

Islandora Security Response Team (ISRT)

1. A member of the islandora community discovers a security concern and sends a summary to the security@islandora.ca mailing list.
2. The response team lead will respond to person and gather more information on the reported issue.
3. Create a Duraspace Ticket, tagged as security or sensitive (TBD)
4. The response team lead will convene an ISRT call within 2 business days of the original report. This call will involve the Repository maintainer to include their knowledge of the module and share the issue.

A determination if any additional people should be included in the call and or resolution development

- Coordinating Committee member(s)
- TAG Member(s)
- Committer(s)
- Other

Only private communication channels will be used until the fix is public. It doesn't have to be encrypted, but don't talk about anything on social media.

5. Develop an initial security assessment report of the risk and impact as defined by the Drupal [security risk levels](#).
6. If the Repository maintainer isn't involved, an ISRT member will be assigned as the tester and is excluded from code development for this fix
7. Send initial report to a representative of the Islandora Foundation.
8. Develop a fix with the decided parties
9. Provide a fix in the form of a patch or an update to repository associated with the incident. README.md will be update if needed.
10. The assigned tester will test the patch when ready
11. Once the assigned tester signs off on patch, a notification will be sent to the Islandora mailing list and the security notifications list using the below guidelines
 - a. Patch notifications come out approximately one week before the patch is released
 - b. Patches are released on Wednesdays only.
 - c. Notifications do not disclose any information but does disclose the public risk level determined in step 5 above.
12. A member that worked on the code will submit a Pull Request. The Pull Request will not specify ticket.
13. The assigned tester will Merge Pull request immediately.
14. A final report will be sent to ISIG and a representative of the Islandora foundation

- Note: The only communication required to be public is the Duraspace ticket after fix is accepted and will be done by a representative of the Islandora foundation

ISRT Team Makeup

1. The team will be made up of around 4-6 members.
2. Membership on the ISRT is a one year term.
3. Membership renews every year in July by email.
 - a. If the member doesn't respond to the renewal email they are assumed to be no longer interested in volunteering for the ISRT responsibility.
4. Team Lead role will move to the next person each year.
5. Membership is secret, but members know each other
6. The list of members and who the team lead is will be known to the Islandora Foundation employees.
7. When a member departs from the ISRT, the remaining members of the team nominate their replacement in coordination with the Islandora Foundation.