FILED UNDER SEAL

EXHIBIT 12

SEV Definitions (fburl.com/SEVdefinitions)

SEV is an acronym that stands for **S**ite **EV**ent and is used at Meta to refer to what is more commonly called an incident in *incident response processes*. This page outlines the general company-wide patterns we use to determine the SEV Level; individual teams may have more specific examples.

General Guidelines

IF IN DOUBT, ERR TOWARDS FILING A SEV

There is no company goal to reduce the number of SEVs we create, because this would result in people being afraid to file legitimate SEVs thinking it would look bad for them or their team. *This is not true!* We aim to not have the same SEV multiple times, and we learn from prior incidents by participating in SEV Review. As long as we keep coming up with new and interesting ways to break stuff, keep filing SEVs!

DON'T BE AFRAID TO "ROUND UP" IF YOU'RE UNSURE.

It's better to get more eyes on a small problem than to have fewer eyes on a big problem. Depending on the actual impact of the event, the owner or Incident Manager On-Call may upgrade/downgrade the assigned SEV level.

THE SEV LEVEL REPRESENTS THE HIGH WATERMARK OF THE ISSUE, NOT THE CURRENT STATUS.

The SEV should never be downgraded to reflect progress in resolving the SEV. It should only be downgraded if the initial assessment of severity was inaccurate. It's also OK to leave a SEV at a more severe level if the response was handled with that level of urgency, even if we discover later that the issue wasn't so bad.

SEV Levels

SEVs are defined in terms of it's level of impact where SEV0 is most severe and SEV4 is a "heads up". The following cards define what these levels mean, when to declare each, and some examples of past SEVs for each level.

SEV0

Company-level crisis

Outage that substantially impairs two or more major products or that substantially impairs a single major product for an extended period of time.

We define a SEV0 as an incident that affects our Family of Apps (Facebook, Messenger, Instagram, and WhatsApp) such that:

1. two or more products are severely impacted for a majority of users or
2. one product is completely unavailable or
3. an ongoing incident is at risk of progressing to meet the above criteria.

A SEV0 can only be declared by the Main Site IMOC, CMOC, or Web Foundation. The declarer should cross check declarations with at least one other member of the groups above.

We use SEV0 sparingly. We hope to need it less than once per year, so when you see one, we are having a major outage.

Examples include:

- Oct 25 2022: S304356 - Whatsapp Down
- Oct 6 2022: S300185 - ENOINT: Everstore i32 volume ids exhausted
- Oct 4 2021: S245757 - Access Denied
- April 8 2021: S227979 - S123
- Mar 19 2021: S225911 - InstaGK
- Dec 10 2020: S217912 - SendLocked
- Sept 17 2020: S210252 - SEV1000
- Apr 1 2020: S198911 - Vip Switch

BETA

- Mar 13 2019: S174900 - Infinite Loop
- Nov 20 2018: S169223 - CAPSLOCK
- Jan 27 2015: S107812 - Silent Night
- Aug 1 2014: S110576 - Call the Cops

Check the SEV0 FAQ for more detail.

SEV1

Red alert! All Hands on Deck!

A major system outage with a large number of users affected.

Examples include:

- Outage of one entire Meta product or service (ie. WWW, Messenger, WhatsApp, Instagram and others)
- Datacenter outage ("PRN1 has lost power", "LLA has lost connectivity")
- Major portions of the site are unavailable ("Feed is down")
- Outages that impact multiple products/services
- Privacy and security issues/bugs that affect very sensitive data or a large number of users
- Issues bad enough to get picked up by the press
- `> 30%` drop in egress
- Example: 92% of offline AI Training jobs are failing

SEV2

Major problem, resolution is very high priority.

An important service is exhibiting intermittent failures, is partially down or degraded, and affects numerous customers.

Examples include:

- Service outages that impact a particular Meta feature ("Multifeed failing, fallback feed served to users")
- Service issues in multiple regions
- Regional network impairment
- `>15%` drop in egress
- Internally disclosed privacy issues (e.g. employee-discovered or whitehat) that affect a moderate number of users, or have the potential to affect a larger number of users but aren't because of a mitigating factor
- Critical internal tools like `Intern` are down, putting the site at risk.
- Large drop in payments.
- Personal Safety of Minors, Kids, or other targeted groups (such as Women, LGBTQ community) is at risk: privacy protections, safety precautions impacted, and/or minors more discoverable or reachable by adults

SEV3

Significant problem, resolution is moderate or high priority.

