Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Objectionable Content Takedown Template

September 2022

The reference URL for this document:
https://www.m3aawg.org/ObjectionableContentTakedownTemplate

Introduction

This document provides a template for designing an enforcement process to use when a organization becomes aware of objectionable content being hosted on its network and determines that it requires a takedown. This objectionable content might fall under – but may not necessarily be limited to – the organization's policies and applicable regulations. As with all handling procedures, these processes need to be developed and available ahead of any potential incident in order to provide a timely response. This template is intended to be used as a guide to suggest steps organizations may take into consideration when developing their Objectionable Content Takedown procedures.

Defining Objectionable Content

For the purposes of this document, objectionable content may include, but is not limited to:

- violent materials, including the most egregious
- violent audio
- visual or audiovisual material produced by a perpetrator or their accomplice
- other material that crosses legal thresholds

The material may take the form of:

- video
- still images (including a series of still images)
- audio recordings
- written text

The material may include:

- streaming or recorded conduct of a person engaging in a terrorist act (involving serious physical harm or death of another person).
- murder or attempts to murder another person, torture of another person, rape of another person or kidnap of another person (where the kidnapping involves violence or the threat of violence).

Important Note Regarding Child Sexual Abuse Material

While Child Sexual Abuse Material (CSAM) unquestionably qualifies as objectionable content, it requires additional considerations not addressed in this template. If the objectionable material is suspected to be CSAM, ***do not*** follow the steps outlined in this template. Suspected CSAM material ***must not*** be investigated by anyone except specially designated government officials (NCMEC, INHOPE, FBI Innocent Images Task Force, etc.). ***Consult legal counsel to determine handling practices for suspected CSAM.***

Additional Notes

The steps outlined in this document are intended to be a guide only; additional and/or alternative procedures may be needed. Readers should consult their organization's legal counsel to determine which regulations and procedures are appropriate.

Once processes are completely developed, it is important that to test their effectiveness through such activities as tabletop exercises.

Agreements: Organizations must ensure that client contracts and/or Terms of Service (ToS) include appropriate language and conditions that clearly spell out the obligations and remedies regarding objectionable content.

The authors of this document are working on a related taxonomy and a compilation of references to specific laws from various jurisdictions. When complete, the information will be added to this document.

Key Steps

Policy Enforcement Team Receives reports of content qualifying for takedown that is hosted on <*ISP*>'s network.	Follow the takedown process for qualifying objectionable content if an incident takes place and is hosted on <*organization name*>'s network. ***Follow separate CSAM procedures for objectionable content suspected to be CSAM.*** • Perform an assessment of the objectionable content to determine or validate the scope of the infraction (content). This may require consultation with the organization's legal counsel or other management. • When required, consult with the appropriate government entity that has jurisdiction over the objectionable content for guidance. (This step prevents the organization from

	unintentionally interfering in an active investigation.) • Set the priority of the takedown action based on the urgency and scope of the infraction. • Notify internal stakeholders including security, legal and management of the presence of objectionable content hosted on or being sent from the organization's network. • Ensure that all necessary internal stakeholders are aligned and agree on immediate next steps to prevent further distribution or hosting of the content. • If and when appropriate, ensure that the client is notified of the infraction. • Take the necessary steps to take down the content or prevent further distribution of the content. When not directly under the organization's control, work with the client on a mitigation plan to meet this objective. • Follow up with additional investigations to ensure the content has not been backed up or stored on other parts of the organization's network. • If you are aware that the content has been distributed elsewhere, where possible, you may want to contact the networks in the distribution chain and inform them of the nature of the content. • Preserve all records, including metadata, and all processes used to remove the objectionable content, including documented rationale supporting the content's removal. • Investigate how the content was posted on the organization's network, its source, and the actors responsible in order to remind the offending party of their obligations under the terms of service. • Consider the welfare of employees who may have been traumatized by this ordeal, and provide professional help when warranted. The attached action checklist will serve as a guide to help ensure that each step has been taken. Record details as requested (who took the action, when it was completed, and so on).

Process Checklist

This template is only a guide; adjust it to the organization's specific needs and situation.

