APPLICATION FOR SGNIC'S REGISTRAR ACCREDITATION

SECTION I: General Information on Submission of Application

1. For purposes of an application to be an accredited registrar, the applicant is required to submit its responses to the questions in this application form, as well as provide all relevant supporting documents, in soft copy via email to dnq@sgnic.sg. Where the supporting documents are unavailable in soft copy, the applicant shall notify SGNIC and submit a physical copy of the responses and supporting documents (by hand, mail or courier) to SGNIC at the following address:

   Attn: General Manager, SGNIC
   Singapore Network Information Centre (SGNIC) Pte Ltd
   10 Pasir Panjang Road
   #03-01 Mapletree Business City
   Singapore 117438

2. The applicant is required to pay an application fee of S$1,000 plus GST at the prevailing rate. The fee is non-refundable and is to be paid by way of a crossed cheque made payable to "Singapore Network Information Centre (SGNIC) Pte Ltd". Foreign registrars may choose to wire the funds over and may request for SGNIC's banking details via email at dnq@sgnic.sg.

3. SGNIC may, from time to time and at any time at its sole and absolute discretion, seek clarification and additional information from the applicant in relation to the application, and may treat the application as withdrawn if such request(s) is/are not met in a timely fashion.

4. Applicants must meet all of SGNIC's accreditation requirements. However, it does not follow that an applicant meeting the accreditation requirements of SGNIC will be granted accreditation.

5. Approval of the application will be at the sole and absolute discretion of SGNIC. SGNIC is not obliged to notify the applicant in respect of the status of the application or inform the applicant of the reason(s) if SGNIC decides, at its sole and absolute discretion, to reject the application.

6. The applicant must declare that the information submitted in the application is true and accurate in all aspects. The applicant will be bound by all terms, commitments, offers, presentations, proposals, plans and obligations stated in the application. The application must be signed on behalf of the applicant by an authorised representative who has overall responsibility in ensuring the applicant's compliance with the terms and conditions of accreditation.

7. All applications are subject to SGNIC's verification and approval. The applicant agrees that SGNIC may collect, use, and/or disclose any information submitted in the application to third parties for assessment, verification and investigative purposes, including reviewing the accuracy and completeness of any information provided by the applicant. The applicant fully authorizes SGNIC to conduct such due diligence checks as SGNIC in its sole and absolute discretion considers necessary, including checks on the applicant's corporate information and particulars, credit and financial information, business operations, background and history, and any other information submitted for purposes of the application.

8. All documents, including supporting documents, must be submitted in English. Any translations, if so requested by SGNIC, must be provided to SGNIC at the applicant's own expense.

9. The applicant further agrees that it has read and understood SGNIC's registration policies and other initiatives, as may be revised from time to time, including the policies and processes for

VerifiedID@SG and RegistryLock. Information on SGNIC's policies and initiatives may be found on SGNIC's website at www.sgnic.sg.

10. By submitting its application, the applicant acknowledges that it has read, understood and agreed to all the terms and information as contained within this document.

SECTION II: Information to be Provided in Registrar Accreditation Application

Please provide the following information, answering each request in a numbered paragraph corresponding with the number of the question. Please give the most complete answer possible, explaining all capabilities in detail, and attaching, labelling, and referencing all necessary supporting documents to be provided together with the response.

PART A - General Information

1. Name and business address of the applicant.

2. Type of business entity (corporation, partnership, etc) and company / business registration number. Where the applicant is not based in Singapore, please provide evidence of accreditation by ICANN and full details thereof.

3. Contact number (both telephone and fax numbers) and email address of the applicant.

4. Name and details of contact person (including contact number and email address) of the applicant.

5. URL of the applicant's corporate website.

6. Corporate and shareholding structure of the applicant indicating the ultimate ownership.

7. Name and details of the directors of the applicant.

8. State whether directors are involved in any other entities, including entities within the domain name industry. For e.g. as a director or shareholder.

