
SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

GUIDEBOOK ON TARGETED FINANCIAL SANCTIONS (TFS)

Framework for SECP-Regulated Reporting Entities
Under UNSC Resolutions, Anti-Terrorism Act 1997,
and Anti-Money Laundering Act 2010

NOTICE

This document is issued for general guidance purposes only. It does not constitute formal legal advice and should be read together with applicable legislation, statutory regulatory orders, and directions issued by the SECP. Regulations and legislation may change, and regulated entities must ensure their understanding remains current.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
SECTION 1. INTRODUCTION AND SCOPE	4
SECTION 2. LEGAL AND REGULATORY FRAMEWORK.....	5
2.1 Applicable Sanctions Lists.....	5
SECTION 3. DISSEMINATION OF SANCTIONS UPDATES	6
3.1 Additional Guidance by MOFA and NACTA	6
3.2 Legal and Regulatory Context for TFS Obligations.....	7
3.3 SRO 920(I)/2020 — Obligations Upon Receipt of SRO Notifications.....	9
3.4 NIL Reporting Obligation	9
3.5 TFS Risk Assessment Requirements Under AML Regulation and SRO	10
3.6 Role of the Central Depository Company (CDC) & National Clearing Company Limited (NCCPL)	11
3.7 SECP Supervisory Tools	11
3.8 Record Keeping.....	11
SECTION 4. IMPLEMENTATION WITHOUT DELAY.....	11
SECTION 5. GENERAL OBLIGATIONS OF REGULATED ENTITIES	12
5.1 Regulation 25 — TFS Obligations (SECP AML/CFT/CPF Regulations, 2020).....	12
5.2 TFS Effectiveness and Integration into Compliance Program.....	13
SECTION 6. SANCTIONS COMPLIANCE PROGRAMME.....	13
SECTION 7. SCREENING AND FALSE POSITIVE MANAGEMENT	154
7.1 Confirming a Match	154
7.2 Match Classification and Required Actions.....	154
7.3 Minimum Standards for Automated Screening	15
SECTION 8. RED FLAGS AND COMPLIANCE MONITORING	16
8.1 Red Flags Under SRO 920(I)/2020	165
8.2 Compliance Checklist Submission — Annual and Quarterly Obligations	17
SECTION 9. ENTERPRISE-WIDE RISK ASSESSMENT	177
SECTION 10. REPORTING AND RECORD KEEPING.....	18
SECTION 11. INTERNAL CONTROLS AND GOVERNANCE	187
SECTION 12. UNFREEZING AND DELISTING	198
SECTION 13. ENFORCEMENT AND PENALTIES	19
SECTION 14. FINAL PROVISIONS	19
GLOSSARY OF TERMS.....	20

EXECUTIVE SUMMARY

These Guidelines are issued by the Securities and Exchange Commission of Pakistan (SECP) to ensure that all regulated entities maintain the highest standards of compliance with Targeted Financial Sanctions (TFS). TFS are legally binding, non-discretionary measures that require the immediate freezing of all funds, financial assets, and economic resources of designated or proscribed individuals and entities, without delay and without exception.

The Guidelines are issued under the legal framework of the United Nations (Security Council) Act 1948, the Anti-Terrorism Act 1997, the Anti-Money Laundering Act 2010, and applicable SECP AML/CFT/CPF Regulations 2020, in line with FATF Recommendation 6. They apply to all SECP-regulated entities including securities brokers, insurance and takaful operators, non-banking finance companies, asset management companies, modarabas, and other licensed intermediaries.

Key obligations addressed in these Guidelines as per the AML/CFT/PF Regulatory framework and SRO 920 include:

Sr.no	Key Obligation	Requirement
1	Implementation of TFS	Immediate implementation of Targeted Financial Sanctions (TFS) without delay upon receipt of any SRO, notification, or designation.
2	Screening Requirements	Screen all customers, beneficial owners, and counterparties against UNSC 1267/1373 lists, NACTA proscribed persons/organizations lists, and domestic SROs.
3	Reporting of Matches	Immediately report confirmed matches, frozen assets, and attempted transactions to SECP and the Financial Monitoring Unit (FMU).
4	NIL Reporting	Submit NIL reports within the timelines prescribed in the relevant SRO where no match is identified.
5	Risk Assessment and Compliance Integration	Incorporate TFS obligations into enterprise-wide risk assessments and the overall AML/CFT compliance programme.
6	Record Keeping	Maintain records of screening exercises, freeze actions, reports submitted, and related documentation for a minimum period of five years.

