Domain Name Abuse Policy

Use of Charleston Road Registry d/b/a Google Registry (Google Registry) is subject to this Domain Name Abuse Policy. Please follow this policy when using our products and services. We may modify this policy so please check back here.

You agree not to use Google Registry in connection with:

- Spam: Do not send or promote unsolicited bulk messages, whether bulk marketing or otherwise.

- Malware: Do not intentionally transmit viruses, worms, defects, Trojan horses, malware, or any other content that may harm user devices, apps, servers, or personal data.

- Phishing and identity theft: Do not capture people's information under misleading or fraudulent pretenses, such as gaining login credentials or credit card information through fake web pages. Do not use stolen credentials or financial instruments to register domain names.

- Pharming and DNS hacking: Do not redirect DNS traffic from the intended website destination to a fake site through the use of DNS hijacking or interference.

- Fast-flux techniques: Do not intentionally use fast-flux techniques to avoid detection in order to conduct illegal activities on domain names.

- Botnet control and command practices: Do not use a network of poisoned or compromised computers to inflict harm on valid computer services. This includes using this coordinated network to launch denial-of-service (DDos) attacks.

- Hacking: Do not illegally penetrate computers, accounts, networks or security defenses of the Google Registry, any other Google product, or those of any Google partners. This includes any attempt that serves as a precursor to an attempted system hack.

- Child sexual abuse imagery: We have a zero tolerance policy towards content that exploits children. Do not publish or distribute child sexual abuse imagery.

- Unqualified applicants: You must meet registration eligibility requirements in order to register a domain.

- Illegal content: Do not host the distribution or publication of any information that is in violation of any applicable laws or regulations.

Reservation Of Rights

Abuse includes the foregoing activities and any other activity that causes actual and substantial harm, or is a material predicate of such harm; and is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

Google Registry 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, as it deems necessary, in its unlimited and sole discretion: (1) to comply with specifications adopted by any industry group generally recognized as authoritative with respect to the Internet (e.g., RFCs); (2) to correct mistakes made by Google Registry or any registrar in connection with a domain name registration; (3) to protect the rights and property of Google Registry and to avoid any potential or actual liability, civil or criminal, on the part of Google Registry as well as its affiliates, subsidiaries, officers, directors, representatives, employees, and stockholders; (4) to protect the integrity and stability of the registry and the operation of the DNS; (5) to comply with all applicable laws, government rules or requirements, requests of law enforcement or any applicable dispute resolution process; or (6) for violation of the terms and conditions set forth in any applicable registration agreement.

*****

Domain Registration Policy

Domain names may only be registered to Charleston Road Registry Inc. and its affiliates, including Google LLC.

*****

Pricing Policy

Charleston Road Registry d/b/a Google Registry (Google Registry or Registry Operator) will provide Registrar with a rate card indicating prices for:

1. Standard Domain Registration Fee
2. Sunrise Registration Fee
3. Domain Renewal Fee
4. Domain Transfer Fee
5. Domain Restore Fee
6. Domain Server Status Change Request Fee

The Registry Operator may update the rate card and modify this Pricing Policy from time to time in accordance with the .play Registry-Registrar Agreement.

Grace Periods

Sunrise Add Grace Period: For domain registrations resulting from Sunrise Period applications, the domain will have a Sunrise Add Grace Period lasting 30 days. During this period, Registrars can delete the domain and avoid charges. Upon setting nameservers, a standard 5-day add grace period begins, and the Sunrise Add Grace period is no longer applicable.

Add Grace Period: For 5 days after registering a domain, Registrars can delete the domain without being charged, and the domain will be open for re-registration.

Auto-Renew Grace Period: Upon its expiration, a domain name will be automatically renewed for 1 year. For 45 days after a domain expires, Registrars can delete the domain to avoid being charged for this renewal.

Redemption Grace Period: For 30 days after a domain is deleted, a Registrar may redeem the domain, subject to the Registrar Abuse Policy and the applicable restore fees. This only applies to fully registered domains that are deleted, not to deletions of domains pending registrations or domains deleted during the Add Grace Period or Sunrise Add Grace Period.

