

Practice-Web Dental Responsible Disclosure Policy

Effective Date: May 20, 2025

Last Updated: May 20, 2025

Practice-Web is providing this service to help ensure a safe and secure environment for all users.

If external parties find any sensitive information, potential vulnerabilities, or weaknesses, please help by responsibly disclosing it to ResponsibleDisclosure@fullsteam.com.

This policy applies to Practice-Web hosted applications and to any other subdomains or services associated with products. Practice-Web does not accept reports for vulnerabilities which solely affect marketing websites practice-web.com, containing no sensitive data.

Security researchers must not:

- engage in physical testing of facilities or resources,
- engage in social engineering,
- send unsolicited electronic mail to Practice-Web users, including “phishing” messages,
- execute or attempt to execute “Denial of Service” or “Resource Exhaustion” attacks,
- introduce malicious software,
- execute automated scans or tools that could disrupt services, such as password guessing attacks, or be perceived as an attack by intrusion detection/prevention systems,
- test in a manner which could degrade the operation of Practice-Web systems; or intentionally impair, disrupt, or disable Practice-Web systems,
- test third-party applications, websites, or services that integrate with or link to or from Practice-Web systems,
- delete, alter, share, retain, or destroy Practice-Web data, or render Practice-Web data inaccessible, or,
- use an exploit to exfiltrate data, establish command line access, establish a persistent presence on Practice-Web systems, or “pivot” to other Practice-Web systems.

Security researchers may:

- View or store Practice-Web nonpublic data only to the extent necessary to document the presence of a potential vulnerability.

Security researchers must:

- cease testing and notify us immediately upon discovery of a vulnerability,

- cease testing and notify us immediately upon discovery of an exposure of nonpublic data, and,
- purge any stored Practice-Web nonpublic data upon reporting a vulnerability.

Thank you for helping to keep Practice-Web and our users safe!

