fTLD Registry Services’ Security Requirements
April 2017

~~fTLD Registry Services’ Security Requirements~~
~~April 2016~~

	Requirement	Control	Rationale	Notes
1.	Registry Operator must define and implement a name selection policy (i.e., what types of names may be registered.)	Registry Operator must provide a description of its name selection policy.	Ensure domains are compliant with the name selection policy.	
2.	Registry Operator must define and implement a name allocation policy inclusive of a process to resolve a conflict between identical or confusingly similar names.	Registry Operator must provide an adequate description of its name allocation policy inclusive of a process to resolve contention between or among names.	Ensure domains are compliant with name allocation policy and that contention is resolved according to pre-published methods.	
3.	Registry Operator must define and implement a registrant eligibility requirements policy.	Registry Operator must provide a description of its registrant eligibility requirements policy.	Ensure domains are compliant with eligibility requirements.	
4.	Registry Operator must define and implement an acceptable use / anti-abuse policy.	Registry Operator must provide an adequate description of its acceptable use / anti-abuse policy.	Ensure domains are compliant with acceptable use / anti-abuse policy.	
5.	Registry Operator must define and implement a policy for amending its registration requirements.	Registry Operator must provide an adequate description of the process it will undertake to amend its registration policies (e.g., name selection, name allocation, eligibility requirements, acceptable use / anti-abuse).	Ensure there is support for the proposed policy changes and that they are consistent with the spirit under which the TLD was granted.	

	Requirement	Control	Rationale	Notes
6.	Registry Operator will ~~certify annually to ICANN its compliance~~comply with its Registry Agreement ~~as required by its Registry Agreement.~~ with ICANN	Registry Operator ~~must provide an adequate description of~~has processes and compliance oversight in place to ensure ongoing compliance with its ~~proposed certification process.~~ Registry Agreement.	Ensure Registry Operator is compliant with its Registry Agreement.	~~The certification process could include an independent, third-party audit, an officer's attestation or an internal review such as that described in Specification 9 (see http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm).~~
7.	~~Registrar~~Registrars must certify annually to ICANN ~~and Registry Operator, respectively, its~~their compliance with ~~its~~the Registrar Accreditation Agreement ~~and Registry-Registrar Agreement.~~.	Registry Operator must ~~include in its Registry~~ confirm Registrar ~~Agreement the requirement for Registrar to annually certify~~ compliance with ~~their Registry-Registrar Agreement and their~~ the Registrar Accreditation Agreement.	Ensure Registrar is compliant with its Registrar Accreditation Agreement ~~and its Registry-Registrar Agreement.~~.	~~Compliance for Registrar could be an identical or similar process to that of Registry Operator.~~ The Registrar Accreditation Agreement certification process could include an independent, third-party audit, an officer's attestation, and/or an internal review as described here: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#compliance.
8.	Registration Authorities (i.e., Registry Operator and Registrar) must provide and maintain valid primary contact information (name, email address, and phone number) on their website.	Registration Authorities must provide a description of how and where they will present such information on their website.	Ensure ~~Internet~~internet users are able to reach a primary contact to resolve an issue.	Registration Authorities are encouraged to provide contact information for other functions, including but not limited to, abuse, compliance, operations, technical, etc.
9.	Registry Operator must re-validate its Registry-Registrar Agreements at least annually.	Registry Operator must provide an adequate description of its re-validation process to include an action plan if Registrar fails re-validation and cannot cure the failure.	Ensure ~~that~~ Registrars ~~continue to meet the requirements defined in~~are compliant with the Registry-Registrar Agreement.	
10.	Registration Authorities must provide and publish an elevated service capability ~~with a well-defined escalation process~~ to acknowledge and respond to an emergency.	Registration Authorities must provide an ~~adequate description of their~~ elevated service capability ~~and their escalation process and both once finalized are~~ to ~~be published on their~~	Ensure that during an emergency ~~the Registrar (and in some cases Registrants and other users) can escalate their~~an issue ~~with~~is escalated to the Registration Authorities for response and handling.	