*****

Google Registry Privacy Policy

At Charleston Road Registry d/b/a Google Registry ("Google Registry") we understand the trust users place in us and our responsibility to protect the privacy of user information. This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can access, update, and delete your information.

Information we collect

We collect information in three ways:

Information you give us

When you use our services, you may choose to provide us with certain personal information. For example, you may provide your name and email address when you reach out with customer support requests, or register for our promotional offerings.

If you use a Google Account to access Google Registry products and services ("Services"), your use of that account for our Services is governed by this Privacy Policy. When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Information we get from your use of our services

We may collect information about the services that you use and how you use them, like when you visit our website. This information may be linked to your Google Account and may include:

- Device information: We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number).
- Log information: When you use our services or view content provided by Google Registry, we may automatically collect and store certain information in server logs (records of the page requests made when you visit our sites). This may include: details of how you used our service; Internet protocol address; device event information such as crashes, system activity, hardware settings, browser type, standard HTTP request headers, including but not limited to user agent, referral URL, language preference, date and time; and cookies that may uniquely identify your browser or your account.
- Cookies and Local Storage: We may use various technologies to collect and store information when you visit the website, and this may include sending one or more cookies or randomly generated identifiers to your device. A cookie is a small file

containing a string of characters that is sent to your computer when you visit a website. Cookies may store user preferences and other information. The "help" portion of the toolbar on the majority of browsers will direct you on how to prevent your browser from accepting new cookies, how to command the browser to tell you when you receive a new cookie, or how to fully disable cookies. However, some of Google Registry's website features or services may not function properly without cookies. We may also collect and store information using mechanisms such as browser web storage (including HTML5) and application data caches.

Information we get from your registrar

Your registrar collects information from you when you register a domain name, including your name, address, contact information, the name servers on which your domain name is hosted and their IP addresses, and the same information for administrative and technical contacts you identify. We receive this information from registrars for Google Registry's top-level domains.

How we use the information we collect

We use the information we collect from our services for the following purposes:

- **Provide our services.** We use your information to deliver our services including fulfilling requirements under our agreement with the Internet Committee for Assigned Names and Numbers ("ICANN"), the accrediting body for top-level domain registries and additional domain-related services we may offer in conjunction with your registration.
- **Maintain and improve our services.** We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues. We maintain a centralized repository of registration information for registrants of our top-level domains to ensure the continuity, stability, and resiliency of the Domain Name System. We may also use your information to make improvements to our services or to offer new services — for example, launching verification services for some new top-level domains or expanding IDNs available for registration based on registrant location and demand.
- **Measure performance.** We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use Google's ad services.
- **Communicate with you.** We may use information we collect, like your email address, to interact with you directly. For example, we may send you information about our services or administrative messages related to your domain registration.

And if you contact Google Registry, we'll keep a record of your request including any contact information provided in order to help resolve any issues you might be facing.

- **Protect Google Registry, our users, and the public.** We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google Registry, our users, or the public. For example, we collect and analyze IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to our registrants. Where abuse is detected through our technical monitoring we may reach out to you, your registrar, or other third parties to assist in mitigation.

Information we share

We do not share your personal information with companies, organizations, or individuals outside of Google Registry except in the following cases:

With your consent

We may share personal information with companies, organizations or individuals outside of Google Registry when we have your consent.

For external processing

We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.

For legal reasons

We will share personal outside of Google Registry if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google Registry, our users, our registrar partners, or the public as required or permitted by law.

To meet our obligations to ICANN

To the extent permitted by law, we may share personal information with ICANN and other third parties as required to comply with ICANN requirements. These obligations include requiring us to:

- Operate registration data directory services that provide free public access to certain registration information including the registrant's self-identified Organization, State/Province and Country.
- Deposit domain name registration information with a third party escrow agent to provide redundancy in the case of failure.
- Provide domain name registration information to an ICANN-authorized Uniform Rapid Suspension (URS) provider upon notification from that provider of the existence of a complaint. The URS system is a rights protection mechanism for rights holders experiencing infringement.
- Provide reasonable access to domain name registration information to ICANN for the purpose of investigating compliance-related inquiries or for other legitimate purposes.