Non-compliance with TFS obligations constitutes a serious regulatory breach and may attract monetary penalties of up to PKR 100 million, individual liability including disqualification of senior officers, suspension or revocation of licence, and criminal referral to law enforcement agencies.

SECTION 1. INTRODUCTION AND SCOPE

The Securities and Exchange Commission of Pakistan (SECP) issues these Guidelines to ensure that all regulated entities maintain the highest standards of financial integrity and fully comply with targeted financial sanctions requirements applicable under the laws of Pakistan. Targeted Financial Sanctions (TFS) are preventive measures intended to prevent the use of Pakistan's financial system for terrorism financing, or the provision of funds or economic resources to designated or proscribed individuals and entities.

What are Targeted Financial Sanctions? Targeted Financial Sanctions (TFS) are legally binding measures imposed by governments or international bodies principally through United Nations Security Council (UNSC) Resolutions that require the immediate freezing of all funds, financial assets, and economic resources owned or controlled by designated or proscribed individuals and entities, and the prohibition of any financial services or transactions involving such persons, whether directly or indirectly. TFS are distinct from broader trade sanctions or sectoral sanctions: they are targeted at specific named persons and entities, and they are non-discretionary in nature. Regulated entities must apply TFS obligations immediately upon designation regardless of any prior business relationship, customer risk rating, or transaction value. Failure to implement TFS without delay constitutes a serious regulatory breach and may attract criminal liability under the Anti-Terrorism Act, 1997.

These Guidelines are issued in line with FATF Recommendation 6 on Targeted Financial Sanctions, United Nations Security Council Resolutions, and the domestic legal framework applicable in Pakistan. The objective is to ensure that all regulated entities are able to identify designated persons and freeze their assets without delay.

These Guidelines apply to all reporting entities regulated by SECP, including securities brokers, insurance and takaful operators, non-banking finance companies, asset management companies, modarabas, and any other intermediary licensed or regulated by the Commission.

Key Principle. All regulated entities must establish a zero-tolerance sanctions compliance framework, recognizing that targeted financial sanctions are a rule-based obligation and not a risk-based measure. TFS obligations must be applied irrespective of customer risk rating, transaction size, or business relationship value.

SECTION 2. LEGAL AND REGULATORY FRAMEWORK

Targeted financial sanctions in Pakistan are implemented through several legal instruments. The following table summarizes the applicable framework:

Legal Instrument	Description
United Nations (Security Council) Act, 1948	Enables the Federal Government to give effect to UNSC resolutions, including sanctions under UNSCR 1267 (ISIL/Al-Qaida), UNSCR 1373 (on local lists), UNSCR 1988, UNSCR 1718 (DPRK), and UNSCR 2231 (Iran).
UN Security Council (Freezing and Seizure) Order, 2019	Provides for freezing and seizure of assets of designated persons pursuant to UNSC resolutions.
Anti-Terrorism Act, 1997	Provides the domestic framework for proscription of individuals and organizations. Notifications are reflected in consolidated lists maintained by NACTA.
Anti-Money Laundering Act, 2010	Section 6A authorizes the SECP to issue regulations, directions, and guidelines. Section 7H requires every reporting entity to implement policies and procedures ensuring TFS compliance.
Statutory Regulatory Orders (SROs)	Issued by the Ministry of Foreign Affairs (MOFA) under the UNSC Act, requiring assets freeze, travel ban, and arms embargo for designated individuals and entities.
SECP AML/CFT/CPF Regulations, 2020 — Regulation 25	Sets out specific TFS obligations for all regulated persons, including screening mechanisms, immediate freezing on confirmed or potential match, STR filing with FMU, and notification to SECP. See Section 5.1 for the full text.
S.R.O. 920(I)/2020 dated 28th September 2020	Requires each regulated person to immediately scan its customer databases and the Beneficial Owners/associates of customers for any matches with stated designated/proscribed persons upon receipt of notifications issued by the Ministry of Foreign Affairs under the United Nations (Security Council) Act 1948, or intimation from NACTA, regarding additions, deletions, and updates under the Anti-Terrorism Act, 1997.

