Handling confidential information Overview

Note: Sensitivity and attribution determined by info-provider	**Sensitive**	**Not sensitive**
Not attributed to source (transmitted through trusted 3rd party or summaries of Type 1 developed by sub-group)	Type 2: Distributed to sub-groups. (Sub-groups determine ultimate distribution)	Type 3: Distributed to DSSA and public ("sanitized" info from sub-groups)
Attributed to source	Type 1: Distributed to sub-groups only (under NDA, most-protected)	Type 4: Distributed to public

Dimensions

- Dimensions
  - Sensitivity
    - Options
      - Sensitive
      - Not sensitive
    - Nature
      - Data (for analysis)
      - Internal processes
      - Trade secrets
    - Decision made by information-provider
    - May require compartmentalization across sub-teams
  - Attribution
    - Options
      - Attributed to source
      - Not attributed to source
    - Decision made by information-provider
    - Non-attributed info transmitted through trusted 3rd party or from sub-team "sanitizing"
  - Distribution
    - Options
      - Distribute to the public
      - Distribute to sub-groups
      - Sub-groups decide distribution for sensitive information

Use cases

- Use cases
  - Type 1
    - Sensitive, attributed
    - Distribution to sub-teams only
    - Governed/enforced by DSSA NDA (and project/use-specific NDAs if needed)
    - Highest standard of protection
  - Type 2
    - Sensitive, not-attributed
    - Distributed to sub-teams only
    - Transmitted through trusted 3rd party or summaries of Type 1 information developed by sub-group
    - Sub-team determines ultimate distribution
  - Type 3
    - Not sensitive, not attributed
    - Distributed to the DSSA and ultimately the public (via email list, wiki, report, etc.)
    - "Sanitized" information developed by sub-groups
    - Primarily Type 2 information that has been approved for release by the sub-group that developed it
  - Type 4
    - Not sensitive, attributed
    - Distributed to the public (via email list, wiki, report, etc.)

Open questions

- Mechanisms needed
  - Tracking membership
    - In DSSA?
    - In sub-groups
- Open questions
  - Code of conduct for group -- is the charter sufficient?
    - Preliminary answer: charter is sufficient
  - Who is the trusted 3rd party for transmitting non-attributed information?
    - ICANN staff?
    - DSSA member?
      - (under special NDA?)
    - Contracted provider (lawyer, consultant)?
    - Anonymous system (NEISAS, remailer, drop-box, etc.)?
    - Preliminary answer: TBD

Charter

- Principles
  - Sub-working groups may need to access sensitive or proprietary information in order for the DSSA to do its work
  - These procedures are an exception to accountability and transparency standards
  - No formal NDA required for membership in the DSSA
- Sub-working groups
  - Only required where members of sub-working groups need to access and protect confidential information
    - If needed: sub-WG members sign formal Affirmation of Confidentiality and Non-Disclosure agreement
    - If needed: project or issue-specific Non-Disclosure Agreement
    - If needed: separate private sub-working group email lists