We may share aggregated, anonymized information with ICANN, publicly, and with our partners. For example, we may share information publicly to show statistical trends about the general use of our services.

If Google Registry is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Retaining and deleting your personal information

We retain your personal information only as long as necessary to provide you services and to safely delete it following termination of services. When we receive an update indicating that you deleted your registration data via your registrar, we start the process of removing it from our systems. First, we aim to remove any publicly visible personal information by removing your information from any registration data directory services we operate. We then begin a process to safely and completely delete the data from our back-up storage systems.

Sometimes business or legal requirements may oblige us to retain certain information, for specific purposes, for an extended period of time. We might retain some data for longer periods of time if:

- An applicable law, regulation, legal process (e.g., a subpoena) or enforceable government request, requires us to do so or it is necessary to enforce applicable

Terms of Service, including investigation of potential violations of those terms or our abuse policies.
- We are investigating or have taken action with respect to a domain for abusive behavior.
- You have directly communicated with us, through a customer support channel, feedback form, or a bug report, in which case, we may retain reasonable records of those communications.

Information security

Google Registry uses strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you or your registrar and help guide you through steps to stay better protected. We work hard to protect you and Google Registry from unauthorized access, alteration, disclosure, or destruction of information we hold, for example:

- We use encryption to keep your data private while in transit
- We regularly review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need access that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of our website, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Compliance and cooperation with regulators

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data Transfers

Our parent company, Google LLC, maintains servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections

described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the Data Privacy Framework described below.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We may work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

Adequacy decisions

The European Commission has determined that certain countries outside of the European Economic Area (EEA) adequately protect personal data, which means that data can be transferred from the European Union (EU) and Norway, Liechtenstein, and Iceland to that third country without any further safeguard being necessary. The UK and Switzerland have approved similar adequacy decisions. We rely on the following adequacy decisions in some cases:

- European Commission adequacy decisions
- UK adequacy regulations
- Swiss adequacy decisions

Model contract clauses

Model contract clauses are non-modifiable written commitments between parties that can be used as a ground for data transfers from the EU (including the EEA), UK and Switzerland to third countries by providing appropriate data protection safeguards. EU Standard Contractual Clauses (SCCs) have been approved by the European Commission (you can see the SCCs adopted by the European Commission here). Such clauses have also been approved for transfers of data to countries outside Switzerland. The UK has approved the International Data Transfer Addendum to the EU SCCs (UK Addendum), which is available here. We rely on SCCs and the UK Addendum model contract clauses for our data transfers where required.

EU-U.S. and Swiss-U.S. Data Privacy Frameworks

As described in our parent company Google LLC's Data Privacy Framework certification, we comply with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (collectively, the "Data Privacy Framework" or "DPF"), as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information received in the U.S. from the EU, UK or Switzerland in reliance on the DPF. Google LLC, including Google Registry and Google LLC's other wholly-owned subsidiaries (unless explicitly excluded), has certified that it

adheres to the DPF Principles. Google Registry remains responsible for any of your personal information that is shared under the Accountability for Onward Transfer Principle with third parties for external processing performed on our behalf, as described in the "Sharing Your Information" section. To learn more about the DPF certification program, and to view our parent company Google LLC's certification, please visit the Data Privacy Framework website.

If you have an inquiry regarding our privacy practices in relation to our DPF certification, we encourage you to contact us. Google Registry is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). You may also refer a complaint to your local data protection authority, and we will work with them to resolve your concern. In certain circumstances, the Data Privacy Framework provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the Data Privacy Framework Principles.

European Requirements

If European Union or United Kingdom data protection law applies to the processing of your information, you have the right to request access to, update, remove, and restrict the processing of your information. You also have the right to object to the processing of your information. The personal information that we process about you is the information we receive from your registrar and any update that you make in your registrar's system will be automatically reflected in our system. If you would like to access, update, or remove any of that personal information, please first contact your registrar.

