auDA Information Security Standard (ISS) for Accredited Registrars

Jo Lim

Chief Operations and Policy Officer

.au DOMAIN ADMINISTRATION LTD

Contents

1. Background

2. ISS Policy and ISS Compliance Program

3. Other Policy Changes

.au DOMAIN ADMINISTRATION LTD

Registrar Security Group

- Established by auDA in November 2011 to consider ways of improving registrar security

- Reps from auDA, AusRegistry, DistributeIT, Uber Global, Melbourne IT, Enetica, NetRegistry Group, assisted by security consultants Vectra Corp

.au DOMAIN ADMINISTRATION LTD

Objectives

- To assist registrars to manage and improve the security of their own businesses – develop a “security culture” among registrars

- To protect .au registrants and the integrity and stability of the .au domain space

Draft ISS

- Sets mandatory baseline standard for information security for registrars
- Flexible, adaptable to different registrar business models
- Aligned to well-established international standards (ISO 27001, PCI DSS)
- Risk-based – registrars do their own risk assessment and select appropriate security controls

.au DOMAIN ADMINISTRATION LTD

2012 Industry Advisory Panel

- 22 Panel members including registrars, resellers, consumers, government, legal
- Two rounds of public consultation
  - all registrars contacted for comment
- Universal support for mandatory registrar security standard
- Final recommendation to auDA Board approved in February

.au DOMAIN ADMINISTRATION LTD

ISS Policy – published today!

- ISS document is attached to the policy as separate Schedule A
- Policy sets out:
  - ISS Compliance Program
  - consequences of non-compliance with ISS
  - ISS phase-in period for existing registrars
- auDA will bear all ISS costs – not including registrar internal costs

.au DOMAIN ADMINISTRATION LTD

ISS Compliance Program

- Vectra Corp appointed as provider of ISS assessment services
- Two assessment processes:
  - registrar self-assessment via online ISS Compliance Portal (TruComply)
  - on-site assessment by ISS Assessor
- All registrars must pass both processes for initial ISS compliance

.au DOMAIN ADMINISTRATION LTD

ISS Compliance Program

- ISS Assessor will provide report to ISS Committee for final sign-off
  - comprises senior auDA and AusRegistry reps plus independent person
- ISS Committee will issue ISS Compliance Certificate to registrar
  - registrar may choose to display ISS Compliance Mark

.au DOMAIN ADMINISTRATION LTD

ISS Compliance Program

- ISS Compliance Certificate valid for 3 years
- Registrars may be required to undertake one or both assessment processes annually or at other intervals determined by ISS Committee
- auDA may require registrar to undertake one or both processes:
  - change of ownership
  - security breach
  - formal complaint

.au DOMAIN ADMINISTRATION LTD

Consequences of non-compliance

- Applies to registrars who do not complete the ISS Compliance Program, or are assessed as non-compliant after 3 month remediation phase
- auDA reserves the right to:
  - suspend accreditation
  - issue public notice
  - terminate accreditation after 3 month suspension

ISS phase-in period

- Existing registrars must be ISS compliant within 24 months of today's date – 17 Oct 2015
- ISS compliant registrars will be listed on auDA's website
- **We welcome all feedback and suggestions for improving the compliance and assessment process** ☺
- Full review of the ISS will be conducted following the phase-in period

.au DOMAIN ADMINISTRATION LTD

Other policy changes

- Registrar Accreditation Criteria updated to include ISS compliance

- Registrar Application Form updated to include ISS compliance as final stage of provisional accreditation, prior to full accreditation

For more info:

Lujia Chen - lujia.chen@auda.org.au
Jo Lim - jo.lim@auda.org.au