fTLD Operations Pledge
September 2017

	Operations Pledge	Rationale
A	fTLD will provide a Name Selection Policy.	Ensures Registrars and Registrants understand the rules for selecting domain names in .BANK or .INSURANCE.
B	fTLD will provide a Name Allocation Policy.	Ensures Registrars and Registrants understand the rules for classifying and allocating domain names in .BANK or .INSURANCE.
C	fTLD will provide a Registrant Eligibility Policy.	Ensures Registrars and Registrants understand the rules for determining organizational eligibility for domain names in .BANK or .INSURANCE.
D	fTLD will provide an Acceptable Use / Anti-Abuse Policy.	Ensures Registrars and Registrants understand the rules for how domain names may and may not be used in .BANK or .INSURANCE.
E	fTLD will provide a Policy Development Process Policy.	Ensures that proposed policy changes are consistent with the terms and spirit under which .BANK or .INSURANCE was granted.
F	fTLD will ensure ongoing compliance with its Registry Agreements with ICANN.	Ensures fTLD complies with its Registry Agreements to operate .BANK and .INSURANCE.
G	Registrars will certify annually to ICANN their compliance with the Registrar Accreditation Agreement. * https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#compliance	Ensures Registrars remain compliant with their Registrar Accreditation Agreement.
H	fTLD will notify Registrar immediately regarding any investigation or compliance action, including the nature of the investigation or compliance action, by ICANN or any outside party (e.g., law enforcement).	Ensures fTLD adheres to high standards of integrity in operations, accountability and transparency.

	Operations Pledge	Rationale
I	Registrars will notify* fTLD immediately upon receipt of a second inquiry or notice regarding any investigation or compliance action, including the nature of the investigation or compliance action, from ICANN or any outside party (e.g., law enforcement). Notification to fTLD must identify the impacted TLD and include the nature of the investigation or compliance action. * May be waived in some cases (e.g., sealed court orders, national security issues).	Ensures Registrars adhere to high standards of integrity in operations, accountability and transparency.
J	fTLD and Registrars will provide and maintain valid primary contact information (name, email address, and phone number) on their websites and are encouraged to provide contact information for other functions, including, but not limited to, abuse, compliance, operations, technical, etc.	Ensures internet users can reach a primary contact to report and/or resolve any issues.
K	fTLD will re-validate its contracts with Registrars at least annually.	Ensures Registrars are compliant with their contracts with fTLD.
L	fTLD and Registrars will establish digital assertion via multi-factor authentication, to include user name and password plus one-time password, or something similar, for access to registration systems.	Ensures communication about registration data is with an authorized party.
M	fTLD and Registrars will provide and publish an elevated service capability to acknowledge and respond to emergencies.	Ensures that, during an emergency, issues are escalated to fTLD and/or Registrars for response and handling, ensuring continuity of service.
N	Registrars and their resellers are prohibited from providing or enabling Proxy/Privacy registrations.	Ensures availability, accuracy and transparency of registration data (e.g., organization, contact, phone number) for domain names in .BANK and .INSURANCE.
O	Registrars will disclose fTLD registration polices and requirements in their registration agreements and on their websites.	Ensures Registrants are provided the policies and requirements for obtaining and maintaining domain name registration.
P	fTLD will conduct due diligence of its third-party providers/vendors who provide technical or registration-related services to ensure appropriate controls are in place to mitigate risk of their services to fTLD.	Ensures third-party providers/vendors are thoroughly vetted, and vulnerabilities are addressed through technical, contractual and operational processes, and/or fTLD policies and requirements.

	Operations Pledge	Rationale
Q	Domain registrations will not be awarded until they have been validated against the eligibility and name selection policies, including verification of the registration data.	Ensures domain names are awarded to eligible organizations in compliance with fTLD Policies.
R	fTLD will re-verify Registrant eligibility every two years, or upon domain renewal, whichever comes first, and when there is a material change to registration data (e.g., organization name, registrant contact).	Ensures ongoing eligibility of the Registrant and its domain names.
S	fTLD will ensure technical implementations do not compromise Security Requirements.	Ensures Security Requirements are maintained and preserved during the implementation of any new registry feature, service, etc.
T	fTLD may from time-to-time modify the Security Requirements. fTLD shall provide Registrars no less than thirty (30) days written notice of any new or modified Security Requirement that has been approved by fTLD, and at least ninety (90) days' notice to implement the Security Requirement. If the Security Requirement is applicable to Registrants, Registrar must promptly provide notice to them and convey the ninety (90) day requirement for implementation. If the Security Requirement is intended to respond to a present or imminent security threat to .BANK or .INSURANCE, and/or any domain in its zone, fTLD reserves the right to require an expedited implementation.	Ensures Security Requirements are responsive to changing needs in security or the community.