Security Policy

Thank you for taking the time to help keep **MacroIBI** secure.

This document explains what potential security issues may arise, how to report them, and what you can expect in return.

Potential Security Concerns

MacroIBI is designed for ecological data processing and does not handle authentication, financial information, or sensitive personal data. As such, the overall security risk of the project is low. However, several realistic concerns may still arise depending on how the app is deployed or used:

1. Accidental Data Exposure

Although MacroIBI typically processes non-sensitive biological and survey data, users may upload internal reports or unpublished results that they do not intend to be publicly accessible. If the app is deployed on a public server or is misconfigured, uploaded data could be exposed to unintended parties.

2. Multi-User Session Interferance

Shiny applications can share underlying resources across sessions. If MacroIBI is hosted centrally (e.g., on Shiny Server or shinyapps.io), simultaneous users may unintentionally interact with shared autosave files or temporary directories, potentially overwriting or accessing each other's session data.

3. File Handling Risks

The application reads user-supplied files and writes outputs such as reports and autosaves. Improper handling of file paths or untrusted filenames may create opportunities for directory traversal or overwriting files outside the expected scope, depending on the hosting environment.

4. Dependency-Related Vulnerabilities

MacroIBI relies on the Shiny framework and several R packages that introduce HTML, JavaScript, LaTeX, and system-level rendering tools (e.g., `webshot`). Vulnerabilities in these dependencies could indirectly impact MacroIBI, including risks such as HTML/JS injection or unsafe interpretation of user-supplied content.

5. Misconfigured Deployment Environment

MacroIBI is intended for use in trusted or internal environments. If it is deployed without proper protections—such as running on a public-facing server without authentication, firewall controls, or HTTPS—users may inadvertently expose internal data or allow unauthorized access to the application.

Supported Versions

MacroIBI is a small, research-focused project. Security fixes are generally only applied to the latest released version.

Version	Security Updates
1.x	✔ Active
0.x	✖ Not supported

If you are using an older version and discover a security issue, please try to reproduce it with the latest release before reporting.

Reporting a Vulnerability

If you believe you have found a security vulnerability in MacroIBI, **please do not open a public GitHub issue**.

Instead, contact the maintainer directly:

- **Preferred:** Email the maintainer at: `sam.swanson@shakopeedakota.org`
- **Subject line:** `[MacroIBI] Security report`

Please include, when possible:

- A clear description of the issue
- Steps to reproduce the problem
- Any proof-of-concept code or screenshots
- Your operating system, R version, and MacroIBI version
- Any thoughts on potential impact or severity

What to Expect

When you report a vulnerability:

1. You will receive an acknowledgment.
2. The issue will be investigated and, if confirmed, a fix will be prepared.
3. Once a fix is available (and ideally released on CRAN/GitHub), a short security note may be added to the release notes or NEWS file.
4. If you would like to be credited, your name or handle can be included in the release notes.

Please do not publicly disclose the details of the vulnerability until a fix has been released or we agree on a timeline.

Data Handling & Threat Model

MacroIBI is an R package containing a Shiny app designed for ecological / macroinvertebrate data analysis. It is typically run:

- Locally on a researcher's machine, or
- On a Shiny server / shinyapps.io for internal use.

Important notes:

- MacroIBI does **not** implement its own user authentication, authorization, or multi-tenant security model.
- The app is intended for **trusted environments** (e.g., internal networks, personal machines).
- Do **not** expose the app directly to the public internet without additional protections (reverse proxy, authentication, HTTPS, etc.).

MacroIBI does not intentionally collect or transmit sensitive personal data. Any data loaded into the app remains under the control of the user and/or hosting environment.

Dependencies

MacroIBI relies on various R packages and the Shiny framework.

- Many security-relevant issues may originate in dependencies (e.g., Shiny, webshot, DT, etc.).
- If you believe a vulnerability affects a dependency rather than MacroIBI itself, please consider reporting it upstream as well.

Out of Scope

The following are generally **out of scope** for security reports:

- Issues caused solely by misconfigured hosting environments (e.g., unencrypted HTTP, open admin ports).
- Problems in forked branches or heavily modified versions of the app.
- Denial of Service caused by intentionally extreme or unrealistic input sizes beyond typical workflows.

If you are unsure whether something is in scope, you should still send a report.

Responsible Use

If you are testing MacroIBI for security issues:

- Only test instances you own or have permission to test.
- Avoid actions that might disrupt work for other users.
- Do not attempt to access data without authorization.

Thank you again for your interest in the MacroIBI app!