	Requirement	Control	Rationale	Notes
		~~website~~ensure continuity of service.		
11.	Registry Operator must 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).	Registry Operator ~~must~~will provide ~~a description of its notification process including under what circumstances~~ notice ~~may not be required~~as appropriate to the notice contact(s) in its Registry-Registrar Agreements.	Ensure that Registry Operator adheres to high standards of integrity in operations, accountability, and transparency. ~~The requirement to report an investigation or compliance action could be included in its Registry Agreement with ICANN.~~	
12.	Registrar must notify Registry Operator immediately upon receipt of a second inquiry or notice regarding any compliance action from ICANN or any investigation or compliance action by a governmental authority with proper jurisdiction. Notification to Registry Operator must identify the impacted TLD and include the nature of the investigation or compliance action.	Registry Operator ~~must include~~provides in its Registry-Registrar Agreement a description of its notice requirements and the circumstances, if any, when notice may not be required.	Ensure that Registrar adheres to high standards of integrity in operations, accountability, and transparency.	This requirement may be waived in cases e.g., of sealed court orders, national security issues. If the results of ~~the~~an investigation ~~becomes~~become unsealed (e.g., domain name seizures), Registrar is required to notify and ~~share~~provide information ~~with~~to the Registry Operator.
13.	Registration Authorities must explicitly define for contracted parties (i.e., Registrars, Registrants) what constitutes abusive conduct including, but not limited to, malicious, negligent, and reckless behavior.	Registration Authorities must include in their contracts the definitions of abusive conduct including, but not limited to, malicious conduct, negligence, and reckless behavior and consequences of such behavior.	Ensure that Registrars and Registrants are fully informed of the definition and consequences of irresponsible behavior~~.~~ (i.e., abusive conduct).	

	Requirement	Control	Rationale	Notes
14.	Registrars with significant compliance infractions will be ineligible to provide registration services.	Registry Operator ~~must include~~includes in its Registry-Registrar Agreement an adequate description of the consequences of significant compliance infractions~~.~~ (e.g., termination and effect of termination provisions).	Ensure that Registrars with an excellent track record in operations are eligible to serve the TLD.	
15.	Proxy/Privacy registrations are prohibited.	Registration Authorities must convey the proxy/privacy registration prohibition to their contracted parties.	Ensure transparency for all registrations.	
16.	Registrars must disclose registration requirements on their websites.	Registry Operator ~~must include~~includes in its Registry-Registrar Agreement a requirement that Registrar must disclose registration requirements on their website.	Ensure ~~that~~ Registrants understand the policies and requirements ~~so they may successfully complete the~~of domain registration ~~process~~and ownership.	
17.	Registry Operator ~~must ensure that~~ will conduct due diligence of third-party providers/vendors who provide technical or registration-related services to Registry Operator and ~~Registrar are obligated to implement~~ensure appropriate controls ~~that are commensurate with any identified~~are in place to mitigate risk to Registry Operator and its domain services.	Registry Operator must provide an adequate description of how it will ensure ~~its~~ third-parties/vendors~~,~~ and ~~the vendors~~resellers of ~~its~~ Registrars, ~~may~~ comply with the TLD policies.	Ensure ~~that~~ third-party ~~service~~ providers/vendors are thoroughly vetted and vulnerabilities ~~with said providers~~ are addressed through technical, contractual and operational processes and/or TLD policies and requirements.	
18.	In the event of transition from ~~one~~ Registry Operator to another, Registry ~~operator~~Operator shall endeavor to propose a		Ensure ~~that once a~~the TLD is operated in accordance with ~~elevated security requirements that it continues to be regardless of the~~ its Registry ~~Operator~~Agreement.	~~ICANN's Explanatory Memorandum on gTLD Registry Transition Processes is available at http://www.icann.org/en/topics/new-gtlds/registry-transition-processes-clean-30may11-en.pdf.~~

