# All Partners Access Network – Community Owner Guidelines

## 1. OVERVIEW

This document will provide APAN Community Owners with guidelines related to administering APAN Communities, (and sub-communities, if applicable) including:

a. Community Owner responsibilities and managing membership access

b. Information Security resources and protection for communities that have been granted approval to share CUI

c. Identifying available APAN training resources

## 2. COMMUNITY OWNER RESPONSIBILITIES

a. An APAN community is any site, group, portal, information page, virtual meeting room or any other type of collaborative workspace that is hosted on APAN platform applications

b. Community Owners are responsible for authorizing user access to as well as managing any data/content contained within their community

   i. Vet users requesting access

   ii. Prior to granting access, validate need-to-know

   iii. Where applicable, limit the number of members who can post information

   iv. Review community activity regularly to ensure postings are appropriate; immediately remove content that is inappropriate

   v. Limit the amount of member contact details available within the community

c. Community Owners are also responsible for any sub-community under the parent community and must only create sub-communities (and retain ownership of such) if they directly relate to the parent community

d. Community Owners who are new to the APAN platform must attend community owner training offered by APAN staff in order to become familiar with how to properly use the capabilities and understand application-specific access/permission settings

## 3. POINT OF CONTACT (POC) INFORMATION / RECORDS

a. The primary community owner - usually the original requestor, *and* any subsequent members assigned the *owner role* - must complete and sign **an APAN Community Owner Acknowledgment (COA) form**: https://community.apan.org/support/m/info/139434

b. Existing owners must ***not*** apply full access or "owner" permissions to another user's account unless he/she sends a signed COA form to the APAN team

c. It is the Community Owner's responsibility to provide APAN with up-to-date POC information for each community owner

d. In the event that the Community Owner transitions or otherwise leaves their position, the Owner is required to provide APAN with replacement POC information

e. APAN may implement deletion procedures if owners are unresponsive to community member requests after 6 months

f. Input/update POC and community information by submitting a ticket (include the URL for the community): https://community.apan.org/support/p/contact

## 4. MANAGING MEMBER ACCESS REQUESTS

a. Vetting Membership Requests

   i. Be certain to review request for authenticity; review user profile to obtain positive ID; verify email address; identify other communities the user is associated with; call user, and/or reach out to APAN Support regarding questionable membership requests

b. Membership Vigilance

   i. Actively review community access levels and permissions - it is each Community Owner's responsibility to know who can view their community and at what privacy level the community has been designated

   ii. ***Be aware***! Membership approval can be a single point of failure in security. Avoid users attempting to gain access through fake user accounts; follow recommendations for vetting pending member lists

   iii. Promote users to minimally required membership level only; limit the number of members promoted to owner or management roles or who may have advanced permissions

   i. Actively review and purge content as necessary for information security and to keep the community current

## 5. INFORMATION SECURITY TRAINING RESOURCES & REFERENCES

a. All APAN end-users (and Community Owners in particular) must review and be familiar with the following references and/or training resources before attempting to publish or share information on the APAN platform:

   i. **Cyber Awareness Challenge**: https://public.cyber.mil/training/cyber-awareness-challenge/

   An overview of cybersecurity threats and best practices to keep information and information systems secure. Every year, authorized users of the DoD information systems must complete the Cyber Awareness Challenge to maintain awareness of and stay up-to-date on new cybersecurity threats. The training also reinforces best practices to keep the DoD and personal information and information systems secure and stay abreast of changes in DoD cybersecurity policies. Other agencies use the course to satisfy their requirements as well.

   ii. **Identifying and Safeguarding Personally Identifiable Information (PII)**: https://public.cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/

   An overview of Personally Identifiable Information (PII), and protected health information (PHI), a significant subset of PII, and the significance of each, as well as the laws and policy that govern the maintenance and protection of PII and PHI. The course is designed to prepare DoD and other Federal employees to recognize the importance of PII, to identify what PII is, and why it is important to protect PII.

   iii. **OPSEC Awareness for Military Members, DoD Employees and Contractors**: https://securityawareness.usalearning.gov/opsec/story.html

   Provides OPSEC awareness for military members, government employees, and contractors. The course provides information on the basic need to protect unclassified information about operations and personal information to ensure safe and successful operations and personal safety.

   iv. **National Information System Security INFOSEC Terms** (NTISSI No. 4009); also known as Committee on National Security Systems Instruction (CNSSI) No. 4009: https://www.cnss.gov/CNSS/openDoc.cfm?kd9wEtCGLSCaUN4H3N0YsQ==

   This instruction applies to all U.S. Government Departments, Agencies, Bureaus and Offices; supporting contractors and agents; that collect, generate process, store, display, transmit or receive classified or controlled unclassified information or that operate, use, or connect to National Security Systems (NSS), as defined therein.

