

Letter of Continued Support

Aug 11, 2026

This Letter of Continued Support is provisioned in addition to the Letter of Unconditional Funds Support dated Aug 4, 2026, the Memorandum of Understanding (“MOU”) established on Jul 27, 2026 between Security Matters (“Partner NGO”) and DotAsia Organisation (“DotAsia”), and the original Letter of Support included in the Applicant Support Program (ASP) application, regarding the application and operation of a New generic Top-Level Domain (New gTLD) through the ICANN process.

DotAsia is the operator of the .Asia gTLD and is the sole member supporting the DotKids Foundation in the operation of the .KIDS community gTLD, an ICANN Applicant Support Program (ASP) Supported Applicant. DotAsia represents and warrants that, as an ASP Incubator, it has the experience, knowledge and funds to support the Partner NGO in the operation of the New gTLD. This letter confirms DotAsia’s continued support to Partner NGO with the understanding that, Partner NGO has received the Determination Letter from ICANN confirming that it has qualified for the ASP support, and that Partner NGO commits to continue to meet the eligibility requirements to be ASP qualified.

As set forth in the MOU, upon the successful bid for the New gTLD or at any time prior, Partner NGO may, at its discretion, enter into a definitive Registry Operation Agreement with DotAsia. Such agreement shall determine the terms of service, which will ensure that, for the purposes of operating the New gTLD, Partner NGO’s self-certification for Financial Evaluation – Standard Profile (Q4.2-1), Security Policy and Planning (Q5.1-1), and, DNS Abuse (Q5.2-1) are supported either by DotAsia or by appropriate Registry Services Providers, including but not limited to:

Standard Profile (Q4.2-1)

SC4.2-1.1 - The applying entity and/or a QPE will fund the startup and long-term operation of all applied-for gTLD strings and (if applicable) currently operated gTLDs of a QPE.

SC4.2-1.2 - The applying entity or QPE has at a minimum of USD 50,000 plus 25% of the application base fee for each applied-for gTLD string in Cash and Cash Equivalents on the balance sheet of the provided financial statements, up to a maximum of USD 300,000, designated to support the startup and operation of all of the applying entity’s applied-for gTLD strings.

Security Policy and Planning (Q5.1-1)

SC5.1-1.1 - The applying entity will appropriately protect confidentiality of data and prevent unauthorized access to data and services.

SC5.1-1.2 - The applying entity will maintain a mature, appropriately funded and staffed security Program, following a recognized, modern security framework based on risk management (such as the ISO27000 series, COBIT, HITRUST CSF, legally required security frameworks, or equivalent). The

security Program must be in place prior to delegation, and exist through at least the period of the Base RA.

SC5.1-1.3 - The applying entity is aware of and has designed its systems and business to comply with the relevant privacy and security regulations for all countries in which it operates.

DNS Abuse (Q5.2-1)

SC5.2-1.1 - The applying entity will, no later than delegation of the Top Level Domain (TLD), establish a dedicated abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning any name registered in the TLD.

SC5.2-1.2 - The applying entity will, no later than delegation of the TLD, establish, publish, and provide to ICANN the location of a mechanism for members of the public to submit reports of abuse in accordance with the current obligations of the Base RA and any Consensus Policies.

SC5.2-1.3 - The applying entity has developed proposed measures for removal of orphan glue records for names removed from the zone when provided with evidence in written form that the glue is present in connection with malicious conduct (see Specification 6).

SC5.2-1.4 - The applying entity has or will have at time of delegation, established policies for handling complaints regarding abuse. Such policies are to be maintained and posted publicly so that anyone can review the policies via the Internet and any other means deemed appropriate by the applying entity. The applying entity's policies at a minimum should contain appropriate confirmation of the receipt of the abuse report, the process of review of the report, and actions that will be taken if the applying entity confirms the report is legitimate.

SC5.2-1.5 - The applying entity understands that DNS Abuse is Phishing, Malware, Botnets, Pharming and Spam (when used to deliver other forms of DNS Abuse). The applying entity understands and is prepared to contribute to the mitigation or disruption of DNS Abuse in domains in the TLD zone.

SC5.2-1.6 - The applying entity's abuse response capabilities are resourced appropriately to ensure a timely and adequate investigation and response to reports of DNS Abuse. This includes capabilities to receive and evaluate evidence of DNS Abuse in reports, and to take action to stop or disrupt the DNS Abuse.

SC5.2-1.7 - The applying entity is prepared to conduct periodic scans of its zone to identify if domains are being used to perpetrate DNS Abuse, and to maintain statistical reports of the scans, the findings, and actions taken.

If Partner NGO, at its discretion, elects not to enter into a definitive Registry Operation Agreement, DotAsia will still continue its Pro Bono support and mentorship for the ASP to provide our guidance, experience and knowledge to Partner NGO, as well as funding support according to the said Letter of Unconditional Funds Support with the addition of operational funding support as put forth in Q213-219 until alternative funding is identified, such that it can deliver on the above commitments for the purposes of operating the New gTLD.

For the avoidance of doubt, as set forth and in alignment with the MOU, any agreement in furtherance of the above shall not allow DotAsia to exercise or have the ability to exercise (or will exercise or will have the ability to exercise) direct or indirect control over: (i) the operations, management, or policies of Applicant or any of its affiliates; or (ii) the applied-for gTLD (to the extent applicable), if different from Applicant, whether by ownership interest, contractual rights or otherwise.

Yours sincerely,



Edmon CHUNG
Chief Executive Officer
DotAsia Organisation