SECURITY & DATA PROTECTION PROTOCOL

THE DESERT CAMEL AWARDS

CLASSIFICATION: CONFIDENTIAL

This document contains sensitive operational guidelines for the protection of personnel, nominees, and recipients laboring in high-risk environments.

Administered by:
Office of the Chief Operations Officer (COO)
An-Nour University

Effective Date: January 2026
Version: 1.1

Mogadishu, Somalia | Diaspora Global Offices
Security@DesertCamelAwards.org

1 Mission and Scope

The Desert Camel Awards (DCA) operates in contexts where visibility can lead to significant risk. The purpose of this protocol is to ensure that "enduring witness in hard places" is supported by a robust architecture of safety, confidentiality, and digital security. This protocol applies to all Regional Directors, Executive Staff, and external nominators.

2 Data Confidentiality & Nomination Security

2.1 Encryption Standards

All nomination data, including personal testimonies and referee contact information, must be stored using industry-standard end-to-end encryption.

- Direct email submissions to `Security@DesertCamelAwards.org` are restricted to authorized Regional Directors and the General Secretary.
- No sensitive nominee data shall be stored on unencrypted personal cloud services.

2.2 Data Retention and Purging

Nomination files for non-recipients will be securely purged six months after the annual award ceremony to minimize digital footprints. Files for recipients will be moved to a high-security offline archive.

3 Honoree Protection & Identity Management

3.1 The Pseudonym Protocol

In accordance with the Official Charter, any recipient laboring in a hostile or sensitive environment has the right to:

- Use a **Pseudonym** for all public announcements and digital listings.
- Request the blurring or omission of facial images in video or photographic promotional material.
- Utilize "Generic Citations" that omit specific geographic locations (e.g., "A Brother in the Sahel" rather than naming a specific village).

3.2 Physical Award Security

The physical "Desert Camel" trophy or plaque shall not be shipped directly to sensitive addresses or through public couriers where intercept is possible. Regional Directors will coordinate "Secure Handover" points in neutral locations or utilize trusted missional networks to ensure the safety of the recipient during the delivery of physical honors.

4 Digital Presence and Social Media

4.1 Geolocation Hygiene

Staff and Regional Directors are strictly prohibited from using "Check-in" features or sharing real-time geolocated content when visiting potential nominees or underground church sites.

4.2 Interaction Policy

Public interactions on Twitter (@DCamelAwards) and Facebook must be monitored to prevent the accidental "tagging" of believers who have not consented to public visibility.

5 Field Operations & Regional Safety

5.1 Travel to High-Risk Areas

Regional Directors for North Africa, West Africa, and East Africa must submit a brief "Movement Plan" to the COO when conducting field visits in active conflict zones.

- Directors are encouraged to maintain a "Low Profile" (the "Desert Camel" approach—unobtrusive and enduring).
- Use of marked DCA vehicles is prohibited in sensitive territories.

6 Incident Response

In the event of a security breach or the compromise of a nominee's identity:

1. **Immediate Silence:** All digital mentions of the individual must be retracted immediately.
2. **Crisis Liaison:** The President and General Secretary will engage with local partners to provide necessary relocation or legal support.
3. **Audit:** An internal review will determine the source of the leak to prevent recurrence.

Integrity in the Gospel includes stewardship of the lives entrusted to our care.