We process your information for the purposes described in this policy, based on the following legal grounds:

When we're pursuing legitimate interests

We process your information for our legitimate interests and those of third parties while applying appropriate safeguards that protect your privacy. This means that we process your information for the following purposes:

- Providing, maintaining, and improving our services to meet the needs of our users
- Detecting, preventing, mitigating, or otherwise addressing fraud, abuse, security, or technical issues with our services
- Centralizing registrant data for our top level domains to ensure the ongoing continuity, stability, and resiliency of the Domain Name System
- Protecting against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law
- Performing research that improves our services for our users and benefits the public
- Fulfilling obligations to ICANN and our registrar partners

- Enforcing legal claims, including investigation of potential violations of applicable Terms of Service and abuse policies

When we're providing a service

We process your data to fulfill registration and operation of your domain that you request through your registrar.

When we're complying with legal obligations

We'll process your data when we have a legal obligation to do so, for example, if we're responding to legal process or an enforceable governmental request. Google Registry may receive requests from governments and courts around the world to disclose registrant data. Respect for the privacy and security of your data underpins our approach to complying with these legal requests. Google's legal team reviews each request and frequently pushes back when a request appears to be overly broad or doesn't follow the correct process. Learn more in Google's Transparency Report.

If you have questions, you can contact Google LLC and its data protection office. And you can contact your local data protection authority if you have concerns regarding your rights under local law.

For the purposes of EEA data protection law, Google Registry has appointed Google Ireland Ltd. as its local representative in the EEA. Google Ireland Ltd.'s address is Gordon House, Barrow Street, Dublin 4, Ireland. For the purposes of UK data protection law, Google Registry has appointed Google UK Ltd. as its local representative in the UK. Google UK Ltd.'s address is Belgrave House, 76 Buckingham Palace Road, London, SW1W 9TQ, UK.

U.S. State Law Requirements

Some U.S. state privacy laws require specific disclosures.

These laws include:

- California Consumer Privacy Act (CCPA);
- Virginia Consumer Data Protection Act (VCDPA);
- Colorado Privacy Act (CPA);
- Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA); and
- Utah Consumer Privacy Act (UCPA)

This Privacy Policy is designed to help you understand how Google Registry handles your information:

- We explain the categories of information Google Registry collects and the sources of that information in Information we collect.
- We explain the purposes for which Google Registry collects and uses information in How we use the information we collect.
- We explain when Google Registry may disclose information in Information we share. Google Registry does not sell your personal information. Google Registry also does not "share" your personal information as that term is defined in the California Consumer Privacy Act (CCPA).
- We explain how Google Registry retains information in Retaining and deleting your personal information. You can also learn more about how Google anonymizes data. As described there, when Google anonymizes data to protect your privacy, we maintain policies and technical measures to avoid re-identifying that information.

U.S. state privacy laws also provide the right to request information about how Google Registry collects, uses, and discloses your information as well as how to request deletion of your personal information. Many of these laws provide the right to not be discriminated against for exercising these privacy rights. Many of these laws also provide the right to opt out of certain forms of profiling and targeted advertising. Finally, the CCPA treats certain kinds of information, like health data, as sensitive; when users provide this information, Google Registry only uses it for purposes permitted by the CCPA, like to provide services that are requested and expected by our users.

If you have questions or requests related to your rights under U.S. state privacy laws, you (or your authorized agent) can also contact Google LLC. And if you disagree with the decision on your request, you can ask Google LLC to reconsider it by responding to our email.

We also provide more information on Google Registry's handling of CCPA requests.

Some U.S. state privacy laws also require a description of data practices using specific categories. This table uses these categories to organize the information in this Privacy Policy.

Categories of information we collect

Identifiers and similar information such as your name and password, phone number, and address, as well as unique identifiers tied to the browser, application, or device you're using.

Demographic information, such as your age, gender and language.

Commercial information such as your payment information and a history of purchases you make on Google's services.

Internet, network, and other activity information such as your search terms; views and interactions with content and ads; Chrome browsing history you've synced with your Google Account; information about the interaction of your apps, browsers, and devices with our services (like IP address, crash reports, and system activity); and activity on third-party sites and apps that use our services. You can review and control activity data stored in your Google Account in My Activity.

Geolocation data, such as may be determined by IP address, depending in part on your device and account settings. Learn more about Google's use of location information.

Business purposes for which information may be used or disclosed

Protecting against security threats, abuse, and illegal activity: Google Registry uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.

Auditing and measurement: Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.

