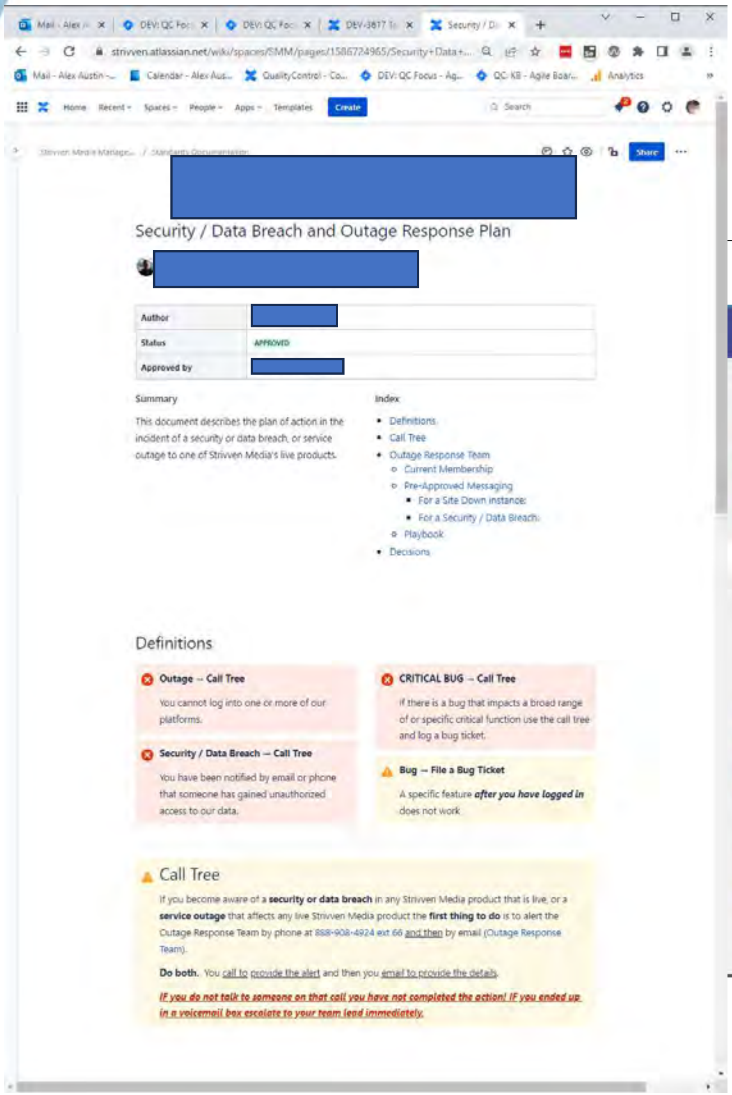
[redacted]

Security / Data Breach and Outage Response Plan

[redacted]

Critical Response Plan



Mail - Alex ... | DEV: QC Foc... | DEV: QC Foc... | DEV-3817 ... | Security / D...
strivven.atlassian.net/wiki/spaces/SMM/pages/1586724965/Security+Data+...
Mail - Alex Austin -... | Calendar - Alex Aus... | QualityControl - Co... | DEV: QC Focus - Ag... | QC KB - Agile Boar... | Analytics
Home | Recent | Spaces | People | Apps | Templates | Create | Search
Strivven Media Manage... / Standards Documentation
Share

[redacted]

Security / Data Breach and Outage Response Plan

[redacted]

Author	[redacted]
Status	APPROVED
Approved by	[redacted]

Summary

This document describes the plan of action in the incident of a security or data breach, or service outage to one of Strivven Media's live products.

Index

Definitions

Outage – Call Tree

You cannot log into one or more of our platforms.

Security / Data Breach – Call Tree

You have been notified by email or phone that someone has gained unauthorized access to our data.

CRITICAL BUG – Call Tree

If there is a bug that impacts a broad range of or specific critical function use the call tree and log a bug ticket.

Bug – File a Bug Ticket

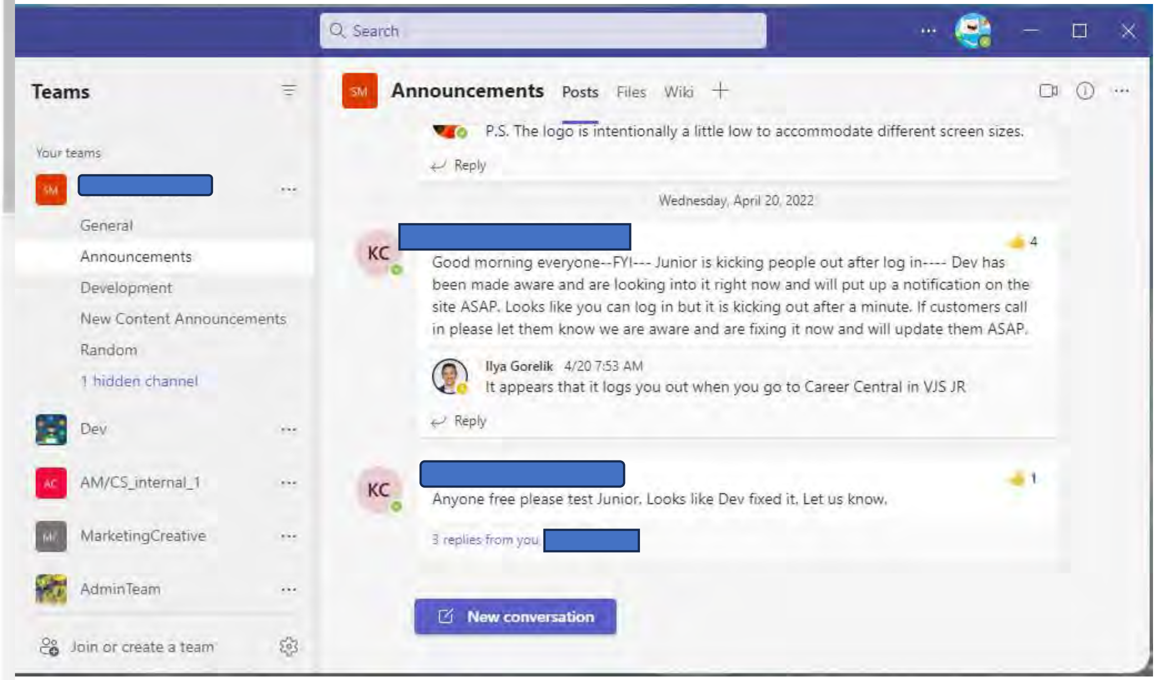
A specific feature ***after you have logged in*** does not work