2.1 Applicable Sanctions Lists

Regulated entities must screen against all of the following lists at all times:

List	Legal Basis	Website Links
------	-------------	---------------

UN Consolidated List	UNSC Act 1948 / SROs	https://www.un.org/securitycouncil/content/un-sc-consolidated-list
1267 List (ISIL/AI-Qaida)	UNSC Act 1948 / SROs	https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
1988 List (Taliban)	UNSC Act 1948 / SROs	https://www.un.org/securitycouncil/sanctions/1988/materials
NACTA Proscribed Organizations	Anti-Terrorism Act 1997	https://nacta.gov.pk/proscribed-organizations/
NACTA Proscribed Persons	Anti-Terrorism Act 1997	https://nacta.gov.pk/proscribed-persons/

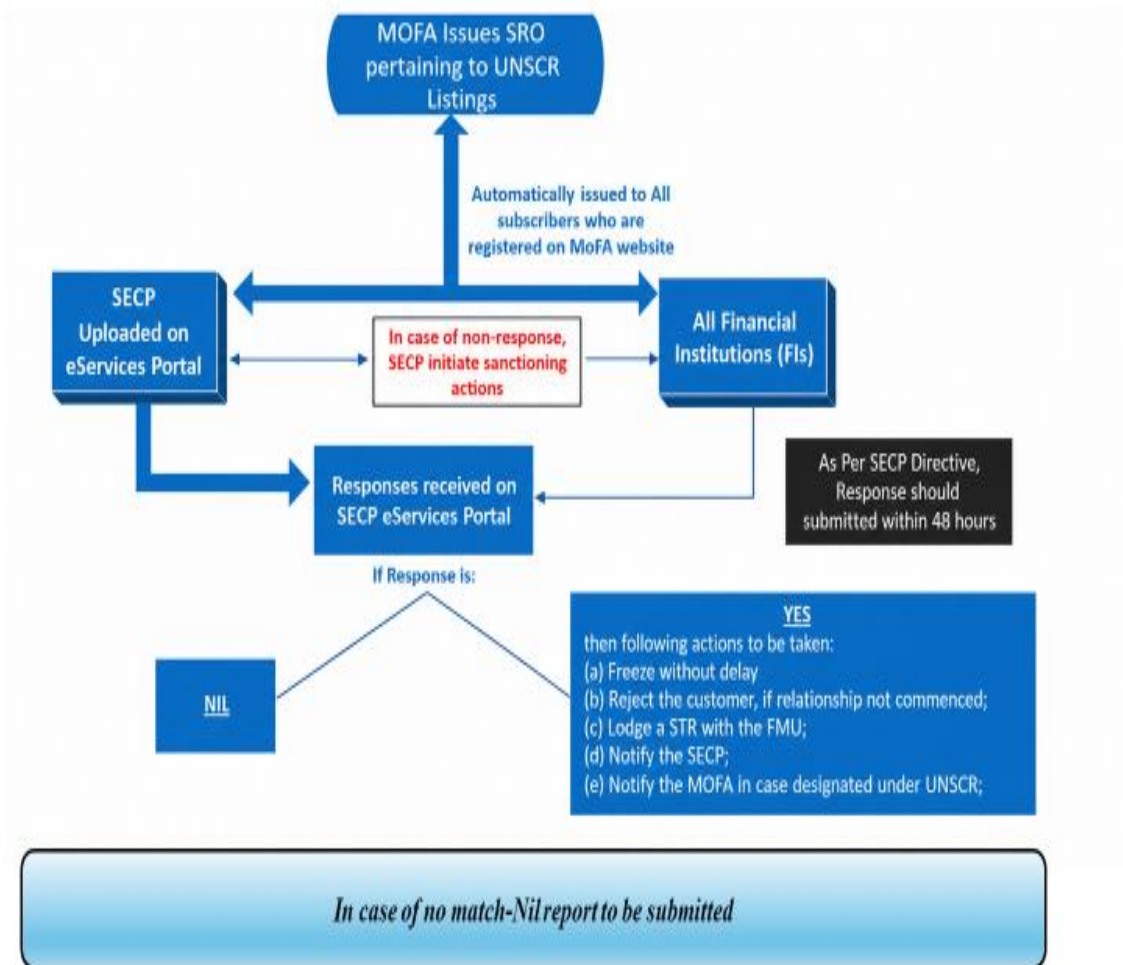
SECTION 3. DISSEMINATION OF SANCTIONS UPDATES

To ensure prompt transmission of SROs issued by MOFA/NACTA to relevant stakeholders, MOFA/NACTA has established an email subscription service. Regulated entities are required to sign up for this service through the respective websites. Similarly, to communicate additions, deletions, retentions, or amendments in the list of proscribed/designated individuals/entities, a system-generated email is disseminated by the competent authorities to regulated entities. The SECP disseminates these SROs and Notifications to its regulated entities as a supplementary measure.