The issue affects a minimum number of customers, and does not prevent normal operation of production services.

Examples include:

- Redundant/contained system failures
- Loss of DR buffers, or other impairment that prevents DR-readiness - additional reading on Disaster Recovery
- System impairments that do not impact or only minimally impact customer experience ("Service X is running hot due to performance regression")
- Bugs with high levels of user reports reported by CO

BETA

- Privacy perception issues that affect only a small number of users. E.g. no violation occurred but it may appear as if one did, or audience was unintentionally decreased instead of increased
- Internally disclosed privacy issues (e.g. employee-discovered or whitehat) that are difficult to exploit and affect very few users

SEV4

"A heads up"

Used to raise visibility of a risky activity occurring. E.g. Planned or Unplanned maintenance

SEV4s are used to raise visibility that a risky activity is occurring. Examples include: a data center maintenance, or migration of a critical system.

Planned maintenance

- Planned physical maintenance that increases the risk to production, but is not expected to have impact
  - A warning/heads up that facilities operations is conducting maintenance which could lead to a higher level SEV and impact to other teams
  - FYI only for all other teams
  - Facilities Operations is in control of communication, reporting updates, and closing SEV4
  - We risk losing a critical power path power through the reduction of redundancy
- A change that risks impacting many users, employees, or systems.
  - For example, a major migration on a shared software service.
- These issues may escalate to a higher level of SEV if actual impact occurs. For example, when a facilities maintenance becomes an "unplanned event."
  - Upon transition to unplanned maintenance, Facility Operations reports specific issue to Site Operations on call, who escalates and notifies as necessary
  - Site Operations determines the if there is a need for escalation in SEV level and takes ownership of the existing SEV

Unplanned Maintenance

- *Low risk unplanned maintenance* that may escalate to a higher SEV

Data Loss

Losing customer data is probably a SEV. If in doubt, ***OPEN A SEV***. This goes for about anything. If you think it's that bad, it probably is. Use your best judgment, and you will self-calibrate as you go on.

Use the appropriate level based on how bad it seems to be. Adjust it according to the actual impact as that becomes known.

SEVs affecting SEV Manager

We can find ourselves in situations where major SEVs (likely a SEV0 or SEV1) take down SEV Manager.

To mitigate this, we have a CLI on every laptop called ohno. We also use MatterMost to communicate on about SEVs; MatterMost is deployed outside of Meta Infra.

Team-Specific SEV Criteria

Top-level guidelines can never describe the specific needs of teams around the company. Many teams have taken the top level guidance and interpreted it into specific criteria that make sense for them. This is encouraged! Feel free to link your team's SEV Criteria here.
Team-specific SEV Criteria

- Ads SEV Guidelines
- AI Infra SEV Guidelines
- A&I (Avatars & Identity) SEV Guidelines
- Continuous WWW SEV Guidelines
- Data Eng SEV Guidelines
- DataInfra SEV guidelines
- Developer Platform SEV Guidelines

- FB Lite SEV Definitions
- Fleet Sev Definitions
- Infra Data Centers · SiteOps SEV Runbook
- Instagram SEV Guidelines
- Internet.org SEV Guidelines
- Messenger SEV Levels
  - RTC Criteria
- NetEng SEV Definitions
- Oculus SEV Definitions
- Pages SEV Guidelines
- Payments SEV Guidelines
- Platform SEV Definitions
- Portal SEV Guidelines
- Privacy SEV Definitions
- SEO SEV Guidelines
- Search SEV Guidelines
- Security SEV Definitions
- Internal Security SEV Definitions and Guidelines
- Storage Mgmt Hardware SEV Guidelines
- Traffic SEV Guidelines
- Tupperware SLA and SEV Guidelines
- WhatsApp SEV Level Criteria
- Workplace Escalations

« Data Use SEVs SEV Types & Status »

SEV Incident Management