8 August 2024

Interim Guidance for the Security Council Resolution 2589 Database

A. PURPOSE

1. The purpose of this Interim Guidance is to provide the framework and clarify relevant operational aspects for the further development, use and maintenance of the comprehensive online database on accountability for crimes against peacekeepers as mandated under paragraph 5 of Security Council resolution 2589 (hereafter "Security Council Resolution 2589 Database").[1]

2. The Security Council Resolution 2589 Database aims to implement the provisions of paragraph 5 of Security Council resolution 2589, as well as to further operationalize the provisions of the *Standard Operating Procedures on the Prevention, Investigation and Prosecution of Serious Crimes Committed Against United Nations Personnel in Peacekeeping Operations and Special Political Missions*[2], dated 1 December 2020. Accordingly, this Interim Guidance complements these Standard Operating Procedures and should be read and interpreted accordingly.

B. SCOPE AND RATIONALE

3. This Interim Guidance provides a general framework to regulate the operational aspects for the use and functioning of the Security Council Resolution 2589 Database. This Interim Guidance applies to all United Nations staff who have a direct or indirect role in the implementation of any of the responsibilities set forth in this document, or with respect to the development, use or maintenance of the Security Council Resolution 2589 Database. It also applies to Authorized Users designated by Member States.

C. DATA PROTECTION AND PRIVACY PRINCIPLES

4. The maintenance, operations, and use of the Security Council Resolution 2589 Database shall be consistent with the Personal Data Protection and Privacy Principles, adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018, and the provisions of ST/SGB/2024/1 (Data protection and privacy policy for personnel of the United Nations) including:

a) any processing and use of data is authorized solely for the purposes reflected in Security Council resolution 2589;

b) any processing and use of data is to be done in a fair manner and be relevant, limited and adequate in relation to the specified purposes;

c) data should be retained only for the time that is necessary for the purposes of the Security Council Resolution 2589 Database (and as reflected in the relevant records retention schedule);

d) data is to be accurate and up to date to fulfill the specified purposes

e) data is to be processed, kept and used with due regard to confidentiality; and

f) appropriate organizational and operational safeguards are instituted to ensure data security, including from unauthorized access.

[1] S/RES/2589 (2021), dated 18 August 2021.

[2] Ref. DPO 2020.18.

5. All United Nations staff[3] who have a direct or indirect role in the implementation of any of the responsibilities set forth in this document, or with respect to the use or maintenance of the Security Council Resolution 2589 Database shall follow key requirements and objectives set out in paragraph 4 above, and the procedures described below. Failure to do so may result in immediate removal of access rights and other measures as may be appropriate.

D. FUNCTIONAL DESCRIPTION AND OPERATIONAL PROCEDURES

6. The functional descriptions and technical procedures for implementing this interim guidance within the Security Council Resolution 2589 Database are set forth in the attached user manuals for administrators and case officers (hereafter "Manuals"). These manuals are considered subsidiary to this guidance, and must be read in conjunction with the guidance.

E. ACCESS TO INFORMATION IN THE SECURITY COUNCIL RESOLUTION 2589 DATABASE

7. The information contained in the Security Council Resolution 2589 Database is of a very sensitive nature and shall be classified and handled in accordance with the provisions of ST/SGB/2024/1 (Data protection and privacy policy for personnel of the United Nations) and ST/SGB/2007/6 (Information sensitivity, classification and handling) and the privacy provisions documented in Section C of this guidance. As provided for in Section 2 (Classification levels) of ST/SGB/2007/6, sensitive information may be classified as "confidential" or "strictly confidential". The designation "confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the United Nations. The designation "strictly confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the United Nations. The designation "unclassified" shall apply to information or material whose unauthorized disclosure could reasonably be expected not to cause damage to the work of the United Nations. The types of information and data that will be processed within the database is listed in the attached Access Rights Matrix. The focal point on accountability for crimes against peacekeepers of the Department of Peace Operations (DPO FP) shall maintain the Access Rights Matrix to ensure that it remains complete and up-to-date.

8. To secure the confidentiality of the information, access to the Security Council Resolution 2589 Database shall be restricted in accordance with an up-to-date Access Rights Matrix approved by the focal point on accountability for crimes against peacekeepers of the Department of Peace Operations (DPO FP). The DPO FP shall ensure that access is limited only to United Nations authorized users and designated representatives of Member States as described below (hereinafter "Authorized Users") in accordance with the Access Rights Matrix. The DPO FP shall limit the number of Authorized Users to those strictly in need of the information, with a view to minimizing risks of unauthorized disclosure of information. Authorized Users are strictly prohibited from disclosing their username and password to any other persons. Accessing the Security Council Resolution 2589 Database with another person's username and password and/or sharing them is strictly prohibited. All such limitations and conditions for access, including the obligations of staff to adhere to ST/SGB/2004/15 on the information and communication technology resources and data; the obligations of member states and the obligations of non-staff personnel shall be communicated when the account is established. The same message can be reinforced periodically and displayed to the user on login to the system. All access and activities performed within the system, including the changes to data, shall be audited at the system level. All changes to data, regardless of who made the modification, shall be displayed to users within the system as a change log.