Regulated entities must implement an internal escalation workflow that documents receipt, validation, freeze decision, FMU reporting, and senior management sign-off. SECP may review these workflows and sample case files during inspections and investigations.

A flow chart reflecting dissemination of the SROs is given below.

DISSEMINATION FLOWCHART



3.1 Additional Guidance by MOFA and NACTA

Guidance Document	Issuing Authority	Links
Guidelines on Implementation of UNSC Resolutions concerning TFS, Travel Ban, and Arms Embargo	MOFA	https://mofa.gov.pk/tfs-guidelines/
Guidelines on Actions for Implementation of UNSCR 1373	NACTA	https://nacta.gov.pk/guidelines/

Guidelines on Implementation of UNSC Resolutions concerning TFS on Proliferation Financing	MOFA / CRMC	https://mofa.gov.pk/pf-guidelines/
--	-------------	---

SECP requires regulated entities to map MOFA and NACTA guidance to their internal procedures covering screening, freezing, reporting, and de-listing.

3.2 Legal and Regulatory Context for TFS Obligations

Regulation 25 — TFS Obligations (SECP AML/CFT/CPF Regulations, 2020)

Regulation 25 of the SECP AML/CFT/CPF Regulations, 2020 sets out the specific TFS obligations applicable to all regulated persons. The full text of the regulation is reproduced below for reference:

25.(1) The regulated person shall undertake TFS obligations under the United Nations (Security Council) Act 1948 and/or Anti-Terrorism Act 1997 and any regulations made thereunder, including:

- *Develop mechanisms, processes and procedures for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with designated/proscribed persons in the SROs and notifications issued by MoFA, NACTA and MoI.*
- *If during the process of screening or monitoring the regulated person finds a positive or potential match, it shall immediately:*
 - *Freeze the relevant funds and assets without delay/block the transaction, without prior notice if it is an existing customer, in accordance with the respective SRO;*
 - *Prohibit from making any funds, other assets, economic resources, or financial or related services available in accordance with the respective SRO;*
 - *Reject the transaction or attempted transaction or the customer, if the relationship has not commenced.*
- *In all cases referred to above, file a suspicious transaction report with the FMU where the person is designated under UNSC Resolutions or proscribed under the Anti-Terrorism Act 1997, and simultaneously notify the Commission in the manner instructed by the Commission.*
- *Implement any other obligation under the AML Act 2010, UN (Security Council) Act 1948, Anti-Terrorism Act 1997, and any regulations made thereunder.*

25.(2) The regulated person is prohibited, on an ongoing basis, from providing any financial services to proscribed/designated entities and persons, or to those known for their association with such entities and persons, whether under the proscribed/designated

name or with a different name. The regulated person shall monitor business relationships on a continuous basis to ensure that no such relationship exists directly or indirectly, including through ultimate control of an account. Where any such relationship is found, the regulated person shall take immediate action as per law, including reporting to the FMU.

Explanation: *For the purposes of this regulation, the expression “associates” means persons and entities acting on behalf of, or at the direction of, or for the benefit of, proscribed/designated entities and individuals. Associates may be determined on the basis of appropriate screening of sanctions lists, disclosed nominee/beneficiary information, publicly known information, Government or regulatory sources, or reliable media information.*

3.3 SRO 920(I)/2020 — Obligations Upon Receipt of SRO Notifications

S.R.O. 920(I)/2020 dated 28th September 2020 requires each regulated person to immediately scan its customer databases and the Beneficial Owners/associates of customers for any matches with stated designated/proscribed persons upon receipt of notifications issued by the Ministry of Foreign Affairs under the United Nations (Security Council) Act 1948, or intimation from NACTA, Law Enforcement Agencies, Home Departments of Provinces, or the Ministry of Interior regarding additions, deletions, and updates under the Anti-Terrorism Act, 1997. The full text of the operative clauses is reproduced below.

Clause C — Immediate Scanning and Action on Match:

Each RP is required to immediately scan its customer databases and their Beneficial Owners/associates for any matches with the stated designated/proscribed person(s)/entity(ies) on receipt of the relevant SRO or notification. In case of a true match or suspicion of a proscribed/designated person, the following actions shall be taken immediately:

- Freeze without delay the customer’s fund/policy or block the transaction, without prior notice if it is an existing customer;
- Reject the transaction or attempted transaction or the customer, if the relationship has not commenced;
- Lodge a Suspicious Transaction Report (STR) with the FMU, and simultaneously;
- Notify SECP and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions, or NACTA in case that person is designated under the Anti-Terrorism Act, 1997.