	Requirement	Control	Rationale	Notes
	successor ~~Registry Operator~~ that will operate the gTLD consistent with ~~Registry Operator's~~the Registry Agreement.	~~N/A~~ICANN's Explanatory Memorandum on gTLD Registry Transition Processes is available at: http://www.icann.org/en/topics/new-gtlds/registry-transition-processes-clean-30may11-en.pdf.		~~Registry Operator shall endeavor to identify a successor Registry Operator.~~
19.	Domain names will not be activated or resolve in the DNS until they have been verified against the eligibility and name selection policies.	Registry Operator ~~must provide~~will implement a ~~description of its~~ verification process ~~to include the milestone~~ for domain ~~name activation~~registrations.	Ensure the legitimacy of registrations prior to activation.	
20.	Registry Operator must re-verify ~~registrants~~Registrants every two years or at domain renewal, whichever is first, or when there is a material change to the registrant organization name.	Registry Operator must provide an adequate description of how data will be re-verified.	Ensure there will be an ongoing verification of registration data.	
21.	Registry Operator must ensure ~~that~~ technical implementations do not compromise security requirements.	Registry Operator must provide an adequate description of its policy to ensure elevated security ~~levels~~requirements are not compromised during the implementation of new technology.	Ensure ~~that~~ elevated security requirements are maintained and preserved during the implementation of any new registry feature, service, etc.	
22.	Registration Authorities must establish digital assertion, or an equivalent process, during the registration process.	Registration Authorities must provide an adequate description of their ~~policy~~requirement for digital assertion, or ~~an~~ equivalent process, using best current practices and how ~~that requirement~~ it will be applied to Registrars and Registrants.	~~Ensure digital identity can be verified and trusted for communication between parties.~~	Two-factor authentication to include e.g., user name and password plus one-time password or something similar.

	Requirement	Control	Rationale	Notes
23.	DNSSEC must be deployed at each zone and subsequent sub-zones for domains that resolve in the DNS.	~~Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar to support DNSSEC.~~ ~~Registrar~~Registrars must communicate the DNSSEC requirement to ~~Registrant~~their Registrants in ~~its~~their Registration ~~Agreement~~Agreements and store Registrant's DNSSEC records. ~~Legacy domains (e.g., .COM, .NET) providing Defined Services are subject to terms of the Authorizations defined in Annex A.~~	Ensure DNSSEC is deployed at all levels within a zone to establish the chain of trust for domain names in the TLD.	~~Registrar~~Registrars must support DNSSEC and ~~Registrant~~Registrants must deploy DNSSEC for each domain and subdomain name that resolves in the DNS. ~~Registrar and Registrant~~DNSSEC deployment shall follow the best practices described in RFC 6781 and its successors.
24.	Registrar and Registrant access to registration systems must be mutually authenticated via Transport Layer Security (TLS) and secured with multi-factor authentication, NIST Level 3 or better.	Registration Authorities must provide a description of their authentication processes and include it in their contractual agreement.	Ensure security and provide additional evidence of the requesting entity's identity to the receiving entity.	TLS controls are defined in requirement #29.
25.	Registration Authorities and Registrants are required to use encryption practices defined by NIST Special Publication 800-57, or its successor, for all electronic communication between parties, including but not limited to web access, mail exchange, and file transfer, avoiding the use of unencrypted protocols ~~in order~~ to prevent tampering with messages.	~~Registration Authorities must include this requirement in their contractual agreements.~~ ~~Legacy domains (e.g., .COM, .NET) providing Defined Services are subject to terms of the Authorizations defined in Annex A.~~ Registry Operator must provide a description of its encryption requirements.	Ensure security of communication over the Internet to prevent eavesdropping, data tampering, etc.	As in all fTLD Security Requirements, this requirement applies to all subdomains. ~~A public key certificate must be used to meet this requirement.~~ .BANK and .INSURANCE are HTTPS-only communities. However, an unencrypted .BANK or .INSURANCE ~~website~~domain may exist for the sole purpose of redirecting to an encrypted version of the ~~website~~domain. TLS controls are defined in requirement #29.