9. Authorized Users are strictly prohibited from any unauthorized disclosure of any information contained in the Security Council Resolution 2589 Database. For United Nations staff and non-staff personnel , failure to comply with the requirements set out in this Interim Guidance may constitute misconduct.

[3] Includes Consultants for the purposes of providing IT Administration support.

10. In accordance with the Access Rights Matrix, the following variables for access rights should be used by the authorized IT administrator or DPO Administrator to customize users' access to the Security Council Resolution 2589 Database:

a) Users with read-only rights are only able to read the information they are authorized to access but cannot modify it. Users with read and modify rights are able to both read and modify the information they are authorized to access; and

b) Users can be given access to all cases contained in the Security Council Resolution 2589 Database, or only to certain cases, which are strictly determined on a need-to-know basis. This access can be limited to case files for a specific nationality (in the case of member state access), or a specific field operation for UN Staff.

11. Access for all roles, including the DPO FP, Mission Case Officer, UN Readers, Member States and IT Administrator shall be granted only by the DPO FP in accordance with the Access Rights Matrix. The following criteria shall be used by the DPO administrator to guide the granting of access rights to the Security Council Resolution 2589 Database:

a) Access rights to the Security Council Resolution 2589 Database are granted solely to United Nations staff directly involved in issues related to accountability for crimes against United Nations peacekeepers and non-staff personnel (IT Administrators) who need to access the system and its data to provide technical configuration and support as authorized by the DPO FP:

b) Access rights to the Security Council Resolution 2589 Database are granted to designated representatives of Member States in accordance with the terms established in the Note Verbale; and

c) Access rights to the Security Council Resolution 2589 Database are granted to users on a strict need-to-know basis. Therefore, authorized users only have access to the part of the information contained in the database that is directly relevant to their functions and activities. As such, a user's need to access information has to be balanced against the need to secure the confidentiality of information.

12. Access rights to the Security Council Resolution 2589 Database at the field level are decided on the basis of the above criteria by the Head of Mission or his/her designate, and in accordance with the Access Rights Matrix. Access rights to the Security Council Resolution 2589 Database at United Nations Headquarters, including by designated representatives of Member States, are decided by the Under-Secretary-General for Peace Operations, or his/her designate. In all cases, the granting of access is to be carried out by the DPO FP.

F. STRUCTURE OF ACCESS RIGHTS

13. There are four types of access rights to the Security Council Resolution 2589 Database, based on the following arrangements and as documented in the Access Rights Matrix:

a) The focal point on accountability for crimes against peacekeepers of the Department of Peace Operations (DPO FP), and his/her alternate, are authorized to have full access to read and modify all information (cases, capacity building, reports) and users in the Security Council Resolution 2589 Database;

b) The focal point (Case Officer) in the concerned peacekeeping operation, and his/her alternate, are provided by the DPO FP with full access to read and modify all information in the Security Council Resolution 2589 Database pertaining to their respective mission as part of their functions for data intake, review and/or approval;

c) United Nations staff may be granted access to the Security Council Resolution 2589 Database by the DPO FP, as readers in accordance with this Interim Guidance. ; and

d) Designated representatives from Member States may be granted access to the Security Council Resolution 2589 Database by the DPO FP as readers in accordance with this Interim Guidance. Member State's access will be limited to the cases concerning personnel of their own nationality and will include only the information as outlined in the Access Rights Matrix.

e) Non-staff personnel from OICT who are authorized by the DPO FP and have supplied an up-to-date non-disclosure agreement shall be assigned with IT Administrator role. These personnel shall have full access to read and modify all information (cases, capacity building, reports) and users in the Security Council Resolution 2589 Database; In addition, and as requested by, authorized by and inspected by the DPO FP, they shall be able to:

- Define/edit/delete roles in the system
- Manage country mapping for NOTICAS data
- Manage authorization structure

14. The list of Authorized Users, the configuration of roles and authorization structure shall be reviewed and updated regularly (on at least a quarterly basis) by the DPO FP in accordance with this Interim Guidance.

G. PROCEDURE TO FOLLOW TO REQUEST ACCESS TO THE SECURITY COUNCIL RESOLUTION 2589 DATABASE

15. The following procedure must be followed in order for a user to be granted access to the Security Council Resolution 2589 Database by the DPO FP in accordance with this Interim Guidance:

a) For United Nations staff and non-staff personnel (IT Administrators), a written request from the concerned individual should be submitted through his/her First Reporting Officer with a detailed justification to the person who is authorized to grant access in accordance with paragraph 12 of this Interim Guidance; and

b) For Member States, a note verbale with a detailed justification should be submitted by the concerned Permanent Mission or Mission for decision by the person who is authorized to grant access in accordance with paragraph 12 of this Interim Guidance.

