

## RESPONSIBLE DISCLOSURE POLICY

**1. General Information.** The SiteLock, LLC (“SiteLock”) Responsible Disclosure Policy details the process by which SiteLock publicly discloses vulnerabilities found during research and malware cleaning processes. The Policy reflects SiteLock’s dedication to a secure web for all site owners and developers, and stresses privacy and the protection of sensitive data.

### 2. Guidelines

It is required that all SiteLock researchers:

- Analyze publicly available code bases, or purchase a copy of licensed code for analysis
- Verify proof of concept exploits on internal test systems
- Understand and adhere to the SiteLock Responsible Disclosure Policy in all steps of the research process

SiteLock commits to developers and site owners to:

- Work with the responsible party to understand and resolve issues quickly, including providing screen shots, code examples, and proof of concept code
- Make every effort to avoid privacy violations
- Recognize efforts to mitigate reported vulnerabilities

SiteLock will not perform security research in the following areas:

- Physical security testing such as building access
- Social engineering tests such as phone calls and spear phishing
- Non-public, proprietary code bases
- Network level attacks or denial of service

### 3. What SiteLock Includes in a Vulnerability Disclosure

SiteLock will strive to provide comprehensive and succinct vulnerability reports to developers which include:

- The description and impact of the vulnerability, including file paths and names, lines of code, and resultant files
- A detailed description of the steps required to reproduce the vulnerability
- Contact information for the researcher and company contact information

**4. Timeline for Disclosure.** SiteLock will provide 30 days from the date of report for developers to respond and mitigate vulnerabilities. Developer requests for disclosure extension will be honored. SiteLock will adhere to the 30 day guideline if there is a lack of or cessation of developer response.

This policy was adapted with changes from the [Open Source Responsible Disclosure Framework](#) using the [Creative Commons Attribution 4.0 International License](#).