9. A certified copy of the Business Registration Certificate from the Accounting and Corporate Regulatory Authority (ACRA) or equivalent government or regulatory authority evidencing the applicant's corporate status.

PART B – Technical Capabilities

A copy of the applicant's final web application vulnerability assessment (VA) test report based on the requirements set out in the Appendix must be submitted. The final VA test report shall be dated no more than twelve (12) months preceding the date of application for accreditation and shall be free of "High" or "Medium" security risk findings.

Please also submit a detailed description of the applicant's technical capabilities or technical plans as specified below:

1. All software and hardware facilities in connection to the provisioning of domain name registration services. This shall include all servers (web, app, log, monitoring, etc.), database, related application software (web portal, DNS, billing, ticketing system, CRM, etc.), backup

systems and network equipment at both the production site and disaster recovery site(s). Please provide the network diagram(s) to assist in the understanding of the setup, along with descriptions of the function(s) of each component. There should also be an adequate number of servers, redundancy, diversity, backup and disaster recovery.

2. Information processing systems used to handle domain name registration and related activities such as request for modifications to domain name registrations, including renewals and transfer of domain name registration, changes of registrar, updates to information and other requests. Please indicate (a) the programming language used for the front end and backend software applications; and (b) number of staff proficient in EPP and their years of experience with EPP.

3. Capability for providing a reliable backup of registration data. Please describe the process in detail, including the frequency of backup, retention period and whether data is archived offsite.

4. Capability for providing information systems security procedures to prevent system hacks, break-ins, data tampering and other disruptions to operations. As a minimum, please include information on the following:

   (a) Hardware equipment and/or systems deployed for prevention, mitigation or detection (e.g. firewall, IDS/IPS, DDoS mitigation services, antivirus solutions, etc.);
   (b) OS and application hardening and security patching practice (e.g. frequency and standards followed, like CIS);
   (c) Whether the company adheres to security standards (e.g. ISO27001) on its information security management or follows certain frameworks such as COBIT or ITSM; and,
   (d) Whether the company undergoes regular Vulnerability Assessment (VA) and Penetration Test (PT), and if so, please state the frequency.

PART C – Business Capabilities

Please provide a detailed description of the applicant's business capabilities or business plans as specified below:

1. Business model, business plans and strategies of the applicant with regard to providing registrar services for .SG names, for e.g. serving both retail and corporate customers, targeting the education sector, etc. Please provide growth projections for the next 3 years for .SG names and also share the marketing and customer acquisition plans intended for .SG names for the next 3 years.

2. Network of resellers, if any, and compliance with SGNIC's requirements, obligations and policies.

   (a) Please provide information relating to the resellers of the applicant, including the number of resellers and the global countries and/or regions where such resellers are located.

   (b) The applicant is required to ensure compliance by its resellers to such requirements, obligations and policies as may be imposed on the applicant by SGNIC. Please provide information as to how the applicant ensures and maintains compliance by its resellers, and enforces such requirements, obligations and policies on its resellers. Please also detail the applicant's proposed remedial or enforcement action(s) against its resellers in the event that such persons fail to comply with SGNIC's requirements, obligations or policies.

3. Intended pricing for .SG names. Please list down the intended pricing for registrations, renewals, transfers, reinstatements, modifications/updates of contacts, modifications/updates of nameservers, etc.

4. Financial capability in the form of working capital for the operation of the registrar business. The applicant must provide evidence of its having maintained a minimum working capital of S$50,000 for at least the preceding two years, such as audited financial statements for the last two financial years, or other similar supporting documents deemed suitable by SGNIC. Applicants not based in Singapore should also provide evidence of their accreditation as a registrar by ICANN.

   (NOTE: Applicants should note that notwithstanding them having satisfied the requirements stated in paragraph 4 above, SGNIC may in its sole and absolute discretion direct an applicant to furnish a performance bond of S$30,000 in the form of a banker's guarantee if SGNIC accepts the applicant as an accredited registrar. Additionally, SGNIC reserves its right to increase the value of the performance bond at SGNIC's sole and absolute discretion.)