Providing our services. Google Registry uses your information to deliver our services, including fulfilling requirements under our agreement with ICANN.

Maintaining and improving our services: Google Registry uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us. We may also use information to make improvements to our services or offer new services (like verification services for some top-level domains).

Research and development: Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's Allanguage models and build products and features like Google Translate, Bard, and Cloud AI capabilities.

Use of service providers: Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.

Legal reasons: Google Registry also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our Transparency Report.

Parties with whom information may be disclosed

Third parties as required by our contracts with ICANN, including registrars, escrow agents, and ICANN.

Service providers, trusted businesses, or persons that process information on Google Registry's behalf, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

Law enforcement or other third parties, for the legal reasons described in information we share.

Requirements under Japan Act on the Protection of Personal Information

Google may transfer your personal data to California based companies. Please click here for information on the personal data protection regulation in California, USA (with regard to US federal law, please see here). For other disclosure, please see here.

About this Policy

When this Policy Applies

This Privacy Policy applies to all of the services offered by Google Registry. This Privacy Policy doesn't apply to the information practices of other companies and organizations or to other Google products and services. For example, our website may contain links to and from the websites of our partners and these websites have their own privacy policies. Please check these policies before you submit any personal data to these websites.

Changes to this Policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes)Any changes we may make to this Privacy Policy in the future will be posted on this page and, where appropriate, notified to you by e-mail.

Contact Us

If you have any questions about this Privacy Policy, please feel free to contact us here.

*****

Registrar Abuse Policy

Use of Charleston Road Registry d/b/a Google Registry ("Google Registry") by Registrars is subject to this Registrar Abuse Policy, which Google Registry may update from time to time.

If not defined here, capitalized terms have the meaning stated in the Registry Registrar Agreement ("Agreement") between registrar or other authorized user ("You") and Google Registry.

You agree to not engage in any abusive behaviors, including the following:

- Allowing registrants to use the Registry Services in any manner that violates the Domain Name Abuse Policy
- Engaging in deceptive practices including fraudulent attempts to manipulate transfers, or sending false or misleading notices to domain name registrants.
- Taking any actions on a registered domain that are not in the interest of, or requested by, the domain registrant, including but not limited to:
    - Restricting transfers of domain names to other registrars
    - Renewing domains other than for use by the existing registrant
    - Transferring domains to yourself or another registrant due to non-payment of fees or non-renewal of domain by existing registrant, or
    - Registering domains for the registrar's own purposes based on user queries (i.e. "Front-running")

Your failure to comply with this policy may result in suspension or termination of the Agreement.

*****

<u>Startup Policy</u>

Startup periods applicable to .play:

- Sunrise Period: end-date
- Sunrise Period allocation process: Auction
    - Participants will be invited to auction via email address. Exact rules of auction will be made available to participants via the website of the auction provider.

I. Definitions of registration periods:

A. Sunrise Period

1. Sunrise Period is an initial registration period, intended to protect trademark owners that precedes the general registration period. A registration is considered a Sunrise registration if it meets the criteria described below and is accompanied by a valid Trademark Clearinghouse ("TMCH") Signed Mark Data ("SMD") file.

B. General Registration Period

1. The general registration period will be a steady state phase for the duration of the Registry Operator's operation of the Registry TLD. During the general registration period, a registrant that meets the requirements set forth in the Domain Registration Policy may apply for any second-level domains in the Registry TLD not registered at that time, and names shall be allocated on a first-come-first-served basis, subject to Section 2.3 and Registry Operator's rights protection mechanisms set forth in Section 3.6 of the Registry-Registrar Agreement.

C. Sunrise Period

1. <u>Registration Criteria</u>

    a) Sunrise applications must be on behalf of qualified trademark owners of marks in the TMCH. The applications for Sunrise must be for second-level domains that are an identical match to their listed trademarks.

2. <u>Application Fees</u>

a) The application fees for the Sunrise Period are detailed in the TLD Pricing Policy.

3. Registration Processing

a) If the Registry Operator receives multiple Sunrise applications for a second-level domain, those applicants will enter a contention resolution process (for example, an auction) to allocate the second-level domain. Registry Operator will resolve all contentions and process all Sunrise applications before the beginning of the general registration period.

