Context

Under CoCCA's gTLD commercial model;

- The SRS uses CoCCA's pamoja software, no sensitive financial information (complete credit card details, bank account information) is stored in the SRS database.
- The SRS is a repository of a compilation of data that is readily available to the general public via WHOIS, RDDS, Historical Abstracts, and Drop Lists. The only sensitive or confidential information stored in the SRS are registrar and administrative login credentials and domain / contact AuthCodes, both these object types are encrypted. Even if decrypted, without the OTP token device, a CoCCA secure certificate and White-Listing of a source IP address, the credentials cannot be used to gain un-authorized access to the CoCCA's production SRS system.
- DNS Anycast is outsourced to established respected Anycast providers Packet Clearing House (PCH) and Internet Software Consortium (ISC). They each have their internal security policy for managing their respective Anycast / Unicast networks. Neither PCH nor ISC have any form of access to appliances in CoCCA's primary SRS – nor does CoCCA have access to their platforms. A breach of security at any one of the Anycast providers does not have an impact on the security of the SRS database.
- DNSSEC Key Storage and Zone signature is outsourced to PCH who has infrastructure and security that rivals that used by ICANN to secure the root. PCH does not have any form of access to appliances at our Sydney NOC nor does CoCCA have any access to the PCH key storage or signing platform.
- The distribution of signed zones files is done by CoCCA using TSIG and AXFR and IXFR - zones are validated by CoCCA and not "released into the wild" by PCH.
- Registry Operators –who contract CoCCA to provide back end registry services run completely autonomous systems for marketing, administration etc., there is no inter-connection of networks nor physical or remote access to appliances in the CoCCA NOC provided to Registry Operators or their staff.
- CoCCA does not host any SRS supporting applications for ourselves or others in the NOC - email, accounting, corporate websites ticket tracking etc. CoCCA hosts those on Virtual Private Servers in the cloud. None of these cloud servers have white-listed IP connections to the NOC.
- 24/7/365 Registrar Support, NOC Support / Monitoring and front line Complaint Resolution for Critical Issue Suspensions ("CIS" and URS) are "roles" carried out by the same individuals concurrently. This makes economic sense, as CoCCA's NOC Support needs to be aware of SRS status to support registrars and also requires a level of access to the SRS GUI that allows them to trigger suspension or investigate glue records or other reported abuse.
- CoCCA exists largely as a virtual entity with fewer than 20 individuals (scattered across the globe) involved in providing Registry Services or developing the pamoja software. Only six are Systems Administrators with any form of remote or physical access to the SRS appliances. The office in Auckland NZ where software development takes place has two full time developers who connect to the NOC via the cloud (there are no Administrative networks or servers), an ADSL link, several iMac desktops, a multi-function printer scanner is the only LAN CoCCA maintains.
- The current Failover and Escrow SRS are hosted on virtual private hosts; they have the same functionality as the Sydney NOC but not the same level of

performance, redundancy or security. CoCCA is currently hosting ccTLDs without the SLA's required by ICANN, in early 2013 - or earlier if gTLDs using our platform are approved, the Palo Alto SRS will be upgraded and a new one in Paris will be fitted out so that they mirror the current Sydney NOC in terms of High Avalability and Redundancy.

- CoCCA's SRS services are only provided from tier 3 data centers that have strict access polices and will not allow any physical access to individuals that have not been formally "inducted"- ID checked, undergone training and clearance by the Data Centre, been and photographed etc.

Should any of the above change substantially then this Security Policy would be updated as required.

Policy & Rules:

Location of Primary or Failover SRS: SRS equipment will only be located in Tier-3 data centers with 24/7 security, video monitoring of access to SRS equipment and technology that allows tracking of individual access to the cage where the SRS appliances are housed. SRS appliances shall be in private, locked racks with keys held only by CoCCA Systems Administrators (not Data Center staff or consultants).

DNSSEC: Keys shall be stored offline, in a facility that complies with best practices and approximates the level of security used by ICANN to secure the Internet root.

Physical Access to SRS Appliances: Only CoCCA Systems Administrators are to be granted any form of physical access to SRS appliances, if a consultant needs to do maintenance on any appliance in a CoCCA rack they must do so only in the company of a CoCCA Systems Administrator.

Prohibition on Collateral Applications: Only software and hardware essential to providing core Registry Services shall be located inside or loaded on an appliance inside the NOC. By way of example, no email services, helpdesk applications, public facing websites (not related to a critical registry function like BIND, EPP or RDDS) shall be installed on servers. All installations or upgrades to software and hardware shall be logged in the inventory.

Software Updates & Security Licences: Software shall be kept current with the latest stable versions, licences that support enhanced features or allow appliances to access the latest firmware or software releases shall be kept current.

Remote Access to SRS | NOC: Access to the NOC GUI, required by Registrars, NOC Support, Registrar Support, Complaint Resolution Service Officers, Ombudsman, CERT Law Enforcement and TLD Managers ("Registry Operator" or "Sponsoring Organization") shall be only via a web-based SSL encrypted web site, from trusted IPs, and require user name, password and OTP token. Wherever possible browser certificates should be employed as well for users with a high level of access.

- The level of access granted in the Registry's administrative interface shall be commensurate with the role of the individual accessing the system. Users shall ensure the workstation or device they are using to access the SRS has current virus or other security software installed.

- All remote access shall be logged by the firewall and servers, and the logs backed up as part of the veeam replication and backup of vm of disk images. These images shall be compressed and shipped daily offsite (NZ).

- Access by non-administrators shall be to the SRS GUI on port 443 only, white listed IP addresses for non-administrators shall only open port 443 or port 700 if they are a registrar who uses EPP.

- Network appliances (firewalls, routers, switches, load balancers) that have a web based management GUI should either have the GUI disabled or made available only from white listed IPs or the LAN.

- Remote logins to servers using the root password shall not be allowed.

- Remote logins by command line should require two factor authentication using PAM and OTP.

- If an administrator needs access while on the road then they must use an IPSec VPN client for OSX that supports Extended Authentication (XAUTH) with OTP, OTP should be enabled for all VPN users.

CoCCA's SRS Software: Independent third party performance and security audit shall be carried out with each major release.

Employment: CoCCA only hires from the talented pool of individuals it has worked with in one capacity or another supporting the administration of existing ccTLDs or gTLDs. CoCCA does not do security or background checks.

On Termination: The System Administrator's OTP device and login credentials shall be deleted.