Clause D — Compliance Report to SECP:

A compliance report on Statutory Regulatory Orders issued by MOFA under the UN (Security Council) Act 1948, or intimation from NACTA/LEAs/Home Departments/Ministry of Interior regarding updates in the list of proscribed persons/entities under the Anti-Terrorism Act 1997, shall be submitted to the Commission within forty-eight (48) hours of receiving the same, in the manner instructed by the Commission from time to time.

3.4 NIL Reporting Obligation

Even where screening results in zero matches against a particular SRO or notification, the regulated person is still required to submit a NIL response to SECP confirming that: (a) the screening exercise was actually conducted; and (b) the entire customer base, including beneficial owners and associates, was checked. The NIL report must be submitted within the timeline specified in the relevant SRO. This obligation is continuous — whether or not a match is found, a documented and reported outcome is required. SECP uses NIL reporting to verify that regulated persons are actively carrying out their screening obligations.

3.5 TFS Risk Assessment Requirements Under AML Regulation and SRO

AML/CFT Regulations read with SRO 920(I)/2020 mandate that regulated entities conduct a formal, documented Institutional Risk Assessment (IRA) that explicitly addresses TFS exposure. The IRA must be approved by the Board of Directors or equivalent governance body and must be updated at least annually or whenever a material change occurs in the entity's business model, customer base, product offerings, or the national/sectoral risk landscape. The following requirements are directly applicable to the TFS component of the enterprise-wide risk assessment:

AML Regulations	TFS-Specific Requirement for Regulated Entities
Regulation 4 — Risk Assessment	Identify and document TFS exposure across all products, customers, geographies, and delivery channels. Categorise entity-level TFS risk as High, Medium, or Low based on assessment outcome. Keep the assessment current and provide data to SECP upon request.
Regulation 5 — Risk Mitigation	Board-approved policies and controls must specifically address TFS risk mitigation, including sanctions screening systems, escalation protocols, and freeze procedures. Enhanced measures must be adopted where higher TFS risk is identified.
Regulation 7 — New Products / Technologies	Before launching any new product, delivery channel, or technology (including digital platforms, e-wallets, or crypto-asset services), regulated entities must conduct a TFS-specific risk assessment and document mitigating controls.

Regulation 19 — Ongoing Monitoring	Transaction monitoring systems must include TFS-specific rules and scenarios. All complex, unusual, or high-value transactions must be screened against sanctions lists and assessed for potential nexus with designated persons.
Regulation 25 — TFS Obligations	Regulated entities must develop and maintain internal mechanisms, procedures, and systems for screening and monitoring customers, beneficial owners, and counterparties against UNSC and domestic proscription lists. In the event of a confirmed or potential match, assets must be frozen without delay, transactions rejected, and reports filed with FMU and SECP immediately.
Regulation 27 — Compliance Programme	The Compliance Officer must be specifically trained on TFS obligations and must have authority and systems access to implement immediate freezing. The internal audit function must test the TFS compliance programme at least annually and report findings to the Board Audit Committee.
SRO 920(I)/2020 Clause A	Each regulated person must put in place internal policies, procedures, and controls to implement TFS obligations as set out in the SRO, commensurate with the nature, scale, and complexity of its business.
SRO 920(I)/2020 Clause B	Regulated persons must maintain adequate internal controls to ensure that designated/proscribed persons are not able to benefit from or access financial services, directly or indirectly.
SRO 920(I)/2020 Clause C	Regulated persons must immediately scan their databases upon receipt of any SRO or notification and take required action on confirmed or potential matches.
SRO 920(I)/2020 Clause D	A compliance report must be submitted to SECP within 48 hours of receiving the SRO or notification, in the manner instructed by the Commission.
SRO 920(I)/2020 Clause E	Regulated persons must maintain records of all compliance actions related to TFS, including screening exercises, freeze decisions, STRs filed, and NIL reports submitted, in a readily accessible manner for SECP inspection.

3.6 Role of the Central Depository Company (CDC) & National Clearing Company Limited (NCCPL)

Each regulated person is responsible for screening its own customers against sanctions and proscribed lists at the time of account opening and whenever a new SRO is issued. However, where onboarding is conducted via the CDC Central Gateway Portal, screening

is carried out by CDC on behalf of the regulated person. Regulated persons must ensure that their CDC-related onboarding workflows are aligned with TFS obligations and that any CDC-flagged matches are actioned immediately in accordance with these Guidelines.