H. DATA RETENTION

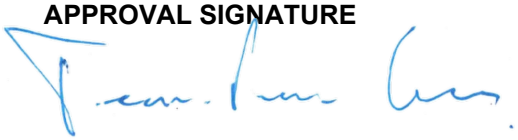
16.In principle, information in the Security Council Resolution 2589 Database should only be retained for the time that is necessary for the specified purposes set forth under paragraph 5 of Security Council resolution 2589. Notwithstanding, any destruction of data must be authorized by USG DPO in accordance with a retention schedule approved in accordance with ST/SGB/2007/5.

I. MONITORING AND COMPLIANCE

17. At the United Nations Headquarters, the focal point on accountability for crimes against peacekeepers of the Department of Peace Operations is responsible for monitoring the implementation of, and compliance with, the provisions of this Interim Guidance.

18. At each peacekeeping mission, the mission's focal point on accountability for crimes against peacekeepers is responsible for monitoring the implementation of, and compliance with, the provisions of this Interim Guidance at the mission level.

APPROVAL SIGNATURE



DATE OF APPROVAL

8 November 2024

Access Rights Matrix

Type of Information	Data Elements	Sensitivity	Access for Authorized Member State Personnel	Access for Authorized UN Staff(Reader)	Access for DPO Focal Point, and alternate (Administrator)	Access for Mission Focal Points (Case Officers)	Access for IT Administrator	Access for Administrator Assistant
List of Cases	Reference No, First Name, Last Name, Nationality, Type of Casualty, Date of Incident, Mission, Status	Confidential	**NO ACCESS** (Separate View for MS, refer below)	Read-only	Read and Write	Read and Write (Specific Mission)	Read and Write	**NO ACCESS**
Case Details	Reference No, Record Status, Incident Information (Country, Location Details), Personnel Information (Name, Gender etc.), Next of Kin Information (Name, Relationship etc.)	Confidential	**NO ACCESS** (Separate View for MS, refer below)	Read-only	Read and Write	Read and Write (Specific Mission)	Read and Write	**NO ACCESS**
Investigation Status / Prosecution / Adjustment of Cases	Current Status (No information available etc.), Referral Information (Date Referred etc.), Administrative Review (BOI Report Number etc.), Investigative Measures Taken (Date Taken etc.), Evidence Management Details (Evidence Type etc.), Alleged Suspect(s) / Perpetrator(s)	Confidential	**NO ACCESS**	Read-only	Read and Write	Read and Write (Specific Mission)	Read and Write	**NO ACCESS**

	(Name etc.), Follow-up Information (Date Followed Up etc.), Criminal Justice Process and Outcome Data (Date Convicted etc.)							
Assistance / Support Provided	Assistance / Support Provided (Type of Assistance etc.)	Confidential	**NO ACCESS**	Read-only	Read and Write	Read and Write (Specific Mission)	Read and Write	**NO ACCESS**
Key Lessons & Challenges / Recommendations	Key Lessons & Challenges / Recommendations (Description etc.)	Confidential	**NO ACCESS**	Read-only	Read and Write	Read and Write (Specific Mission)	Read and Write	**NO ACCESS**
Documents	Documents (Document Type etc.)	Strictly Confidential	**NO ACCESS**	Read-only	Read and Write	Read and Write (Specific Mission)	Read and Write	**NO ACCESS**
General Capacity Building	Capacity Building (Type of Capacity Building etc.)	Confidential	**NO ACCESS**	Read-only	Read and Write	Read-only (Specific Mission)	Read and Write	**NO ACCESS**
Monitoring & Reports	Follow-ups on Pending Cases (Reference No etc.), Open Cases (Reference No etc.), Annex D Report (Reference No etc.)	Confidential	**NO ACCESS**	Read-only	Read	Read-only (Specific Mission)	Read	**NO ACCESS**
Member State View 1	List of Cases (Reference No etc.)	Confidential	Read-only (Member State Nationals)	**NO ACCESS**	**NO ACCESS**	**NO ACCESS**	**NO ACCESS**	**NO ACCESS**
Member State View 2	Case Details (Reference No, Case Status, Date of Incident, Location, Type of Casualty, Personal Information, Assistance Provided)	Confidential	Read-only (Member State Nationals)	**NO ACCESS**	**NO ACCESS**	**NO ACCESS**	**NO ACCESS**	**NO ACCESS**

User Management	Names: User Category: Country: Organization: Active?	Confidential	**NO ACCESS**	**NO ACCESS**	Read and Write	**NO ACCESS**	Read and Write	Read and write
Role Management	Role Title Role ID Role Description Active? Element Title Element Ref ID Menu Elements View (y/n) Execute (y/n)	Unclassified	**NO ACCESS**	**NO ACCESS**	Read	**NO ACCESS**	Read and Write	**NO ACCESS**
Manage Data from NOTICAS	NOTICAS countries mapping to SCR 2589 DB countries NOTICAS organizations mapping to SCR 2589 DB organizations/entities	Unclassified	**NO ACCESS**	**NO ACCESS**	Read	**NO ACCESS**	Read and Write	**NO ACCESS**
Manage Authorization Structure	Org Unit Name Org Unit Chart Acronym Time Zone Unit Type Active?	Unclassified	**NO ACCESS**	**NO ACCESS**	Read	**NO ACCESS**	Read and Write	**NO ACCESS**