Q28_Attachment_Table: Implementation Plan of Domain Name Abuse Prevention and Mitigation

Domain name registration abuse	**Criteria for determination**	**Policies on registrar supervision**	**Policies on application review**	**Active monitoring and corresponding policies**	**Policies on complaints handling**
Cybersquatting	Cybersquatting is the deliberate and bad‐faith registration or use of a name that is a registered brand or mark of an unrelated entity, for the purpose of profiting (typically, though not exclusively, through pay‐per‐click advertisements).	When the domain name is in dispute, registrar needs to lock the name from any transfer or update. After the dispute resolution provider or the court made final decision based on UDRP, the registrar shall take further steps to unlock the domain name or transfer the domain name to its rights holder.	In the sunrise period, only registered trademark holders validated by Trademark Clearing House (TMCH) can register domain names. In the trademark claim service period, a clear trademark notice will be provided to the prospective registrant of the scope of the mark holder's rights in the registration review period.	N/A	Registrars are required to handle disputes in accordance with UDRP, and The registry will handle in a timely manner in respect of complaints sent via Uniform Rapid Suspension System.
Front Running	Front-running is when a party obtains some form of insider information regarding an Internet user's preference for registering a domain name and uses this opportunity to pre-emptively register that	The registry will conduct supervision on the services provided by the registrars pursuant to the provisions of agreements with registrars;	N/A	Domain name availability lookups should be performed with care. Our information security management will restrict unintended or unauthorized disclosure of insider information.	The registry will receive complaints through its complaint contact point and suspend domain names registered by relevant registrar once the front running behavior has been confirmed.

Domain name registration abuse	Criteria for determination	Policies on registrar supervision	Policies on application review	Active monitoring and corresponding policies	Policies on complaints handling
	domain name.				
Pornographic or offensive domain names	Pornographic/offensive domain names includes strings that contain adult or pornographic content or dirty words or words with offensive meaning against certain group of people or certain country.	N/A	The registry will review the application manually and check if any pornographic or offensive strings exist. The registry will inform the registrar to cancel the registration if such case is spotted during the application review procedure;	N/A	The registry will receive complaints through its complaint contact point. The complainant will be advised to resort to the court or domain name dispute provider for dispute resolution.
Domain spinning	Domain spinning is the practice of using automated tools used to create permutations of a given domain name string.	Conduct supervision on the services provided by the registrars and manage the same pursuant to the provisions of agreements with the registrars;	N/A	N/A	N/A
Fake Renewal Notice	Fake renewal notices are misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar. These are sent for a variety of	Conduct supervision on the services provided by the registrars and manage the same pursuant to the provisions of agreements with the registrars;	N/A	N/A	The registry will receive through its complaint contact for complaints filed by registrants and resellers, and require registrars or relevant parties to take penalties upon confirmation of

Domain name registration abuse	**Criteria for determination**	**Policies on registrar supervision**	**Policies on application review**	**Active monitoring and corresponding policies**	**Policies on complaints handling**
	deceptive purposes.				its misconduct.
Domain Tasting	Registrants may abuse the Add Grace Period through continual registration, deletion, and re‐registration of the same names in order to avoid paying the registration fees.	The registry will include provisions in the RRA requiring registrars to receive a reasonable assurance of payment from any potential domain name registrant prior to submitting any registration request on behalf of that registrant.	N/A	N/A	N/A

Malicious Use of domain names	**Criteria for determination**	**Policies on registrar supervision**	**Policies on application review**	**Active monitoring and corresponding policies**	**Policies on complaints handling**
Phishing	Phishing is a Web site fraudulently presenting itself as a trusted brand in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords).	Upon confirmation of reports on abuse, registrars shall suspend the domain name in a timely manner and contact relevant domain name registrant for corrections.	Registrars are required to verify the accuracy of the registration information to make sure that the registrants are accessible when resolving domain name dispute or carry out law enforcement.	The registry will monitor on a regular basis orphan glue records related to abuse and remove corresponding record accordingly. The registry will also monitor the susceptive phishing website on a regular basis. The registry will also limit the ability of registrants to repeatedly change their name servers via a programmatic interface to reduce or eliminate automated name server hopping.	The registry will receive complaints filed by users through its complaint contact. The registry will also cooperate with APAC and suspend reported phishing websites in a timely manner
Spreading malware/ notnet Command-and-Control	Malware/ Botnet Command-and-Control is to use domain names as a way to control and update botnets. Botnet s can be used to perpetrate many	N/A	N/A	Upon confirmation of reports on abuse, the registry shall block the domain name in a timely manner to avoid further attack.	The registry will receive complaints filed by users through its complaint contact. The registry will also cooperate with CNCERT/CC and block

Malicious Use of domain names	Criteria for determination	Policies on registrar supervision	Policies on application review	Active monitoring and corresponding policies	Policies on complaints handling
	kinds of malicious activity, including distributed denial‐of‐service attacks (DDoS), spam, and fast‐flux hosting of phishing sites.				reported websites in a timely manner
Spam	Spam is generally defined as bulk unsolicited e‐mail. Spam may be sent from domains, and spam is used to advertise Web sites.	N/A	Registrars are required to verify the accuracy of the registration information to make sure that the registrants are accessible when resolving domain name dispute or carry out law enforcement.	N/A	The registry will receive complaints filed by users through its complaint contact. The registry will also cooperate with 12321 Center and jointly block reported IP address in a timely manner.
Spreading Malicious Content	Use domain names to disseminate malicious information, including those in violation of the laws of the People's Republic of China and world recognized ethics and morality	Upon confirmation of reports on abuse, registrars shall suspend the domain name in a timely manner and contact relevant domain name registrant for corrections.	Registrars are required to verify the accuracy of the registration information to make sure that the registrants are accessible when resolving domain name dispute or carry out law enforcement.	The registry will monitor on a regular basis orphan glue records related to abuse and remove corresponding record accordingly.	The registry will receive complaints filed by users through its complaint contact. The registry will also cooperate with 12321 Center and suspend reported websites account in a timely manner.