5. Ability to meet all of a registrar's responsibilities and obligations under the Registrar Accreditation Agreement.

PART D – Operational Capabilities

Please provide a detailed description of the applicant's operational capabilities as specified below:

1. Track records of operational experience in dealing with domain name registrations. The applicant must have at least six (6) months prior experience in domain name registration and management either as a reseller of a current registrar of SGNIC or as a registrar of other gTLDs or ccTLDs. If the applicant is currently a registrar, please provide a list of existing ccTLDs or gTLDs which the applicant is accredited with.

2. The organisation structure it intends to set up and the deployment of staff, with details of names of staff and their background and experience in providing the registrar service. Please indicate how many staff will be in the team managing .SG operations, including the management team, customer support, technical support, finance, registration fulfilment and processing, etc. Please provide information on where the various teams will be based and whether the support services are on a 24/7 basis. Please demonstrate the applicant's organisational capability to engage a sufficient number of qualified employees to handle the technical, administrative and customer support aspects of the registrar business.

3. The number of .SG names that the applicant is currently managing. Please also indicate which existing SGNIC accredited registrar(s) or partner(s) the applicant currently works with to register .SG names and since when has the applicant been managing .SG names.

4. Management and communication systems used to handle domain name registrations and related activities such as requests for modification, renewals, transfers, changes of registrar, updates to information and other requests. Please elaborate on the process flow for handling a customer's request from the moment it is received. Please also indicate whether a customer can self-manage any transactions through your system.

5. The plan that sets out the processes and procedures the applicant intends to / has put in place to validate the identity and eligibility of registrants. The applicant must have in place appropriate systems and processes to enable it to validate the identity of registrants and ensure that registrants meet the eligibility criteria for the domain name category applied for. Please explain the steps the applicant will take to verify that a registrant satisfies all the applicable eligibility criteria and other conditions of the relevant domain name category stated in the Rules for Registration (RoR). Please also indicate whether the processes and procedures are managed manually or automated via the applicant's system(s).

APPENDIX

Web Application VA Test For Registrar Accreditation Application

1. The VA test should be conducted on the external facing portal/website(s) of the information processing system that will be used to handle .sg domain name registration and related activities (e.g., request for modifications to domain names, renewals and transfer of domain names, changes of registrar, updates to information and other requests submitted by the registrants).

2. The vendor appointed to perform the VA test can either be the applicant's preferred security partner (with industry-recognized security certification(s) e.g. CREST) or one from the SGNIC's pre-screened security vendors listing[1].

3. The VA test(s) shall be performed at the applicant's own expense.

4. The final VA test shall be dated no more than twelve (12) months preceding the date of application to be a registrar.

5. The VA test should scan for vulnerabilities including but not limited to:
   a) Weak SSL/TLS ciphers & protocols used by the web application;
   b) Cross-Site Scripting (XSS);
   c) Cross-Site Request Forgery (CSRF);
   d) SQL Injections;
   e) Insecure configurations (e.g. not setting Secure and HTTP Only flags in the cookie); and,
   f) Click-Jacking.

6. The final VA test report should be free of open High or Medium security risk findings and capture the following information in English:
   a) Executive Summary summarizing the security status of the system
   b) Technical Report highlighting information on:
      i. Severity (High, Medium, Low) of the vulnerability initially found;
      ii. Description/Potential impact/Affected areas of vulnerability initially found;
      iii. Reference to the vulnerability or exploit initially found (i.e., CVE reports);
      iv. Ease of exploitation; and
      v. Whether the vulnerability was remediated adequately.

7. SGNIC reserves the right to reject the final VA test report submitted or to request for the VA test to be redone if the VA test report is deemed to be inadequate or if the vendor is assessed to be unqualified/uncertified to perform the VA test.

[1] Refer to: https://www.sgnic.sg/docs/default-source/faq-pdfs/va_pre-screened_security_vendor.pdf