TENNESSEE VALLEY AUTHORITY

EMPLOYEE CONCERNS TASK GROUP

PROCEDURE

ECTG A.2

FILING AND PROTECTION OF SENSITIVE INFORMATION

INTERIM ☐
CURRENT REVISION LEVEL: FINAL ☒ 3

PREPARED BY: Technical Assistance Staff

REVISED BY: Technical Assistance Staff

APPROVED BY: W R Brown

DATE APPROVED: 3/14/17

0683T

HISTORY OF REVISION

REV NUMBER	PAGES REVISED	REASON FOR CURRENT REVISION
1	All	General Revision.
2	1	Remove Reference 2.2.
	4	Clarify filing requirements.
	6	Correct paragraph reference.
3	Cover sheet, 3, 4, and 5	Revised to enhance requirements and include nonsensitive file maintenance and control.

PROTECTION OF SENSITIVE INFORMATION

1.0 PURPOSE/SCOPE

The purpose of this procedure is to identify responsibilities and to establish methods for the receipt, maintenance, management, and control of access to sensitive and nonsensitive information. This includes expurgated Quality Technology Company (QTC) Employee Concern interview and evaluation files, unexpurgated files relating to previous TVA programs while in the control of the Watts Bar Nuclear Plant (WBN) Employee Concerns Task Group (ECTG), employee concern files which do not contain sensitive information, and ECTG Administrative files.

2.0 REFERENCES

2.1 Program Procedure ECTG M.1, "Employee Concerns Task Group Program Procedure."

3.0 DEFINITIONS

3.1 Sensitive Information - Information that specifically documents the interview process which QTC conducted with TVA employees and which further addresses the investigative process (if available) that resulted from the interviews. This data developed during the interview and any other information that might identify the interviewee will be masked (i.e., expurgated) by the contractor or NRC prior to TVA taking possession of the files. This also includes any information deemed as Sensitive Information by the ECTG Program Manager. Sensitive Information includes some unexpurgated files of previous programs conducted by TVA.

3.2 Need to Know - A determination made by the ECTG Program Manager/CEG-H/PC&A supervision that a proposed recipient's access to Sensitive Information is necessary in the performance of official, contractual, or other duties of employment.

3.3 Security Storage Container - The following defined repository is acceptable:

3.3.1 A steel filing cabinet equipped with a steel locking bar and a three-position, changeable combination, General Services Administration (GSA) approved padlock for storage of Sensitive Information in a building located within a controlled access area (e.g., Central Office).

3.4 Working Files - Files that are essential to the ECTG Program and do not contain any unexpurgated information but are necessary for day-to-day operations of the ECTG Program.

3.5 Administrative Files - Files that are required for the control and administration of the ECTG Program.

3.6 Sensitive Class 1 Files - Files that may have unexpurgated sensitive information.

3.7 Sensitive Class 2 Files - Files that may have been expurgated of all confidential information and completed case files.

3.8 Review Area - An area designated for the protective storage containers and file review worktables associated with the safekeeping of the Sensitive Information.

4.0 RESPONSIBILITIES

4.1 The Employee Concerns Task Group (ECTG) Program Manager shall appoint a Control Officer (CO) who shall be responsible for the administration of the Employee Concerns Sensitive Information Program.

The ECTG Program Manager shall make the final determination concerning the classification of and access to documents. Decisions to change the classification of information shall be made by the ECTG Program Manager on a case-by-case basis.

4.2 The CO may designate others, in writing, as Assistant Control Officers (ACOs). The ACOs shall have the authority to control access to sensitive information.

4.3 The CO or appointed ACO shall be responsible for the day-to-day operation of the document control activities and the associated area.

5.0 PROCEDURE

5.1 Access To Sensitive Class 2 Files

5.1.1 Except as TVA may authorize (by determining the need to know - see paragraph 3.2) or as required by law, no person shall have access to Sensitive Class 2 File Information unless the individual has established a "need to know" for the information and qualifies as one of the following:

5.1.1.1 An employee, agent, or contractor of TVA, NRC, or the United States Government.

5.1.1.2 A member of a duly authorized committee of the United States Congress.

5.1.2 TVA or its Contractor--or any other person having possession of Sensitive Information--have significant discretionary authority in making the determination that a proposed recipient's access to Sensitive Information is necessary in the performance of official, contractual, or other duties of employment.

5.1.3 Category Evaluation Group Heads (CEG-Hs) and the PC&A Staff Supervisor shall provide the CO with a list of names of individuals from their respective sections/units who are authorized access on a "need to know" basis. This list should be updated on an "as needed" basis.

