The security working group is proposing this policy around disclosure of private information. We are seeking community feedback.

In the past our policy has been a tad thin. *"State that you are willing to keep the confidential issues of the team confidential"*

This document aims to add clarity to that sentence and some example scenarios to guide team members decision making.

We want to avoid a few scenarios:

- Having a security issue leaked beyond the team and posted to the public, outside of the release window and before a patch is released.
- Creating a situation where people use still-private knowledge gained on the team to get an unfair advantage with no regard for the health of the Drupal ecosystem.

In general, information shared within the Drupal security team should only be shared outside the team on a "need to know" basis. If knowledge of team information will allow actors to create a patch or provide direct support to the security team in fixing an issue, this satisfies "need to know" and the actors should be invited directly to the issue. Offering team information to give actors advance knowledge of a supported patch release does not satisfy "need to know" (e.g. letting an organization know about a zero day for purposes of operational preparedness).

Some examples of common situations and how to handle them:

- If a team member wants to get sponsored time from their employer to spend more time moving the issue forward, it's appropriate to provide their manager with a statement like "there is a serious vulnerability that affects code we frequently use. I would like to spend six hours working on it to help write a patch." However, do not give details as to what the exact security issue is.
- If a team member wants to enlist the help of a colleague who has expertise in the area that is affected, it's appropriate to add them directly to the issue so the colleague can review and collaborate with the team. Security team members should confirm a person is approved to contribute to the issue by asking at least one other team member (who does not work at the same company/organization) before inviting that person to the issue.
- Do not use private information gained via the security team, or privileged access to that private information, for marketing purposes. In other words, marketing people should not write posts about your activity. Do not allow your company to market the fact that you have advance access to information. Instead, focus marketing on how contributing to the team has improved your organization's handling of security issues across a wide variety of situations. This is not to conceal that you have access to team information, but rather to prevent misunderstandings when non-technical people read and write about technological topics.

If your use case is not covered, here, ask the team: security@drupal.org

If you feel the need to discuss an issue to help resolve the issue, it is generally acceptable to share the following information with a colleague or community member outside of the security team:

- Any information that is already public, e.g. a release window.
- The numeric criticality of the issue (e.g. 20/25).

It is generally **not** OK to share outside of the security team/security team issue tracker:

- The specific project that is affected (e.g. Core, Views).
- The nature of the vulnerability (e.g. SQL Injection, XSS).
- Specific ways to mitigate the issue.
- Any other details related to the vulnerability or the sites it might affect.

A security team member can request an exception to this policy by emailing the security team. The security team member should include, why they want the exception, how the exception benefits the Drupal community, and how they will mitigate the risk if any is created by the exception. The security team will make allowed exception requests public at a time when there is no risk to doing so. When deciding on exception requests, team members should indicate if they have a COI. If there is not consensus, the request will be escalated to the security working group.

Conflict of Interest Policy when adding team members:

If you comment on an application to become a team member AND you have a potential conflict of interest (e.g. you are employed by a competitor of the applicant) then you should explicitly disclose that fact prior to casting a vote. You should also give specific reasons why you think the person is or is not a good candidate (this is true regardless of any conflict of interest).