	Requirement	Control	Rationale	Notes
26.	Registrants must publish a valid Domain-based Message Authentication, Reporting and Conformance (DMARC) record with a requested mail receiver policy of either quarantine or reject for domains that resolve in the DNS. For domains intended to send email, Registrants must publish at least one of the following email authentication DNS Resource Records: • Sender Policy Framework (SPF), • Domain~~-~~Keys Identified Mail (DKIM). When used to protect non-email sending domains, Registrants are required to publish a DMARC reject requested mail receiver policy.	~~Registration authorities must include this in their contractual agreements.~~ ~~Legacy domains (e.g., .COM, .NET) providing Defined Services are subject to terms of the Authorizations defined in Annex A.~~Registry Operator must provide a description of its email authentication requirements.	Enhance security, integrity and trustworthiness of the email channel by preventing the delivery of invalid or spoofed email purporting to originate ~~within the secure~~ from an in-zone domain.	For clarification purposes, Registrants must publish a valid email authentication record under all circumstances. For example, if the Registrant does not use their domain for sending email then they must publish the appropriate record (p=reject) reflective of that policy. When deploying DMARC, Registrants may temporarily use a "none" (p=none) or "quarantine" (p=quarantine) during the implementation phase of email capabilities on the affected domain, but must change the policy to reject for ongoing operations within 90 days of deployment. It is recommended that DMARC records specify strict identifier alignment for both SPF and DKIM via the adkim and aspf tags. It is recommended that DMARC records published at an organizational domain level set an appropriate sp: tag.
27.	DNS Resource Records (e.g., CNAME, DNAME, ~~SRV) are prohibited from aliasing~~MX) may be used to ~~DNS records outside~~ alias to out-of~~ the secure -~~zone domains.	Registry Operator must provide a description of their DNS Resource Records requirements. ~~Legacy~~ Out-of-zone domains ~~(e.g., .COM, .NET) providing Defined Services~~ are subject to ~~terms of~~requirement #23, DNSSEC, by January 1, 2018, and requirements #25 and #29 (i.e., TLS encryption at the ~~Authorizations defined in Annex A.~~relevant version).	~~Ensure traditional DNS zones may not impersonate higher security DNS zones.~~ Out-of-zone domains may be aliased from in-zone domains if certain requirements are met.	As in all fTLD Security Requirements, this requirement applies to all subdomains. PTR and SOA Resource Records are not in scope.

	Requirement	Control	Rationale	Notes
28.	Name server host names must be in the parent zone.	Authoritative name servers must be in the parent zone.	Ensure authoritative name servers are trusted and verifiable.	As in all fTLD Security Requirements, this requirement applies to all subdomains.
29.	Transport Layer Security (~~TLS~~the successor to SSL) must be implemented ~~using trusted protocol versions~~as detailed in the Notes column.	~~Transport Layer Security~~TLS must be implemented securely to protect the integrity and confidentiality of data in-transit. A public key certificate must be used to meet this requirement.	Some implementations of TLS~~/SSL~~ contain known vulnerabilities.	As in all fTLD Security Requirements, this requirement applies to all subdomains. ~~Transport Layer Security 1.1 or greater must be used. Any version of SSL is explicitly prohibited as is TLS 1.0.~~ a. Web connections: TLS v1.1 or greater should be maintained. TLS v1.0 may be used to serve educational information about the importance of browser hygiene and provide guidance about how to update a browser. Registrants should communicate to customers/visitors to their websites a specific date when access to their websites using TLS v1.0 will no longer be possible. b. Server-to-Server Email: For domains sending or receiving email, TLS v1.1 or greater must be offered at the highest priority. However, when exchanging mail with out-of-zone domains earlier versions of TLS/SSL are permitted, including, as the lowest priority, defaulting to unencrypted email when it is not possible to provide encryption. c. Other services: TLS v1.1 or greater should be used and TLS v1.0 does not need to be disabled at this time. RFC 5746 must be implemented (prevents a known man-in-the-middle attack). The following non-exhaustive list of cipher suite components (authentication, encryption, message authentication code and key exchange algorithms) are excluded

