BNP PARIBAS

ACCEPTABLE USE AND TAKEDOWN POLICY

BNP Paribas ("the Registry") as the operator of the TLD .bnpparibas attaches great value to the secure use and usability of the services available under the TLD .bnpparibas.

Abuses of .bnpparibas are a threat to the stability and security of the Registry, registrars, registrants and the security of Internet users generally. This Acceptable Use Policy (« AUP ») sets forth the terms and conditions for the use by a Registrant of any domain name registered or renewed under .bnpparibas.

The Registry reserves the right to modify or amend this AUP at any time in order to comply with applicable laws and terms and/or any conditions set forth by ICANN.

Acceptable Use Overview

All domain name registrants must act responsibly in their use of any .bnpparibas domain or website hosted on any .bnpparibas domain, and in accordance with this policy, ICANN registry agreement, and applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, and intellectual property rights.

The Registry will not tolerate abusive, malicious, or illegal conduct in registration of a domain name; nor will the Registry tolerate such content on a website hosted on a .bnpparibas domain name.

This AUP will govern the Registry's actions in response to abusive, malicious, or illegal conduct of which the Registry becomes aware. The Registry reserves the right to bring the offending sites into compliance using any of the methods described herein, or others as may be necessary in the Registry's discretion, whether or not described in this Acceptable Use Policy.

Upon becoming aware of impermissible conduct, the Registry (or its designees) may alert any relevant Registrar about any identified threats, and may work with them to resolve such issues. The Registry will also utilize such other methods, like the internal mediation, in compliance with applicable laws and ICANN policies, as it deems appropriate.

Reporting abuses

The Registry may receive AUP violations through a claim thanks or an internal mediation process. A point of contact is defined in these AUP to receive notices related to an AUP's violation.

At its discretion, the Registry, through an automated system or otherwise, may view any website hosted on a .bnpparibas domain, for the purpose of identifying AUP violations.

Abuse Point of Contact

Any complaint should be addressed to: csirt@bnpparibas.com

Complaints can also be sent by mail at the following address:

BNP PARIBAS
CSIRT
59 rue de la république
93100 MONTREUIL
FRANCE

You can find the BNP Paribas CSIRT First page at the address below:
https://www.first.org/members/teams/csirt_bnp_paribas

Prohibited actions

Conduct in violation of this AUP includes but is not limited to:

Phishing	Attempting to defraud and defame Internet users via masquerading as a known website, with the intent to steal or expose credentials, money or identities.
Domain Name or Domain Theft	Changing the registration of a domain name without the permission of its original registrant.
Botnet Command and Control	Running services on a domain name to control a collection of compromised computers or "zombies," or to direct Distributed Denial of Service attacks ("DDoS attacks").
Distribution of Malware	The creation and/or distribution of "malicious" software designed to infiltrate a computer system, mobile device, software, operating infrastructure, and/or website, without the owner or authorized party's consent. Malware includes, without limitation, computer viruses, worms, keyloggers and trojan horses.
Fast Flux Attacks／Hosting	The sheltering of phishing, pharming and malware sites and networks from detection, and the frustration of methods employed to defend against such practices, whereby the IP addresses associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find.
Hacking	The attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
Pharming	The redirecting of Internet users to websites other than those the user intends to visit, usually through, but not limited to, unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers, or DNS hijacking or poisoning.
Spam	The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and spamming of websites and Internet forums.

Piracy	The unlicensed publication, display and/or dissemination of any material that infringes the copyrights of any person.
Counterfeiting	The sale and advertising of illegal goods, including without limitations, goods that infringe the trademarks of any party.
Pornography	The storage, publication, display and/or dissemination of pornographic materials depicting individuals.
Front-running	The practice whereby use of insider information is made to register domains for the purpose of re-selling them or earning revenue via ads placed on the domain's landing page.
Gripe sites	Type of website devoted to the critique and or mockery of a person, place, politician, corporation, or institution.
Name spinning	Practice that helps people looking for a website address by suggesting alternative variations of a word or term that they enter. It can help them sort through similar sounding options and more importantly, provide alternatives when a domain name is already taken.
Domain kiting／tasting	Practice of temporarily registering a domain under the five-day Add Grace Period at the beginning of the registration of an ICANN-regulated second-level domain. During this period, a registration must be fully refunded by the domain name registry if cancelled.
Fast-flux	DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also refer to the combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and countermeasures.
419 scams	There are many variations on this type of scam, including advance-fee fraud, Fifo's Fraud, Spanish Prisoner Scam, the black money scam, and the Detroit-Buffalo scam. The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.

As well but not limited to cybersquatting, deceptive and ／or offensive domain names, fake renewal notices, cross gTLD registration scam, gripe site, pay-per-click, traffic diversion, false affiliation, or if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its Registrar partners and ／or that may put the safety and security of any registrant or user at risk.

Policy Purposes

The Registry reserves the right, in its sole discretion and without notice to any other party, to take appropriate actions (whether administrative, operational or otherwise) to:

• Protect the integrity and stability of the Registry;

• Comply with any applicable laws, government rules or requirements, ICANN regulations, requests of law enforcement, or any dispute resolution process;

• Comply with the terms of the registry agreement;

• Correct when possible mistakes made by the Registry in connection with a domain name registration;

• Allow for the resolution of a dispute of any sort whether or not the dispute appears to be unmerited or unsubstantiated;

• Respond to complaints of abusive behaviour on websites hosted on .bnpparibas domains; or

• Otherwise implement the Acceptable Use Policy.

Actions The Registry May Take

To enforce this Acceptable Use Policy, including responding to any prohibited activities, the Registry may take actions including but not limited to:

• Conduct an assessment to determine whether any alleged abusive or otherwise harmful behaviour violates the Registry's policies, applicable laws, or ICANN regulations;

• Lock down a domain name preventing any changes to the contact and name server information associated with the domain name;

• Place a domain name "on hold" rendering the domain name non-resolvable or transferring the domain name to another Registrar;

• Cancel or transfer or take ownership of any domain name, either temporarily or permanently;

• Use relevant technological services, whether our own or third party, such as computer forensics and information security; and

The Registry may also take preventative measures at its sole discretion including (without limitation):

• Place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Dispute Resolution Alternatives

The Registry is not bound to adjudicate any dispute between parties and cannot and does not accept any responsibility for any loss or damage a domain name registrant or anyone else may suffer as a result of any action or omission by us or by anyone else under this Acceptable Use Policy.

Disqualification of Registrants

Registrants, their agents or affiliates, determined by the Registry, in its sole discretion, to have repeatedly engaged in abusive, malicious or illegal conduct may be disqualified from maintaining any registrations or making future registrations of .bnpparibas domain names.

In addition, name servers that are found to be associated with fraudulent registrations may be added to a local blacklist and any existing or new registration that uses such fraudulent NS record may be investigated.

Following disqualification or a registrant, the Registry may cause such registrant's .bnpparibas domain names to resolve to a page noting that the domains have been disabled for abuse-related reasons.

Disclaimer and limitation of liability

The registrant's attention is particularly drawn to (a) the limitation of liability and indemnity provisions set out in the registration agreement that the registrant has agreed apply to the domain name, and (b) the fact that the registry (and registry related persons) can directly enforce these provisions against the registrant.