5.2 Access To Sensitive Class 1 Files Information

5.2.1 Except as authorized in writing by the ECTG Program Manager, and/or as required by law or a court of competent jurisdictional authority, no person shall have access to Sensitive Class 1 Information.

5.3 Sensitive Information Protection While In Use Or Storage

5.3.1 Sensitive Information documents shall be under the control of an individual with authorized access. Documents shall be deemed as being "under control" if material is attended even though it is in fact not constantly being used.

5.3.2 When unattended, Sensitive Information documents shall be stored in a locked security storage container, as defined in paragraph 3.3.

5.3.3 The combination for the locks on the security storage containers should be issued and protected in a manner that limits the knowledge of lock combinations to the CO or ACO. An CO or ACO will change combinations when a combination is required to be changed. The CO or ACO will document the change using Attachment D. The CO will maintain a file of all Attachment Ds. Lock combinations should be changed under the following conditions:

5.3.3.1 A time interval not to exceed one year.

5.3.3.2 When a combination is suspected to have been compromised.

5.3.3.3 When an individual with knowledge of a combination is determined by the CO or ACO to no longer have a "need to know", (i.e., transfer, termination).

5.4 Initial Receipt Of QTC Files

5.4.1 Upon initial receipt of the expurgated files and associated documents, the Document Control clerk shall:

5.4.1.1 Verify the contents of transmitted packages against any transmittal documents that may have been used to ensure that all documents transmitted were received.

5.4.1.2 The CO will establish and maintain a File Control Log (Attachment A)

5.4.1.3 File the package in the appropriate file.

5.5 Access To Files

5.5.1 The authorized file requester shall execute the File Access Request and Sensitive Information Acknowledgement Form (Attachment B). The recipient shall be made aware that the information is Sensitive.

5.5.2 The Document Control Clerk, CO, or ACO shall:

5.5.2.1 Verify the requester against the Authorized Access List for Expurgated Sensitive Information or against written authorization of the Manager of Nuclear Power or the ECTG Program Manager for Unexpurgated Sensitive Information.

5.5.2.2 File Attachment B.

5.5.2.3 Pull the file.

5.5.2.4 Execute (in ink) the File Control Log.

5.5.2.5 Instruct the requester to work at a review table.

5.5.3 Upon completion of the file review, the Document Control Clerk, CO, or ACO shall:

5.5.3.1 Note the return on the File Control Log.

5.5.3.2 Return the file to the appropriate cabinet.

5.6 Filing System

5.6.1 The CO shall establish a filing system for the concern file packages as follows:

5.6.1.1 File in alphanumerical order as received within the agency or organization from which they were received; i.e., QTC: EX-85-001-001, EX-85-002-001, IN-85-001-001, IN-85-002-001

5.6.1.2 Filing cabinets located in the Central Files shall be labeled as follows:

- File cabinets that contain unexpurgated sensitive information shall be labeled as Sensitive Class 1.
- File cabinets that contain expurgated sensitive information and all completed case files shall be labeled Sensitive Class 2.
- File cabinets that contain the administrative files shall be labeled as administrative files.
- File cabinets that contain the working files shall be labeled as working files.

5.6.2 Access to Working Files/Administrative Files

5.6.2.1 Access to the Working files/Administrative files shall be controlled by the CO, ACO, or Document Control Clerk.

5.6.2.2 The Document Control Clerk shall place an out card in the files for any file that will be removed from the Central File Area.

5.6.2.3 The check-out card shall have the file number, name of individual checking out the file and the date the file is checked-out. When the file is returned the Document Control Clerk shall replace the check-out card with the file.

5.6.2.4 Administrative files will be located in the Central File under the control of the CO, ACO or Document Control Clerk.

5.6.2.5 The Administrative files will be separated into two (2) categories, "Routine Administrative" and "Administrative Confidential." The Routine Administrative files do not require any approval to review the files. The PC&A Supervisor shall provide the CO with a list of administrative files that are to be filed as Administrative Confidential.

5.6.2.6 Access to the Administrative Confidential files require approval of the PC&A Supervisor. When the PC&A Supervisor receives a request to allow an individual access to the Administrative Confidential files, the PC&A Supervisor will notify the CO that the requestor has authorized access.

5.6.2.7 Paragraph 5.6.2.3 shall be used for administrative files removed from the central files.

5.7 Reproduction And Destruction Of Matter Containing Sensitive Information

5.7.1 Expurgated Sensitive Information may be reproduced on pink paper; however, reproduction should be kept to a minimum. Unexpurgated Sensitive Information shall not be reproduced unless required by law or a court of competent jurisdictional authority and authorized in writing by the ECTG Program Manager. Reproduced material shall be given the same protection as original documents. The request shall be authorized via the File Reproduction Request form (Attachment C) and filed in the File Reproduction Request Log. All copies shall be stamped "COPY" in red ink.

