

.scb Domain Name Anti-abuse Policy

Version 1.0

Available on: 2014/06/01

Effective on: 2014/06/01

Domain names under .scb will be registered through SCB's technical staff under SCB ownership. SCB will be the registrant and all contacts of the domain names and will take full controls of the domain names under .scb TLD. During the registration process, technical staff will check and verify that all information and contacts are completed and accurate. Therefore, the Whois will be 100% accurate.

Resourcing Plan :

There will be two IT staff handling the registration front-end to check & verify all registration information and being the abuse contact point to execute all duties as stated in the following Anti-abuse Policy.

Anti-abuse Policy Declaration :

Since .scb will be used internally, SCB will be the only registrant of all registered domain names, some concerning topics regarding anti-abuse has been covered or doesn't have any possibility to be occurred including "Innocent Registrant Protection".

Anti-abuse Policy :

To prevent and/or mitigate the effect of abuse, .scb prepared the ".scb Domain Name Anti-abuse Policy" as the following: **.scb Domain Name Anti-abuse Policy**

.scb Domain Anti-abuse Policy is announced in effect between .scb, Siam Commercial Bank PCL. [SCB] and the Registry Operator, Thai Name Server Co., Ltd. [ThaiNameServer], and the Registrar, DotArai Co., Ltd. [DotArai], and .scb Registrant. Abusive use(s) of .scb domain names should not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrar and registrants, as well as for users of the Internet in general. SCB defines abusive use of a domain as the wrong or excessive use of power, position or ability, and includes, without limitation, the following: Abusive use(s) of .scb domain names should not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrar and registrants, as well as for users of the Internet in general. SCB defines abusive use of a domain as the wrong or excessive use of power, position or ability, and includes, without limitation, the following: Illegal or fraudulent actions;

□

Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;

Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;

□

Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;

□

Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses.

□

Fast flux hosting: Use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fastflux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of SCB;

□

Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks); Distribution of child pornography; and Illegal Access to Other Computers or Networks: 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 an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

SCB reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or

any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of SCB, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by SCB or any Registrar in connection with a domain name registration. SCB also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute. Abusive uses, as defined above, undertaken with respect to .scb domain names shall give rise to the right of SCB to take such actions under the RRA in its sole discretion.

This policy is addressing a significant potential harm to Internet users. Abuses that may be prevented include identity theft, harm to children, and an erosion of trust in the Internet by users. SCB is enforcing its terms of service to registrar to prevent abuse across the .scb domain for the benefit of all users. The Domain Name Anti-abuse Policy is enacted under the clear, long standing, contractual authority of SCB. It is the goal of SCB that only those who abuse the domain system and engage in illegal or fraudulent activity will be affected by this policy. Ordinarily, there should be no change in the relationship with the registrar or the operation of .scb domain. While SCB is taking steps to ensure a mistake does not occur, we recognize that the rare false-positive may happen. SCB will place domains suspected of abuse on hold and not immediately delete them. This should ensure that in the extremely rare case that an innocent domain is suspended, that it can quickly be corrected. If the team confirms the abuse case, then SCB informs the related government agencies. Also, SCB coordinate with police to arrest the attackers. Once abuse is identified, SCB may notify and assist the registrar in resolving the abusive activity. This policy is designed to assist the registrar by providing them with important information for the betterment of the Internet as a whole. To prevent the malicious orphan glue records, SCB do not allow any orphan glue record in the system. All the orphan records will be automatically remove by the detection script. This policy is not a replacement for the UDRP. This policy is aimed at illegal and abusive use of domain names and is not a substitute for current remedies to resolve intellectual property disputes involving domain names and websites.

Abuse contact :

Any abuse report would be performed through a single security contact which is noc(at)scb.thains.co.th.

* The registrant is a .scb domain name holder. The registrant information and all contact information will be verified and completed in registration process. To verified contact information, SCB will ask for establishment documentation or identification card. In addition, the regular information update request will be sent to registrants email annually. All contact information will be placed in the WHOIS** system.

** WHOIS is an Internet service that allows anyone to obtain registration and contact information about domain name registrants. Although there are certain limitations on SCB's commercial use of the information, there are no effective means for protection of personal privacy. SCB holds this information for .scb as other registries hold it for other generic TLDs. And like all generic TLDs, SCB currently is required to make this information available through the WHOIS service in accordance with its agreement with ICANN. What procedures will SCB take to use the revised .scb Domain Name Anti-abuse Policy ? In case of a new policy arose to reflect certain current circumstances and technologies, SCB will announce them publicly on our registry website as well as on the registrar website one month prior the effective date.

Authorization :

SCB would declare the right to perform any action stated in this policy and would be fully controlled by the registry to access all domain functions in case of the abuse prevention or mitigation.