its possible adverse effects