Uchaguzi Privacy and Security Guidelines

Privacy and Security Guidelines

The privacy and security of the public, our partners, and our team members is of the utmost importance to the Uchaguzi team and to Ushahidi.

As such, we have developed these guidelines for our core team to include as part of the training of all volunteers, across all levels and responsibilities. This page is an introduction to our security goals, recommendations, and general requirements for all volunteers. More explicit instructions on submitting, managing, and publishing data from the public and our partners are included elsewhere on the wiki (links forthcoming).

Uchaguzi Access and Training for All Team Members

We are asking all reporters and Partners to review and agree to our Code of Conduct (or, lightly put, Code of Collaboration) before engaging with the platform and the project.

In addition, each team member working with data submitted to the Uchaguzi platform requires training and scheduled times for their assigned tasks. According to their assigned tasks, each member will have a set access level. Heather Leson and Angela Odour from Ushahidi are managing these access levels.

While anyone can create an account to have a "member" status, they will only be able to view their reports submitted. All other Uchaguzi access tiered will have various levels of permissions pertinent to their assigned tasks. Only the Superadmins, Admins, Verification, and Reports team members will have the right to approve reports that can be viewed by the public at https://uchaguzi.co.ke.

Guidelines for reviews, admins, reporters when securing their own browser

1. Remain logged out as much as possible
    a. Only login when you are actively reviewing reports
    b. Avoid doing other tasks while reviewing reports
    c. This reduces risk of various hijacking attacks
    d. Always log out when you're done. Don't leave your computer logged in and unattended
2. Check the URL:
    a. It should be: https://uchaguzi.co.ke
    b. Is the certificate valid? You shouldn't receive browser warnings and you should see a green padlock next to the URL.
3. Use a secure password? How to create secure passwords
4. Avoid logging in to the site from public or untrusted connections
5. Avoid keeping copies of sensitive info. For example: don't edit reports in a word doc.
6. Install NoScript for Firefox or NotScripts for Chrome
    a. Detailed guide to Firefox security addons
7. If possible: use Tor when accessing the Uchaguzi admin

Our Submission, Review, and Verification Process

Questions to consider when posting (reviewing) a report to Uchaguzi

1. What private information is in the message? Should it be included or excluded?
2. Will publishing this report endanger the reporter?
    a. Will the reporter be safer if I delay publication? (to avoid clearly and immediately identifying a victim)
3. Is the report urgent or an emergency?
    a. Have I contacted the emergency desk of my team lead?
    b. Should the item be posted or removed?
    c. Should certain partners also be contacted?
4. Am I working in a secure location? Is my password ok? How to create secure passwords
5. Are there any URLs in the report? Are these reports suspicious? Should they be removed?
6. Is there any code / HTML in the report? This should be removed.
7. ....

Additional Resources

Tips from the Uchaguzi 2010 Case Study

on Security & Privacy:
"The ability to create questionnaires gets people to start thinking about the security that I think needs to be a standard set of questions that people ask for in any installation at all. While the issues of information security, privacy and the possibility of retribution for sharing information was not a major issue in the Uchaguzi- Kenya project; it may play a very large role in other election monitoring projects that use Ushahidi or Crowdmap. Risks to people systems and organizations are constantly evolving approaches to security privacy will need to be regularly evaluated."

A security and privacy review should begin with:

- A discussion of potential risks to the crowd and organizations if they use the platform
- Plans on how to keep technology hardware (e.g., servers) safe and secure
- Plans for how volunteers and others should be trained to keep information private and secure, if necessary
- A contingency plan for security and privacy related events.

Materials

- Security FAQ
- Security Research
- Security in a Box (Tactical Tech)
- “Securing Crisis Maps”, written by Rob Baker and George Chamales is a helpful infographic that shows different areas of information, security and privacy risks.
- “Crisis Mapping and Cybersecurity” by Anahi Ayala Iacucci describes one approach to addressing these issues
- Questions from Toolbox 1, Slide 16 “ICT, Privacy & Security” can also be used as a guide to think about these issues in election monitoring projects.CrisisMapping and CyberSecurity - Part III (Security is Knowledge) * - article by Anahi Ayala Iaccuci

We also recommend that you review George Chamales' Security Webinar: