

Acceptable Use Policy (Web Software Services)

This Acceptable Use Policy ("Policy") governs your use of the Web Based Hosted Software Services ("Services") provided by PenRad. If you engage in any of the activities prohibited by this POLICY, PENRAD may suspend or terminate the Services. The POLICY is a nonexclusive list of the actions prohibited by PENRAD. The use of PENRAD Services constitutes the understanding and acceptance of the POLICY.

No Illegal, Harmful, or Offensive Use or Content. You may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include:

Illegal Activities. Any illegal activities, including HIPAA violations, copying, taking pictures of or communicating, releasing PHI to anyone or entity not approved to have, see, or use the PHI. Any other illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting, facilitating, displaying, performing, sending, receiving or storing any content that is obscene, pornographic, lewd, lascivious, or excessively violent, regardless of whether the material or its dissemination is unlawful. Prohibited activities also include advocating or encouraging violence against any government, organization, group, individual or property, or providing instruction, information, or assistance in causing or carrying out such violence, regardless of whether such activity is unlawful.

Harmful or Fraudulent Activities. Activities that may be harmful to others, our operations or reputation, including without limitation offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming), obtaining unauthorized access to any system, network, service, or account, or engaging in other deceptive practices.

Infringing Content. Content that infringes or misappropriates the intellectual property, privacy, or proprietary rights of others, including without limitation, accessing, sending, receiving, displaying, performing, disclosing, storing, or executing any content a) in violation of any copyright, right of publicity, patent, trademark, service mark, trade name, trade secret or other intellectual property right, b) in violation of any applicable agreement, or c) without authorization, or deleting or altering author attributions, copyright notices, or trademark notices, unless expressly permitted in writing by the owner.

Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable.

Harmful Content. Interfering with service to any user, site, account, system, or network by use of any program, script, command, or otherwise, and content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

No Network Abuse. You may not make network connections to any users, applications, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

Resale of Services. Reselling PENRAD Services, in whole or in part, to any entity or individual, without prior written consent of PENRAD, or misrepresenting your relationship with PENRAD.

Monitoring or Crawling. Monitoring or crawling that impairs or disrupts the system being monitored or crawled.

Denial of Service (DoS). Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.

Intentional Interference. Interfering with the proper functioning of any system, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

Operation of Certain Network Services. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on a system, such as access and storage restrictions.

Load Testing. Any test with the purpose of placing traffic or load on the system to stress the system utilizing automated tools or manual means without the explicit authorization of PENRAD.

No E-Mail Abuse. You will not distribute, publish, send, or facilitate unsolicited mass e-mailings, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. You will not collect replies to messages sent from an Internet service provider if those messages violate this POLICY or the acceptable use policy of that provider.

No Security Violations. You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.

Interception. Monitoring of data or traffic on a System without permission.

Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

Hacking. Circumventing user authentication or security of any application, host, network, or account; nor interfere with service to any user, host or network (referred to as "denial of service attacks").

Acceptable Use Policy (Web Software Services)

Monitoring and Enforcement

PENRAD, in its sole discretion, will determine on a case-by-case basis what actions will be taken in response to a violation of this POLICY. PENRAD reserves the right to investigate suspected or alleged violation of this POLICY, including gathering information from Customer, the complaining party, and examining of material on PENRAD servers. Nothing contained in this policy shall be construed to limit PENRAD'S actions or remedies in any manner. PENRAD reserves the right to take any and all additional actions it may deem appropriate with respect to such activities, including without limitation taking action to recover the costs and expenses of identifying offenders and barring their access to its Services and levying cancellation charges to cover PENRAD costs in the event of termination for the causes outlined above. PENRAD reserves at all times all rights and remedies available to it with respect to such activities at law or in equity.

POLICY Changes or Modifications. PENRAD reserves the right to amend, alter, or modify this POLICY at any time. Any amendment or modification is effective when posted and any use of its Services after the posting of a modification or amendment will be considered acceptance of those modifications.

Reporting of Violations of this POLICY. If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please contact PENRAD by telephone at (763) 475-3388.

Customer must immediately notify PENRAD of any breach, or attempted breach, of security known to Customer.

Customer is responsible for ensuring that connections or interfaces are configured in a secure manner. Customer may not, through action or inaction, allow others to use PENRAD Services for illegal or inappropriate activities.

Customer Responsibility for Customer's Users. Each Customer is responsible for the activities of its users and, by accepting service from PENRAD, is agreeing to ensure that its customers, representatives, or end-users abide by this POLICY. Complaints about customers, representatives, or end-users of a Customer will be forwarded to the PENRAD Customer's primary contact for action. If violations of the PENRAD POLICY occur, PENRAD reserves the right to terminate services with or take action to stop the offending customer from violating PENRAD'S POLICY as PENRAD deems appropriate, without notice.

Effective Date: 05/2020