

# Email Alert Case Management User Guide

A step-by-step guide for responding to automated email alerts.

## Step 1: Responding to email alerts

Review the alert and scroll to the bottom of the email to select the appropriate response.

**Please scroll down to the bottom of this email and select one of the responses below.**

Hello [redacted],

Please see alert below:

Case Notification

You have a new or updated case. Please review the information below. Click on the Case # hyperlink to view case details, and then reply with your action.

Case #:  
**234150**

Client Name:  
[redacted]

**Schools**

Case Status:  
**Investigating**

Case Created: 04/21/2024 17:26 UTC    Case Criticality: Low    # of Alerts: 5

Recent Narrative Time	Narrative
04/27/2024 01:37 UTC	Update : Unusual SharePoint Download Activity User : [redacted] Source IP : [redacted] Kindly confirm this activity.

Thank You,

**Securus360 Alert Support**  
(949) 266-6900 | [s360alerts@securus360.com](mailto:s360alerts@securus360.com)



100 Spectrum Center Drive, Suite 900  
Irvine, California 92618

[www.securus360.com](http://www.securus360.com)

**Select and confirm one of the options below to respond.**

- 1. Legitimate
- 2. Investigate
- 3. Malicious



**Review Alert and select response via these buttons.**

# Email Alert Case Management User Guide

## Response Option Definitions:

**1. Legitimate:** Select the "Legitimate" button if you identify this activity as legitimate. At this stage, we will mark this case as "Closed".

NOTE: Marking cases as legitimate will help improve the accuracy of the auto-silencer.

**2. Investigate:** Select the "Investigate" button if you're uncertain about the legitimacy of this activity and need more time to investigate internally. If you need assistance, please reach out to us at [investigate@securus360.com](mailto:investigate@securus360.com).

**3. Malicious:** Select the "Malicious" button if you identify this activity as malicious. If remediation assistance is needed, please provide further details in a separate email to [remediation@securus360.com](mailto:remediation@securus360.com).

**NOTE:** Please do not Reply or Forward the automated email to Securus360 with text response 1, 2, or 3, this response will not be processed. A follow-up email will be sent automatically if none of the options are selected.

## Step 2: Confirming your response action

After selecting the appropriate response, you will be asked to confirm your action. Please select "Confirm..." to validate your response selection.

**Confirm Action**

Do you want to confirm your option and send this response back to the sender?

Response confirmation will be displayed along with the response type selected.

Thank you! Your response '1. Legitimate' has been successfully registered.

# Email Alert Case Management User Guide

## Step 3: Response confirmation email

When the response confirmation is processed, you will receive a confirmation email which will also include the original alert details.

Hello [redacted] USD,

Your selection of **1. Legitimate** has been noted.

You have a new or updated case. Please review the information below. Click on the Case # hyperlink to view case details, and then reply with your action.

**Case #:**  
**23215**

**Client Name:**  
**[redacted] Unified School District**

**Case Status:**  
**Investigating**

Case Created:	Case Criticality:	# of Alerts:
08/02/2023 15:39 UTC	Critical	4

Recent Narrative Time	Narrative
08/03/2023 13:11 UTC	This is a test case email for Securus360. This case includes for instances of possible exploits of CVE-2017-8759. The device name is [redacted] and the actions were taken by user [redacted]. The parent process is csc.exe.

**Please respond with your course of action.**

1. Legitimate
2. Investigate
3. Malicious

Thank You,

**SOC Support**  
(949) 266-6900 | [s360alerts@securus360.com](mailto:s360alerts@securus360.com)

**SECURUS 360**  
100 Spectrum Center Drive, Suite 900  
Irvine, California 92618  
[www.securus360.com](http://www.securus360.com)

**Note:** Please ensure **all** alerts are addressed, and the confirmation email is received, as soon as possible. If confirmation is not received after **4 attempts** to reach your team, we will reach out to your team per the agreed escalation policy to ensure alerts are fully vetted and closed. If you have any questions, feel free to reach out to our technical staff via email at [support@securus360.com](mailto:support@securus360.com)