	Requirement	Control	Rationale	Notes
				from use ~~within the secure~~ with in-zone domains and the generation of TLS certificates: Anon, CBC, DES, 3DES, FIPS, GOST 28147-89, IDEA, SEED, WITH_SEED, MD5, NULL, SHA (SHA1), RC4, EXPORT, EXPORT1024 and SRP.
30.	~~Redirection.~~URL Redirection to an out-of-zone domain must be made from the HTTPS version of an in-zone domain.	~~Redirection to domains outside of the secure zone:~~ ~~- Access to secure services (e.g., online banking, transactional operations) are subject to compliance with requirements 23*, 25, 26 and 29.~~ ~~- Access to third-party content (e.g., affiliates, blogs, social media) is permissible.~~ ~~* Requirement must be met by January 1, 2018.~~ Any redirection must be made from the HTTPS (i.e., encrypted) version of an in-zone domain.	Ensures accessibility to ~~secure~~ services ~~via domains outside of the~~, information, etc. is made from a secure in-zone domain.	The secure zones are HTTPS-only communities and ~~therefore any~~require a public key certificate. Any redirection must be made from the HTTPS (i.e., encrypted) version of ~~the secure~~ an in-zone ~~website to legacy domains (e.g., .COM, NET).~~domain. Registrants that redirect from in-zone domains to out-of-zone domains ~~in the secure zone to those outside~~ are strongly encouraged to inform visitors of this action via an explicit message to avoid confusion and to ensure that visitors understand they are leaving the ~~secure~~ in-zone~~.~~ domain.
31.	~~Registrant compliance with~~Registrants are exempt from requirements 23, 25, 26, 27, 28, 29 and 30 in Emergency Situations.	Registrants are exempt for these specifically enumerated requirements in Emergency Situations. Registrants must provide written notification to fTLD ~~at compliance@ftld.com~~using the Incident Notification Form at https://www.ftld.com/incident-form/ of Emergency Situations lasting longer than three (3) business days by the end of the third business day.	Registrants must be permitted flexibility to protect themselves and their customers in Emergency Situations.	Emergency Situations are defined as present or imminent events such as: - Incidents that threaten systematic security, stability and resiliency of registrant infrastructure; - Unauthorized access to or disclosure, alteration, or destruction of registrant data or that of its customers; - An occurrence with the potential to cause a failure of registrant infrastructure.

	Requirement	Control	Rationale	Notes
32.	Registry Operator will periodically review these requirements and implement a repeatable and documented change management process.	Registry Operator will publish modifications to these requirements on its website and provide notice to Registrars as described in the notes.	Ensures requirements are periodically reviewed and amended as necessary and appropriate to respond to changing needs in security or the community.	This commitment is memorialized in fTLD's Affirmation of Commitments available at www.ftld.com/resources. Registry Operator may from time-to-time make modifications to the Security Requirements. Registry Operator shall provide Registrar no less than thirty (30) days written notice of any new or modified Security Requirement that has been approved by Registry Operator 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 the TLD and/or any domain in its zone, Registry Operator reserves the right to require an expedited implementation.

~~Annex A~~

~~Authorizations for Defined Services Deployed on Non-.BANK or Non-.INSURANCE Domains~~

~~Requirements/~~ ~~Defined Services~~	~~#23 – DNSSEC~~	~~#25 & #29 - TLS/Encryption Practices~~	~~#26 - Email Authentication~~	~~#27 - DNS Resource Record Restrictions~~
~~Hosted Email Solutions~~	🟨 ~~Required by January 1, 2018~~	🟨 ~~Required for Email and Web Services Only~~ ~~Required by April 1, 2017~~	🟩	🟥 ~~Exceptions for CNAME and MX~~
~~Content Delivery Networks~~	🟨 ~~Required by January 1, 2018~~	🟩	🟧 ~~N/A~~	🟥 ~~Exception for CNAME~~
~~Security[*] and Fraud Services~~	🟨 ~~Required by January 1, 2018~~	🟩	🟧 ~~N/A~~	🟥 ~~Exception for CNAME~~
~~Aliasing to Legacy Domains~~	🟩	🟩	🟩	🟥 ~~Exception for CNAME~~

~~Key: Green - fTLD Security Requirements apply now~~
~~Yellow - Delayed implementation of fTLD Security Requirement~~
~~Red - Enduring changes to fTLD Security Requirements~~
~~Orange – N/A (Not Applicable)~~

[*] ~~The Security Requirements do not apply to Distributed Denial of Service mitigation services that do not use DNS Resource Records within the .BANK or .INSURANCE Domain Name System.~~