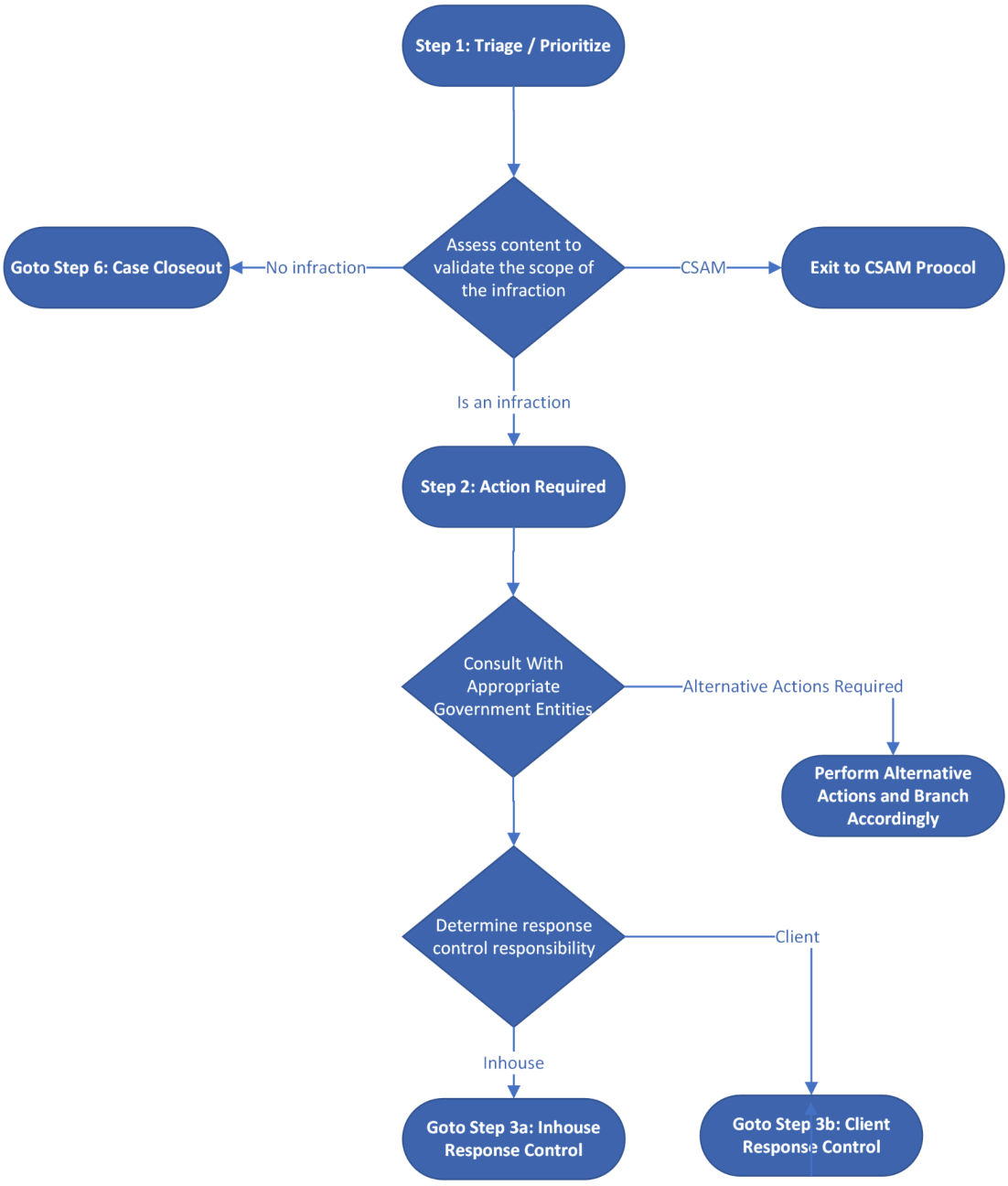
Please ensure each step below has been taken. Note details requested such as names, date and times.

Step Taken	Date/Time Completed	Details/Sign-off
Step 1: Triage/Prioritize		
Perform an assessment of the objectionable content to determine or validate the scope of the infraction.		(Include how the content was vetted, by whom, and the rationale for the assessment.)
Material is CSAM. Invoke separate CSAM handling procedures and exit.		
Meets the threshold for objectionable content. *Go to Step 2: Action Required*		
Does not meet the threshold. No further action required. *Go to Step 6: Case Closeout*		
Step 2: Action Required		
When required, consult with appropriate government entities to determine if alternative actions are required.		
Alternative actions required. Perform alternative actions and branch accordingly.		
Determine who has response control.		(Determine whether in-house or client responsibility.)
In-house responsibility *Go to Step 3a: In-house Response Control*		
Client responsibility *Go to Step 3b: Client Response Control*		
Step 3a: In-house Response Control		
Determine appropriate mitigation steps.		
Initiate and execute mitigation steps.		
Go to Step 6: Case Closeout		
Step 3b: Client Response Control		
Determine what is required to perform		