5.7.2 Sensitive Information, when directed by the ECTG Program Manager, shall be destroyed by shredding. Shredded material may be disposed of as normal waste.

5.8 Transmission Of Documents And Material Containing Unexpurgated Sensitive Information

5.8.1 Documents and material containing Sensitive Information shall be enclosed in two sealed envelopes or wrappers. The inner envelope or wrapper shall be marked in a conspicuous manner "Sensitive Information." The outer envelope and wrapper shall contain the intended recipient's name and address, with no indication that the document inside contains Sensitive Information. This package may be transmitted by messenger/carrier; United States first-class, registered, express or certified mail; or by any individual authorized under section 5.0 of this procedure.

5.8.2 Except under extraordinary conditions, Sensitive Information shall be electronically transmitted only with the approval of the ECTG Program Manager.

5.8.3 The routing of Sensitive Information between sections at Watts Bar Nuclear Plant or TVA Divisions shall be through the in-plant or TVA mail or by hand-carrying, and only with the express approval of the ECTG Program Manager.

5.8.4 Hand-carrying Sensitive Information does not require any special packaging, as long as the material is physically turned over from one person to another and both individuals are authorized on a "need to know" basis to have possession of the material. The person transporting this material shall ensure the recipient understands that the document(s) they are receiving contain(s) Sensitive Information. Leaving a Sensitive Information package on someone's desk does not constitute hand-carrying.

5.8.5 To transmit Sensitive Information in the in-plant or TVA mail system, packaging shall be as described in paragraph 5.8.1 of this procedure.

5.9 Automatic Data Processing

Expurgated Sensitive Information may be processed or produced on an Automatic Data Processing (ADP) system, provided that the system is self-contained within TVA's facilities and requires the use of an entry code for access to stored information.

5.10 Compromise Of Sensitive Information

5.10.1 The CO or ACO(s) in receipt of Sensitive Information or in custodial charge of a Sensitive Information repository shall determine suspected or confirmed compromise. Some examples of incidents that may be determined, suspected, or confirmed as compromises are:

5.10.1.1 Sensitive Information that has been received but not properly transmitted.

5.10.1.2 Discovery of unsecured (unlocked) repository.

5.10.1.3 Observation or evidence of forcible entry into a Sensitive Information repository.

5.10.1.4 Sensitive information being found in an uncontrolled area.

5.10.2 Each section having custodial responsibility for Sensitive Information shall designate at least one individual--upon determination of a compromise--to inventory and report any losses or tampering where applicable.

5.10.3 The CO shall be notified immediately and informed of details and shall initiate an investigation to determine the circumstances of the incident.

5.10.4 The subsequent Investigation Report shall be placed in the corresponding Sensitive Information file.

5.11 Permanent Storage

At the completion of the evaluation process/phase of the ECTG program, the files shall be transferred to a controlled storage facility yet to be determined for permanent storage.

6.0 ATTACHMENTS

Attachment A, File Control Log.

Attachment B, File Access Request And Expurgated Sensitive Information Acknowledgement

Attachment C, Expurgated Sensitive Information File Reproduction Request.

Attachment D, Sensitive Information Lock Combination Change Form

File Number_____

FILE CONTROL LOG

DATE ACCESSED	REQUESTER	TIME OUT	BY	TIME IN	BY	NOTES (REPRO, ETC.)

FILE ACCESS REQUEST AND EXPURGATED SENSITIVE INFORMATION ACKNOWLEDGMENT

I hereby request access to case file number _____.

It is understood that access to this information is needed by me in the conduct of an official inquiry and that this information will be treated as sensitive. I will not discuss this information unless there is a specific need to know. I further understand that improper use or discussion of this information could result in disciplinary action.

Acknowledged _____

Date _____

EXPURGATED SENSITIVE INFORMATION FILE REPRODUCTION REQUEST

I hereby request that _____ (number of copies) of

Pages: _____

of case file number _____ be reproduced and released to

Name: _____

Section: _____ for official use.

It is agreed that upon release (name) _____,

(unit) _____ will become the responsible custodian of the released information until such time as it is returned to this Document Control Section.

Authorized: _____
ECTG Program Manager

_____
Date

_____ _____
Received By Date

SENSITIVE INFORMATION LOCK COMBINATION CHANGE FORM

Date Combinations Changed: _____

Combinations Changed By: _____

Reason for Combination Change: _____

_____

_____

_____

Combination change complete and new combinations revealed to all ACO's _____ / _____

CO Date