LAW ENFORCEMENT GUIDELINE

This law enforcement guide ("Guide") addresses ("SECURECRYPT", "we", or the "Company") procedures for responding to law enforcement agencies seeking information about SECURECRYPT user accounts. The information contained herein outlines how SECURECRYPT operates and the extent to which it would be able to assist law enforcement if served with a valid legal order.

This guide is published for informational purposes only, and no statement is to be construed as a promise or guarantee that SECURECRYPT will act in a given way in response to a law enforcement request. SECURECRYPT reserves the right to depart from the practices outlined herein should the circumstances require.

About SECURECRYPT

SECURECRYPT is a mobile security and device management solutions provider for persons that need to manage their internal team and retain internal information integrity. SECURECRYPT's mobile device management application enables internal teams to communicate through a secured and encrypted channel with the assurance that their confidential information is transferred (whether it be messages, files, photos, recordings) in an encrypted channel that is protected from any malicious attacks or espionage. Among other features, the SECURECRYPT application allows users to receive read and deliver notifications, the ability to recreate security keys, encrypt pictures and storage, encrypted saved messages, and participate in group conversations.

SECURECRYPT does not collect any personal information about any of its users. SECURECRYPT does not have access to any phone numbers or email addresses of its users. We do not know who our users are or with whom they communicate. Additionally, SECURECRYPT does not preserve or maintain copies of any content sent by its users including, text messages, photographs, or videos. If SECURECRYPT is temporarily in possession of any user data, such data is fully end-to-end encrypted with keys, which are, at all the time, in the sole possession of the end-users. The Company has no ability to view, monitor, access, or decrypt messages sent between SECURECRYPT users.
SECURECRYPT users have the ability to delete their messages at any time which in turn eliminates all of the encrypted records from the SECURECRYPT servers, the user's phone, and all of the devices of the SECURECRYPT user's mobile contacts.

Information that SECURECRYPT Cannot Provide

SECURECRYPT's operations have been tailored to ensure that users can communicate in a private environment free from monitoring and interference. SECURECRYPT does not require any personal identifiable information from its users in order to use its messaging service. The content of SECURECRYPT user communications are not available to the Company. Where law enforcement agencies seek access to user content or messages, the Company's response will simply reflect that such information does not exist on its servers. If SECURECRYPT does possess any data on its servers, such information would be fully encrypted and the Company will not have the ability to decrypt it. For absolute precision, due to the design of SECURECRYPT's operations, the Company does not have access to, and as such, cannot provide law enforcement with any of the following information pertaining to users of SECURECRYPT:
• text messages, photographs, and videos;
• phone numbers;

• email addresses;
• display images;
• birth date;
• metadata for messages;
• number of sent/received messages or images;
• IP address; and
• user's location.

What Can SECURECRYPT Provide You?

As noted above, SECURECRYPT cannot provide law enforcement with any decipherable user content.

To the extent that the account ID has been provided to SECURECRYPT, the only information the Company will be able to provide to law enforcement agencies will be limited to the following:
• date an account was created; and
• date of last use.

Service of Orders on SECURECRYPT

SECURECRYPT is committed to respecting the rules and laws of the jurisdictions in which it operates while also upholding the privacy rights of its users. Accordingly, SECURECRYPT will cooperate with law enforcement only to the extent that the law requires. SECURECRYPT responds to valid legal process issued in compliance with Canadian law. Requests for user information requires a production order, search warrant or other valid legal order from an agency with proper jurisdiction over SECURECRYPT.

The Company will not respond to a request voluntarily.

To protect our customers' rights, we scrutinize all requests to ensure that they comply with the law. SECURECRYPT does not respond to requests from law enforcement agencies outside of Canada unless the legal process has been supplied under a mutual legal assistance treaty or letters rogatory. As per our Terms of Service, if a device is being investigated as part of a valid legal process with proper jurisdiction in connection with any illicit, illegal or criminal activity, we will deactivate the account associated with that device. We will also decline a customer's request to remote wipe a device that we know is subject to a valid legal investigation; however, it should be noted that our software automatically erases all data at least every seven days (fewer, if users change their settings), and we are unable to prevent such data from being erased, or provide any access to any decipherable user content.

Receipt of correspondence and communication with law enforcement by email does not waive any objections to the lack of jurisdiction or proper service inherent in attempted service of process via email. SECURECRYPT will process requests as quickly as possible; however, law enforcement can typically expect a response to take to upwards of 30 days.

In order for SECURECRYPT to better evaluate the nature of the request, the following information must be included in the request:

• name of the SECURECRYPT user being investigated;
• account ID;
• law enforcement letterhead;

• valid official return email address and mailing address;
• details for an agency contact person including, name, identification number and phone number;
• specific list of user information being sought;
• production order, search warrant, or other valid legal process for information; and
• request is signed and dated.

Please send all requests to: securecrypt.mobile@protonmail.com ATTN: Privacy Officer.