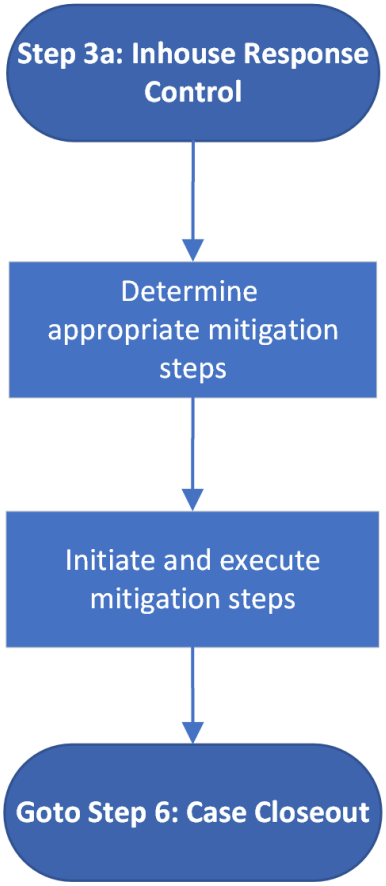
Step Taken	Date/Time Completed	Details/Sign-off
immediate blocking of the service/material prior to notifying the client.		
Adequately notify the affected client of the issue and actions that have already been taken.		(Include who was notified and when.)
Notify customer account representatives.		(Include who was notified and when.)
Have all parties agreed on a mitigation action plan and timeframe. Plan should consider both regulatory and contractual requirements.		(Include details and timeframe.)
Obtain acknowledgement from the customer that remedial actions will be enforced (including potential termination of services) if mitigation steps are not completed within the agreed timeframe.		
Step 4: Client Action		
Client executes mitigation steps.		
Client has successfully executed mitigation steps within the agreed timeframe. *Go to Step 6: Case Closeout*		
Client has not executed the mitigation steps within the agreed timeframe. *Go to Step 5: Remedial Action*		
Step 5: Remedial Action		
Obtain approval from legal counsel for the execution of remedial action.		(Provide an approved date of remedy.)
Provide remedial action notice to the customer.		(Include who was notified and when.)
Execute remedial action (may include termination of service). *Go to Step 6: Case Closeout*		
Step 6: Case Closeout		
Perform applicable post-takedown procedures.		(May include informing the reporting party of action taken.)
Close case.		