Call Tree

If you become aware of a **security or data breach** in any Strivven Media product that is live, or a **service outage** that affects any live Strivven Media product the **first thing to do** is to alert the Outage Response Team by phone at 888-908-4924 ext 66 and then by email (Outage Response Team).

Do both. You call to provide the alert and then you email to provide the details.

IF you do not talk to someone on that call you have not completed the action! IF you ended up in a voicemail box escalate to your team lead immediately.



[redacted]

P.S. The logo is intentionally a little low to accommodate different screen sizes.

Reply

Wednesday, April 20, 2022

KC [redacted]

Good morning everyone--FYI--- Junior is kicking people out after log in---- Dev has been made aware and are looking into it right now and will put up a notification on the site ASAP. Looks like you can log in but it is kicking out after a minute. If customers call in please let them know we are aware and are fixing it now and will update them ASAP.

👍 4

Ilya Gorelik 4/20 7:53 AM
It appears that it logs you out when you go to Career Central in VJS JR

Reply

KC [redacted]

Anyone free please test Junior. Looks like Dev fixed it. Let us know.

👍 1

3 replies from you [redacted]

New conversation

Critical Response Plan

Today's definitions

1. **Outage**
   a. **What it is, what it means, and what to do.**
2. **Critical Bug**
   a. **What it is, what to do.**
3. **Data Breach**
   a. **What it is, and what to do.**

Critical Response Plan

Process:

1. **Check Teams - General Announcements if it is already reported**
2. **If it’s not reported – Report It**
   1. **Call Tree**
   2. **E-mail**
3. **Proper messaging to customer**
   1. **Thank you for reaching out to us!**
   2. **Proper Follow-up**

Critical Response Plan

Site Down messaging:

- Thank you for reaching out to us!
- Our development and support teams are aware the platform is currently unavailable and is currently working to restore the service.
- We apologize for any inconvenience. We will notify you as soon as the systems are restored.

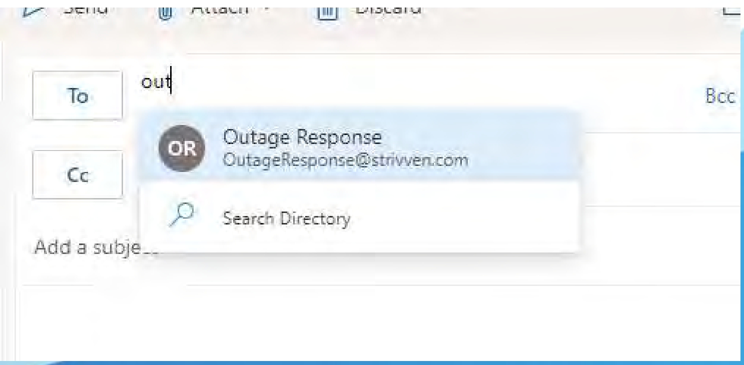
Security / Data Breach messaging:

- Thank you for reaching out to us!
- We are aware of the issue and will notify any party impacted.
- If you have not been notified, your data was not exposed or impacted.

Critical Response Plan

Plan:

1. **Check on Teams General Alerts if the issue has been reported.**
2. **If not - Alert the Outage Response team by phone at** [redacted]
3. **Email Outage Response Team**
   - **Security / Data Breach and Outage Response Plan**



To: out

Outage Response
OutageResponse@strivven.com

Critical Response Plan

Gather and share the information:

1. Behavior being reported
2. Any available contact information for the reporter
    a. Contact person, school, district, license,
    b. Which Platform
    c. Time of discovery
    d. How they discovered it
3. Data Breach? (all of the above, and)
    a. Why do they believe their data is compromised?
    b. How did they discover it?

Discussion

Any questions or concerns to raise for the basic submission process and how it's managed?

This Photo by Unknown Author is licensed under CC BY-SA-NC

Related Links

Links

Google Phishing Quiz

[redacted]

OUR MISSION

To inspire individuals [redacted]

[redacted]