STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS	APPLICABILITY **DEPARTMENT WIDE**		
	REVISION DATE 7/22/22	**PAGE NUMBER** 1 of 4	**NUMBER** **DOC 470.500**
POLICY	**TITLE** **SECURITY THREAT GROUPS**		

REVIEW/REVISION HISTORY:

Effective: 1/28/02 DOC 400.310
Revised: 1/14/05
Revised: 12/4/06
Revised: 11/21/08
Revised: 8/6/10
Revised: 12/15/12 DOC 470.500
Revised: 4/19/19
Revised: 7/22/22

SUMMARY OF REVISION/REVIEW:

Updated title
I.A., II.B., III.A.1., III.B., IV.A., IV.A.1., and IV.B. - Adjusted language for clarification
II.A.4. - Removed unnecessary language
II.B.5. - Added language for clarification
Removed III.A.2.a. that the STG contact will document and evaluate information from outside sources
Removed III.A.3. that information/documentation will be scanned in the STG SharePoint site

APPROVED:

Signature on file

CHERYL STRANGE, Secretary
Department of Corrections

6/28/22
Date Signed

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; RCW 72.09.745

POLICY:

I. The Department has established a system to identify and monitor the movement and activities of individuals it supervises and associated groups who pose a potential threat to the security or safety of employees, contract staff, volunteers, visitors, other individuals under the Department's jurisdiction, criminal justice partners, and the community.

DIRECTIVE:

I. General Requirements

A. Information maintained on the Security Threat Group (STG) SharePoint site and in the STG database in the electronic file is confidential information and intended for the sole purpose of authorized employees. Limited information will be available to all other employees.

1. The STG Coordinator/Chief of Investigations will evaluate the need for full access for employees. Employees must make at least one entry every 6 months to maintain access.

B. Information will not be copied, printed, or disseminated to anyone without the approval of the STG Coordinator/Chief of Investigative Operations.

II. Responsibilities

A. The Headquarters STG Coordinator/designee will:

1. Maintain a statewide STG database
2. Review submitted validations and determine STG status
3. Act as liaison with law enforcement and/or other intelligence groups (e.g., regional intelligence groups, joint analytical centers, joint terrorism task forces)
4. Provide information and analysis to employees upon request
5. Provide training on STG-related issues

B. Each facility/section will designate an employee to act as the facility/section STG contact person, who will:

1. Identify suspected STG affiliation via the assessment/validation process
2. Investigate incidents where there is suspected STG involvement

3. Serve as the liaison for the STG Coordinator and law enforcement
4. Enter STG-specific information pertaining to individuals into the STG database
5. Scan documents supporting validation into the STG SharePoint site, including DOC 21-881 Security Threat Group Membership Assessment

III. Security Threat Group Membership Identification and Validation

A. Assessment and Documentation

1. Individuals on community supervision and incarcerated individuals entering or transferring within the Department will be assessed for STG affiliation, which will include, but not be limited to:

   a. Completion of DOC 21-881 Security Threat Group Membership Assessment and entering of STG information in the STG database

      1) Employees who identify STG-specific information will complete DOC 21-881 Security Threat Group Membership Assessment and forward to the STG contact person.

      2) The STG contact person will evaluate the information and update the STG database when applicable.

   b. Interviews

   c. Documentation of objective information and photographs of scars, marks, and tattoos relevant to STG

   d. Notifying the individual of the dropout process

      1) New arrivals will be notified during facility orientation. Affected individuals will be notified as needed by the Intelligence and Investigations Unit (IIU).

      2) Individuals on community supervision will be notified by the section STG contact person.

2. All information and supporting documentation will be reviewed by the STG contact person, who will enter any missing information not in the STG database.

   a. Documentation from external sources will include identification of the source.

B. Investigation and Validation

1. STG affiliation will be determined based on the criteria listed on DOC 21-881 Security Threat Group Membership Assessment as follows:

   a. One criterion must be met to have STG Suspect status
   b. Two criteria must be met to have STG Affiliate status
   c. Three criteria must be met to have STG Member status

2. The STG Coordinator will determine STG status after a complete review of the submitted criteria.

IV. Debrief/Appeal

A. Individuals who wish to participate in the debriefing process must submit a written request to the facility IIU Chief Investigator/section STG contact person.

1. The IIU Chief Investigator/section STG contact person will consult with the STG Coordinator to determine next steps.

2. All debriefing documentation will be forwarded to the STG Coordinator upon completion.

3. The STG Coordinator will determine if the debrief is accepted and should conduct an interview and verify the information obtained.

B. Individuals who wish to appeal being identified as a suspect, affiliate, or member in the STG database must submit a written request to the Senior Director of Comprehensive Case Management.

DEFINITIONS:

Words/terms appearing in this policy may be defined in the glossary section of the Policy Manual.

ATTACHMENTS:

None

DOC FORMS:

DOC 21-881 Security Threat Group Membership Assessment