4. Contention Resolution

a) If a second-level domain goes into contention, all applicants will be contacted and invited to the contention resolution process directly.
b) The rules of the contention resolution process will be made available to all applicants before the process to allocate second-level domains begins.
c) The winning applicant of the contention resolution process will be allocated the second-level domain as described in the "Allocation and Registration" section.
d) If none of the parties participates in the process to the minimum required extent (for example, in an auction, pay the minimum bid), the second-level domain will not be allocated to any of the Sunrise applicants, and will be treated as if no Sunrise applications were submitted for it.

5. Allocation and Registration

a) Once Registry Operator determines who the final recipient of a second-level domain is, it will register the name to that recipient and charge their sponsoring Registrar the full registration price of the second-level domain, for the entire registration period requested by the applicant.
b) In order to provide the sponsoring Registrar an opportunity to collect these fees, a Sunrise Add Grace Period (as defined in the TLD Pricing Policy) will apply, during which Registrar can delete the second-level domain (if, for example, they never receive payment from their customer), and avoid being billed for it. However, once Registrar sets nameservers for the second-level domain, Registrar only has the standard Add Grace Period

(as defined in the TLD Pricing Policy) within which to delete the second-level domain and avoid being charged.

c) The registration prices for second-level domains awarded during all registration phases are detailed in the TLD Pricing Policy.

6. Failure Scenarios

a) Domain allocation in the event applicants who are engaged in a contention resolution process do not participate is specified in the "Contention Resolution" section.

b) In the event that a second-level domain is awarded, but then deleted by the Registrar due to nonpayment of registration fees or deleted by the Registry Operator due to SDRP (as defined below) objections:

(1) Registry Operator or an authorized vendor will contact any prior contending applicants, in order of their standing in the contention resolution process, and offer them the opportunity to register the domain.

(2) If none of the prior contending applicants choose to register the domain, then, the second-level domain opens up for the general registration period.

7. Sunrise Dispute Resolution Policy

a) Registry Operator will incorporate a Sunrise Dispute Resolution Policy ("SDRP"). The SDRP will allow challenges to Sunrise Period registrations by third parties for a 10-day period after acceptance of the registration based on the following three grounds: (i) at the time the challenged second-level domain was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the second-level domain is not identical to the mark on which the registrant based its Sunrise Period registration; and (iii) the trademark registration on which the registrant based its Sunrise Period registration is not of national or regional effect or the trademark had not been court-validated or protected by statute or treaty.

b) After receiving a complaint challenging a Sunrise Period application via the "Report a Problem" link at www.google.com/registry ("Complaint"), the Registry

Operator's designated contact ("Sunrise Contact") will review the Complaint to see if the Complaint reasonably asserts a legitimate challenge as defined by the SDRP. If the Complaint does not, the Sunrise Contact will email the complainant within 36 hours of the Complaint to indicate that the subject of the Complaint does not fall within the SDRP, and that Registry Operator considers the matter closed.

c) If the Sunrise Contact requires further information from the Sunrise Period registrant or if the second-level domain is not found to have adequately met the Sunrise Period eligibility requirements ("SERs"), the Sunrise Contact will promptly notify the registrant of the action and the nature of the Complaint, and provide the registrant with the option to respond within ten days to cure the SERs deficiencies. All such actions will be ticketed in Google's customer relationship management software to maintain accurate SDRP processing records.
If the registrant responds within 10 business days, its response will be reviewed by the Sunrise Contact to determine if the SERs are met. If the Sunrise Contact is satisfied by the registrant's response, the Sunrise Contact will then notify the complainant that the Complaint was ultimately denied and provide the reasons for the denial. If not, both the registrant and the complainant will be notified that the second-level domain will be released.

d) Registry Operator reserves the right to suspend a second-level domain during the pendency of a SDRP dispute, and/or to cancel, transfer, or take other action deemed necessary in its discretion upon completion of its review and/or receipt of a decision under the SDRP. Upon receipt of a decision that the registration does not meet the SERs, Registry Operator expressly reserves the right to cancel, transfer, or take other action deemed necessary in its discretion.

*****