## 6. CONTROLLED UNCLASSIFIED INFORMATION (CUI)

a. CUI is a document handling designation, not a classification. This may be used by DoD and other Federal agencies to identify information that is not appropriate for public release. As a Community Owner, it is important to understand the proper DoD and USG guidelines, categories, and policies for handling this data and also understand your organization's specific information management policies.

b. APAN is certified and accredited up to unclassified at Impact Level 4 (IL4)

c. APAN is authorized to host information designated as CUI ***only with approval from the APAN Technical Director***

   i. This authorization is granted on a case-by- case basis by request. *Refer to the APAN CUI SOP at* https://community.apan.org/support/m/info/262862 *for complete details and instructions*

d. Any "unauthorized" CUI found within an unapproved APAN community will be permanently deleted

## 7. CUI COMMUNITIES RULES OF ENGAGEMENT

*Guidance in sections 8-9 only applies to APAN communities which have successfully completed CUI process requirements and are already approved to host and store CUI by the APAN Technical Director*

a. Community owners are required to review the SOP at https://community.apan.org/support/m/info/262862, complete the APAN CUI process and receive approval from the APAN Technical Director ***before*** any CUI content is posted to the community

b. All CUI community owners must notify their APAN KM representative or the APAN Help Desk *before* attempting to create sub-communities and/or utilize Adobe Connect, ArcGIS, or chat, if not already identified on their CUI request form

   i. Community owners must not create sub-communities under a parent CUI community if those sub-communities are not also designated CUI

c. Only APAN administrators can activate the CUI banner that denotes authorized/approved status on the APAN platform; sub-communities are *not authorized* if owners do not notify APAN Support Staff!

d. For specific questions about APAN CUI processes, please contact APAN support at https://community.apan.org/support/p/contact

## 8. CUI SHAREPOINT (SP) SITES:

*Owners must abide by the following rules:*

a. All sites will be set to **no searching** and **no offline client downloads**
   i. Click *Site Actions > Site Settings*
   ii. Within the Site Administration, locate *Search and Offline Availability*
   iii. Set all three options to: ***No***

b. Alerts must *not* be set for any lists or libraries contained on a CUI site, as notification emails might post CUI content to third-party email clients (the alerts option is disabled by default)

c. Unique access permissions at the list/library/page or content level must be diligently reviewed

d. All SP owners must verify that *anonymous access is turned off*
   i. The "All Windows Users", "NT Auth" or similar entire enterprise directory-level permission groups **must not be used**

## 9. CUI TELLIGENT GROUPS:

*All CUI groups must be set to **Private Unlisted** access only. No exceptions.*

a. Each user will have to be manually added to the group by an owner

b. APAN users will not be able to request access as Private Unlisted communities are not searchable

c. Sharing the link via email will not work; a user must be a member of that community in order to access a Private Unlisted group

d. Owners must not change the permission access for individual Telligent application containers (wiki, gallery, blog, forum)

## 10. RESOURCES AND TRAINING

| | |
|---|---|
| APAN University | https://community.apan.org/support/p/apanu<br>Enroll in live-training Webinars, view recorded webinars, request individual training sessions for you and/or your team and review demo communities<br>Find tips and other resources to assist with community ownership |
| Help Desk Hotline | https://community.apan.org/support/p/contact<br>COMM: 808-472-7855<br>DSN: 315-472-7855 |
| Knowledge Base | https://community.apan.org/support |
| News and Updates | https://community.apan.org/support/b |
| Resources | https://community.apan.org/support/m/info |

## 11. CONCLUSION

a. APAN is an **UNCLASSIFIED** DoD information system, all data contained on the communities should be publicly releasable without violating Federal Laws or DoD Policies

b. It is every user's responsibility to ensure that all unclassified information residing on APAN Communities is cleared for public release before uploading or publishing content

c. There is a separate approval process for CUI on APAN; SOPs, policies and guidance must be followed to protect CUI

d. Community Owners are required to complete information security training and be familiar with resources & references; they must be vigilant in identifying potential information security violations and vetting users for membership

e. Communities that are found to repeatedly violate standards will be suspended, and Community Owner rights will be revoked, pending refresher training and/or community "policing" - continued problems will be brought to the attention of the APAN Technical Director and the community may even be removed from the APAN platform