ADDENDUM B - Process Decision Flows

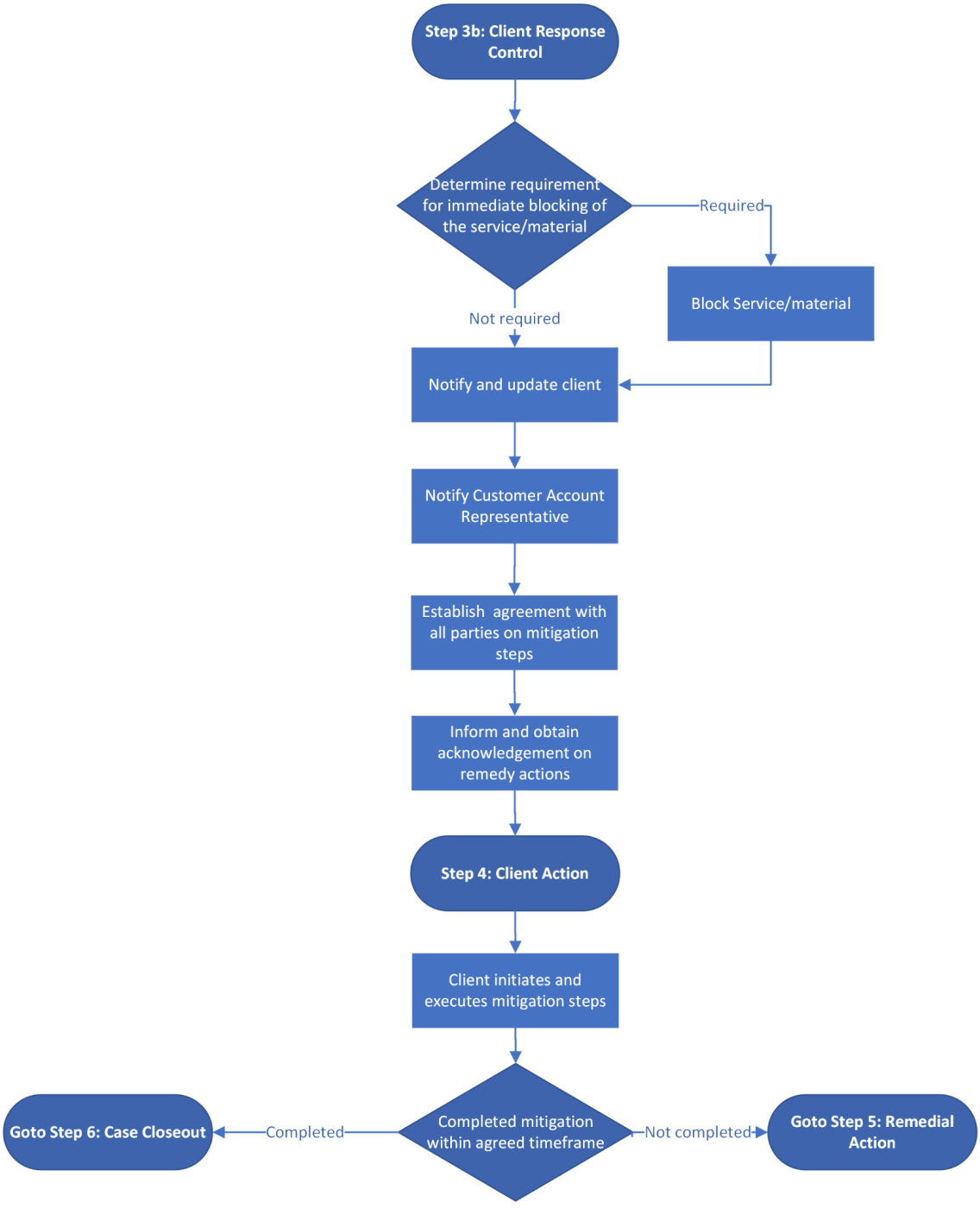
Step 1: Triage / Prioritize



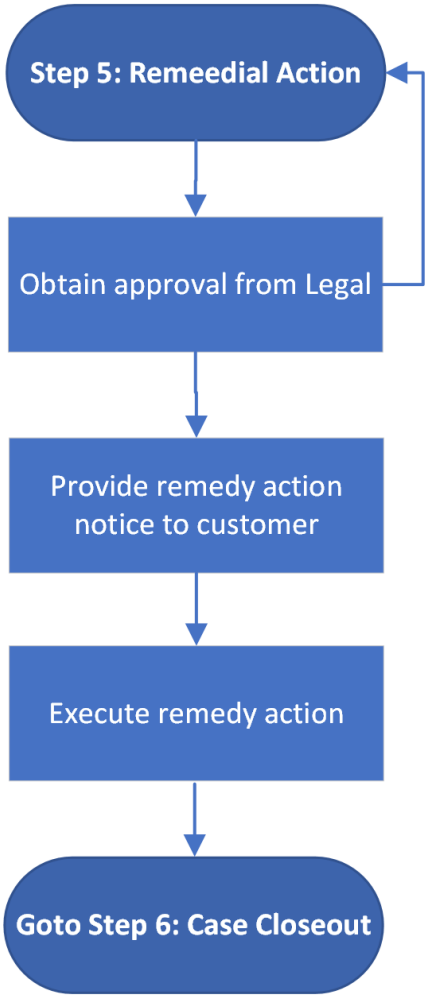
Step 3a: In-house Response Control



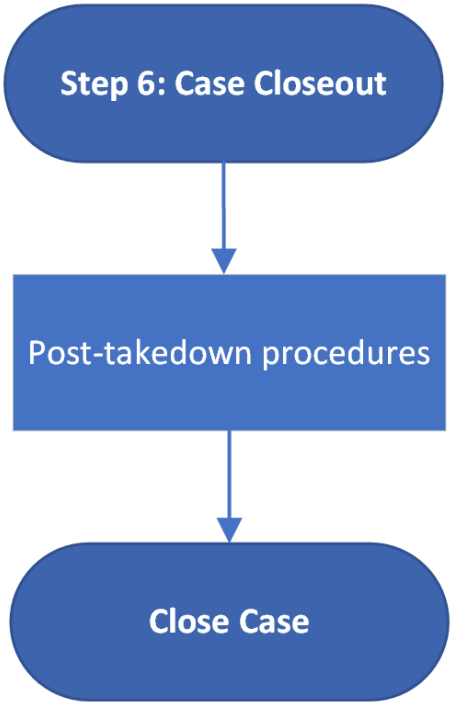
Step 3b: Client Response Control



Step 5: Remedial Action



Step 6: Case Closeout



As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates.