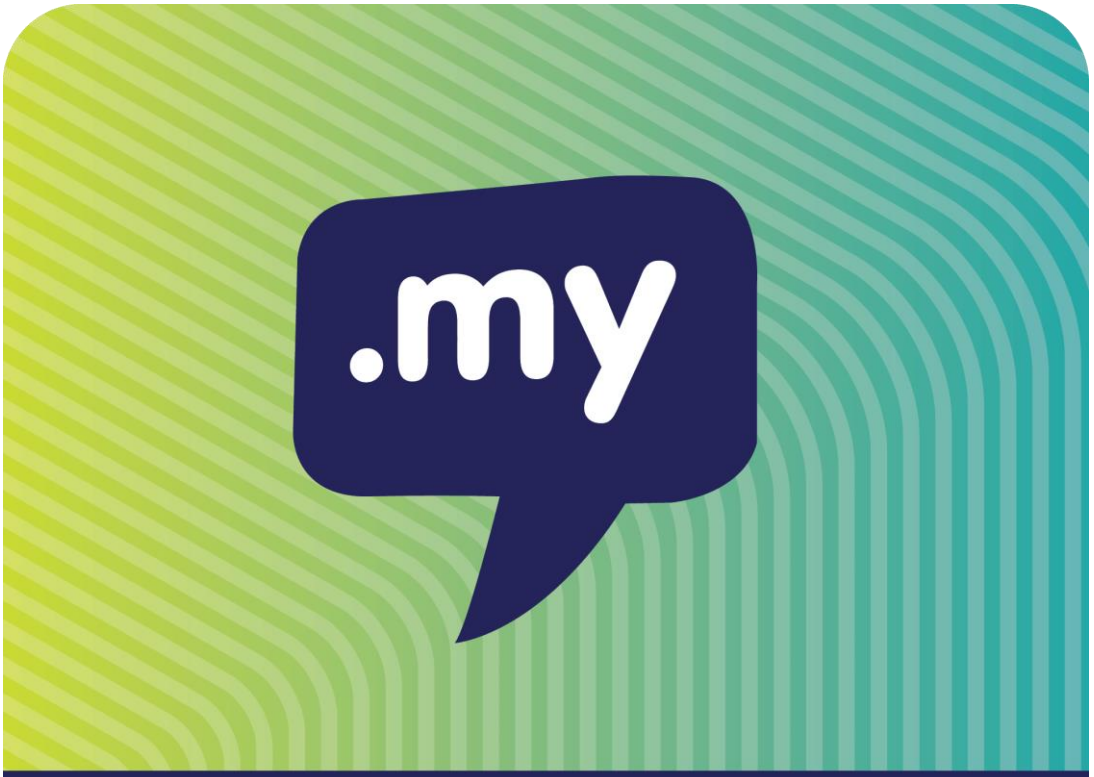

Acceptable Use & Abuse Policy

Effective 15 May 2025

.myNIC

Contents

1. Introduction and Purpose

1.1 MYNIC is the Registry for the top-level Malaysian Internet Domain, ".MY", whose core business is the registration of domain names, administration, and technical operation of the national domain registry as well as promoting the positive development of the Domain Name System ('DNS') in Malaysia.

1.2 The purpose of this Policy is to set rules, general principles, and procedural steps governing how the Registrant may or may not use the registered domain names for any illegal purposes in contravention to the Malaysian law.

1.3 The Policy is also an integral part of the framework of information security policies and would define the sanctions that will be applied if a user breach any of the terms and conditions of the Policy or in violation to any of Malaysian laws and regulations.

2. Scope

2.1 This Policy applies to all .MY domain names registration and must be complied by both Registrars and Registrants including but not limited to all other policies that is made available in MYNIC official website as well as the Malaysian Communications and Multimedia Content Code.

3. Definition of Terms

No.	Term	Definition
3.1	Abuse	Abuse of a domain name generally refers to any illegal, disruptive, malicious, fraudulent, or deceptive action.
3.2	CMCF	Content Forum of Malaysia.
3.3	MCMC	Malaysian Communications and Multimedia Commission.
3.4	MYCERT	Malaysia Computer Emergency Response Team.
3.5	NEAP	Numbering and Electronic Addressing Plan (Section 13 Domain Names). This is a Plan established under subsection 180(1) of the Communications and Multimedia Act 1998 [Act 588] that applies to all Licensees, Registrars, Resellers, and Registrants.
3.6	POTA	Prevention of Terrorism Act 2015.

No.	Term	Definition
3.7	Registrant	Refers to an individual or entity who registers a domain name with the respective Registrar.
3.8	Registrar	Refers to an entity that offers domain name registration services to Registrants.
3.9	Registry	Refers to persons or entities responsible for providing registry services which include customer database administration, zone file publication, DNS and DNSSEC operation, marketing, and Policy determination.
3.10	SMATA	Special Measures against Terrorism in Foreign Countries 2015.
3.11	SOA	Security Offences (Special Measures) Act 2012.

4. General Principles

4.1 This Policy is developed in relation to the .MY domain name Policy. As and when required, the Policy shall be updated accordingly to reflect any changes in either internal or external circumstances to avoid conflicts or inconsistencies.

4.2 The Policy shall be reviewed in its entirety on an annual basis or as and when required to ensure its contents' continued relevance and appropriateness.

4.3 The Acceptable Use & Abuse Policy contains proprietary information of MYNIC. The Acceptable Use & Abuse Policy and any of the information contained therein shall not be reproduced and/or disclosed under any circumstances without the express written permission of MYNIC.

5. Registrant Obligations

5.1 Prior to registering a .MY domain name, the Registrant shall ensure:

5.1.1 The domain name applied is in compliance with the relevant Malaysian laws and regulations;

5.1.2 The domain name applied for is not scandalous, indecent, obscene, offensive, or against the Malaysian public norms and values whether directly or indirectly in any manner whatsoever;

5.1.3 The content of the website does not misrepresent any specific eligibility criteria requirements of the domain name that was applied for under the NEAP;

5.1.4 To obtain the necessary consent and/or approval from the State Secretary's for domain names that fall within the category of reserved names under the Malaysian laws and regulations;

5.1.5 The registration or use of the domain name is not for any illegal and/or unlawful purposes and does not infringe the right(s) of any party or any other intellectual property rights of a third party;

5.1.6 The domain name is directly related to the lawful content, goods and/or services provided by the resolving website;

5.1.7 All information in the application for domain name(s) is complete, correct, and accurate as at the date of submission and shall always continue to update the domain contact information; and

5.1.8 The suitability of the persons chosen to act for contact purposes as stated in the domain name application requirements are met.

6. Registrar Obligations

6.1 The Registrar shall ensure the following obligation to the Registrants:

6.1.1 Registrant's compliance to the NEAP issued by MCMC under the CMA 1998;

6.1.2 Verify the identity of their customers while processing the registration of any Product or Services including request copies of documents to verify customers identity or contact information such as National IDs, Company/Business Certificate, utility bills, etc;

6.1.3 To provide accurate, correct and complete registration information for domain names, and immediately correct and update the Registrant's information upon notification by the Registrant in a timely manner;

6.1.4 To carry out random checks on the accuracy of the information provided by the Registrants on a yearly basis;

6.1.5 To send WHOIS data reminder notification to Registrant via email at least once a year to ensure all the information provided by the Registrant is complete, correct and accurate;

6.1.6 To provide support to Customers including but not limited to receiving and responding to queries and applications for registration, cancellation, modification, renewal, deletion or transfer, complaints, managing billing and collection as well as technical support;

6.1.7 To ensure that each transmission or transaction in relation to .MY domain name(s) and any other Products and Services shall be authenticated or encrypted using such protocol or procedure as required by MYNIC, which protocol or procedure may be updated or modified from time to time on reasonable notice to the Registrar. Registrars is recommended to implement Two-Factor Authentication (2FA) in customer domain management portal to improve domain name security in protecting registrants' account. Both Parties hereby agree to employ adequate security measures to ensure the security of data exchanged and shall promptly inform the other on detection of any hacking, crawling, compromised passwords or other security breach;

6.1.8 To implement transfers of domain names registration from one Registrar to another pursuant to the Inter-Registrar Transfer Policy.

6.1.9 To not send any unsolicited emails, engage in spamming activities, encourage, or participate in cybersquatting or domain name abuse.

7. Registry Obligations

7.1 The Registry shall ensure the following obligation:

7.1.1 To provide the Registrar with access to any of MYNIC's Registrar system with a right to temporarily suspend access to the system (for any legitimate purposes) to protect the internet sovereignty;

7.1.2 To process applications and payments of .MY domain name(s) and other Products and Services that have been properly procured and submitted by the Registrar, provided that final acceptance of all applications and renewals shall be made by MYNIC in its sole discretion;

7.1.3 To maintain the registrations of Registered Names sponsored by Registrar in the Registry System;

7.1.4 In complying with Malaysian laws and regulations, to initiate inspection on any .MY domain name based on a third-party complaint or on its own initiative and reserves its rights to monitor the domain registry for any misuse or abuse purposes;

7.1.5 To issue a takedown notice to the Registrar to remove or disable access to malicious website upon obtaining actual knowledge of the illegal activity;

7.1.6 To suspend, delete, redirect, or transfer any registration or transaction, or place any domain names on registry lock, hold, or similar status as it determines necessary;

7.1.7 To register, modify and renew .MY domain names;

7.1.8 To reject any .MY domain application due to certain circumstances including but not limited to sensitive or reserved .MY domain names;

7.1.9 To determine eligibility criteria for .MY domain names;

7.1.10 To carry out audit sampling as post-verification on the veracity of the contact information submitted by the Registrars;

7.1.11 To request supporting document(s) from Registrars and Registrants (if any) to verify info for the registration, modification or transfer of .MY domain names;

7.1.12 To provide 24x7x365 days technical support on the Registrar system and operations to address any engineering issues.

8. Violations

8.1 Any misuse or abuse of a .MY domain name is a violation of the terms and conditions of the Registrant Agreement. Registrants are strictly prohibited from using or allowing the use of a registered .MY domain name to facilitate any illegal or wrongful activities or purposes.

8.2 Misuse of a domain name refers to any use of a .MY domain name that fails to comply with the terms and conditions described in this Policy as well as Malaysian laws and regulations.

8.3 Abuse of a domain name generally refers to any illegal, disruptive, malicious, fraudulent, or deceptive acts which leads to security and stability issues for Registries, Registrars, Registrants as well as end users of the Internet. This includes, without limitation to the following:

No.	Term	Definition
8.3.1	Malware (malicious software)	Malicious software, installed and/or executed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
8.3.2	Spam	Unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message is sent as part of a larger collection of messages, all having substantively identical content. Spam is only considered to be DNS Abuse when it is being used as a delivery mechanism for either malware, phishing, pharming and botnets.
8.3.3	Phishing	Occurs when an attacker tricks a victim into revealing sensitive personal, corporate or financial information (e.g. account numbers, login IDs, password), whether through sending fraudulent or look – alike emails, or luring end users to the copycat websites. Some phishing campaigns aim to persuade the user to install malware.

No.	Term	Definition
8.3.4	Pharming	The redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking can occur when the attackers use malware or redirect victims to the perpetrator's site instead of the one initially requested. DNS poisoning causes a DNS server (or resolver) to respond with a false Internet Protocol address bearing malware. Phishing differs from pharming in that pharming involves modifying DNS entries, while phishing tricks users into entering personal information.
8.3.5	Botnets	Collections of Internet-connected computers that have been infected with malware and can be commanded to perform activities under the control of a remote attacker.
8.3.6	Malicious fast-flux hosting	Namely the use of fast-flux techniques to disguise the location of websites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. In the context of ICANN, fast flux hosting refers to the automated, rapid modification of IP addresses, assigned to hosts in the DNS to hide the location of web sites supporting malicious, illegal, or criminal activities.
8.3.7	Hacking	Exploiting and violating a network security system.
8.3.8	Man in the browser attack	The use of malicious software or compromised network facilities for fraudulent or deceptive purposes.
8.3.9	Pornography	Any portrayal of sexual activity that a reasonable adult considers explicit, and pornographic in nature. The portrayal of sex crimes, including rape (attempted and statutory), as well as the portrayal of such sexual acts, through animation whether consensual or non-consensual.
8.3.10	Child Pornography	This includes the depiction of any part of the body of a minor in what might be reasonably considered a sexual context, and any written material or visual and/or audio representation that reflects sexual activity, whether consensual or non- consensual.
8.3.11	Misleading Advertisement	Offering for sale or distribution goods or services that are counterfeit or constituting of an invitation to participate in an activity

No.	Term	Definition
		and conveyed by or through any signage, image or sound disseminated through electronic medium for advertising purposes or infringing third party intellectual property rights or any applicable local or international laws and regulations.
8.3.12	Abusive Content	Content of a domain name which is scandalous, profane, indecent, obscene, menacing, offensive, or objectionable whether directly, indirectly, or defamatory in nature wherein the content by itself is prohibited under the Communications and Multimedia Act 1998 or any other local or international applicable laws and regulations. In this context, content means any sound, text, still picture, moving picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved, or communicated electronically.
8.3.13	Infringement to Intellectual Property	Such as trademark, copyright, patent, industrial designs, and geographical indications infringement, fraudulent or counterfeiting practices as well as other deceptive practices that is prohibited or do not comply with the requirements of local or international laws and regulations.
8.3.14	Terrorism	Use of domain names in contravention of anti-terrorism laws including but not limited to the Prevention of Terrorism Act 2015 (POTA), Special Measures against Terrorism in Foreign Countries 2015, National Security Council Act 2016, and Security Offences (Special Measures) Act 2012 as well as other applicable local and international laws and regulations enforced by law enforcement authorities.
8.3.15	Online Illegal Activities	Activities which are in contravention of the Malaysian laws and regulations such as illegal gambling, betting, bookmaking, prostitution, human trafficking, illegal distribution of drugs and incitement of violence.
8.3.16	Unauthorized Access and Cybersecurity Violations	Illegally accessing computers, accounts, or networks belonging to another party or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to

No.	Term	Definition
		an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).
8.3.17	Prohibited uses	Includes any unlawful use (i.e. in breach of statute, contractual obligations, duty of care etc), fraudulent use, defamatory use, causing damage or disruption to MYNIC systems, or any action taken which is likely to endanger any part of the domain name registry system, MYNIC systems or internet connections as a whole.

9. Compliance

9.1 In complying with the Malaysian laws and regulations, MYNIC shall initiate an inspection of any domain name in the .MY domain registry based on a third-party complaint or on its own initiative and reserves the right to monitor the domain registry for any misuse or abuse of the domain name.

9.2 In the event if the domain name is used in such unacceptable manner in MYNIC reasonable opinion, MYNIC reserves the right, at its sole discretion to issue a takedown notice to the Registrar to remove or disable access to malicious website upon obtaining actual knowledge of the domain name abuse. In addition, MYNIC may suspend, delete, redirect, or transfer any registration or transaction, or place any domain names on registry lock, hold, or similar status as it determines necessary either temporarily or permanently for any of the following reasons:

9.2.1 To protect the integrity, security and stability of the Domain Name system;

9.2.2 To comply with the terms of the Registrant Agreement;

9.2.3 To comply with any applicable laws, instructions, government rules or requirements, requests of law enforcement for the purpose of investigations, or any dispute resolution process;

9.2.4 To comply with any applicable terms and conditions, rules, policies, or procedures determined by MCMC and/or other regulatory requirements from time to time.

9.2.5 To avoid any potential liability, civil or criminal, on the part of MYNIC, its affiliates, subsidiaries, officers, directors, contracted parties, agents, or employees; and

9.2.6 To comply with Malaysian laws, procedures, or guidelines as MYNIC deems fit and necessary.

10. Abuse Monitoring

10.1 MYNIC shall periodically conduct a technical analysis to assess if the domain names are being used to perpetrate security threats, such as those identified in the abuse management process, and maintain statistical reports on the number of security threats identified and actions taken due to periodic security checks.

10.2 MYNIC shall reserve the right to suspend and/or delete the domain names which violate the terms and conditions of this Policy.

10.3 MYNIC may coordinate with the Registrars, MCMC, law enforcement agencies, government authorities and/or other third parties (such as hosting companies) in connection with any potential misuse or abuse associated with the domain names. MYNIC may work with users to remedy violations and ensure no re-occurrence of the violation prior to terminating the service.

11. Notices & Complaint Channels

11.1 Victims of any breaches or infringements of this Policy are encouraged to contact MYNIC at **abuse@mynic.my.** MYNIC shall investigate the matter and refer to the appropriate body for the next course of action.

11.2 In addition, besides the complaint channel as mentioned in paragraph 8.1 above, the victim of any breaches or infringements of this Policy may either:

11.2.1 lodging a report with the police where relevant, or

11.2.2 commencing a legal action against the domain name registrant subject to the legal action being based on a legal right(s) which are actionable in law.

12. General Terms

12.1 This Policy does not exhaustively cover all potential abuses or misuses of domain names, which may result in the suspension or deletion of a domain name under this Policy.

12.2 Any domain names content related matters that is illegal, offensive, obscene, scandalous, indecent, or against Malaysian public norms or values shall be subject to the Malaysian laws and regulations.

12.3 This Policy does not give rise to any rights of compensation or claims against MYNIC howsoever caused. The Registrant acknowledges and agrees that, to the extent permitted by law and regulation, the Registry shall not be liable for any direct or indirect, incidental, special, or consequential damages, including but not limited to loss of profits, business suspension, termination, or the inability to use of the domain name.

12.4 Additionally, the Registry shall not be liable for any losses or damages that the Registrant may suffer due to unauthorized use of a .MY domain arising from hacking, virus, system failure, use of passwords, or circumstances incidental to force majeure or any other unauthorized use in relation thereto.

12.5 MYNIC will be in compliance with all applicable laws, rules, and regulations and shall always enforce Malaysian's laws.

13. Review of Policy

13.1 Modification may be necessary, among other reasons, to maintain compliance with laws and regulations and/or accommodate organizational changes within MYNIC. As such, this Policy shall be reviewed in its entirety on an annual basis or as and when required to ensure the continued relevance and appropriateness of its contents.