3.7 SECP Supervisory Tools

SECP continuously monitors compliance responses and undertakes desk-based review of each SRO disseminated to regulated entities. Onsite inspections include a dedicated review of screening processes and procedures to confirm that proper and timely screening is being undertaken. Additionally, SECP conducts risk-based thematic inspections to assess the implementation and effectiveness of TFS obligations by the RPs.

3.8 Record Keeping

Regulated entities must maintain records of all screening exercises, match decisions, and NIL reports in a manner that is readily accessible to SECP inspectors.

SECTION 4. IMPLEMENTATION WITHOUT DELAY

The requirement to implement sanctions without delay originates from FATF Recommendation 6, which requires that the funds and assets of designated persons be frozen immediately upon designation and that no funds or financial services be made available, directly or indirectly, to such persons.

SECP regulated entities must ensure screening is conducted:

When to Screen:

- At onboarding (new customers): Every new customer must be screened against all applicable UNSC consolidated lists including 1267 and 1373, NACTA proscribed persons and organizations lists, and any domestic SROs, before the business relationship is established. No account may be opened or transaction processed for a new customer without completion of a sanctions screening check.
- For existing customers upon issuance of every new SRO: Upon receipt of a new SRO or notification from MOFA, NACTA, Ministry of Interior, or a Law Enforcement Agency, regulated entities must immediately screen their entire existing customer database, including beneficial owners and associates, against the updated list. Screening must be completed without delay and, where a manual system is used, within a maximum of 24 hours from issuance of the SRO or notification.
- Periodic screening: In addition to event-triggered screening, regulated entities using automated systems must conduct periodic re-screening of their entire customer base to capture any updates to sanctions lists that may not have been captured by real-time or batch processes.

Screening Method	Standard	Maximum Timeline
Automated Systems	Real-time screening at onboarding; batch screening after list updates; Periodic screening	Immediate / within hours of list update
In-house Systems	Complete database screening and freezing measures	Immediately / without delay from SRO/notification issuance

Failure to act within these timelines may constitute a regulatory breach.

SECTION 5. GENERAL OBLIGATIONS OF REGULATED ENTITIES

5.1 Effective implementation of targeted financial sanctions:

Regulated entities must establish policies, procedures, and systems to ensure effective implementation of targeted financial sanctions:

Obligation	Description
Immediate Freezing	Freeze all funds, financial assets, and economic resources of designated persons without delay and without prior notice.
Prohibition of Services	No funds, financial services, or economic resources may be provided directly or indirectly to designated persons, including through third parties, nominees, or intermediaries.
Screening	Screen all customers, beneficial owners, authorized signatories, and counterparties against updated UNSC and domestic sanctions lists.
Ongoing Monitoring	Monitor transactions and business relationships on a continuous basis for any nexus with designated or proscribed persons.
Reporting	Report all confirmed matches, frozen assets, and attempted transactions to SECP and FMU.
Record Keeping	Maintain documentation of all compliance actions for a minimum of five years.

Sanctions obligations must be applied irrespective of the customer's risk classification and must form part of the overall AML/CFT framework.

5.2 TFS Effectiveness and Integration into Compliance Program

Effectiveness

REs should operationalize TFS by implementing automated, real-time screening systems covering customers, transactions, and beneficial owners, and ensuring immediate action on matches (freeze, prohibit, reject). They should conduct continuous monitoring to detect indirect ownership or control linkages, regularly update and re-screen against sanctions lists, and maintain accurate MIS on frozen assets, alerts, and rejected transactions. Effectiveness is strengthened by staff training, clear escalation protocols, and timely subscription to updates issued by Ministry of Foreign Affairs and National Counter Terrorism Authority.

Compliance

REs should embed TFS within their AML/CFT framework by developing documented policies, procedures, and internal controls aligned with the Anti-Money Laundering Act, 2010 and requirements of SECP. This includes screening at onboarding and on an ongoing basis, extending checks to beneficial owners and associated persons, and strictly prohibiting services to designated entities. REs must ensure timely filing of STRs with the Financial Monitoring Unit, integrate TFS triggers into transaction monitoring systems, and align controls with their risk-based approach, ensuring coordination across compliance, operations, and reporting functions.

SECTION 6. SANCTIONS COMPLIANCE PROGRAMME

Every regulated entity must establish, document, and maintain a dedicated Sanctions Compliance Programme as part of its overall AML/CFT framework. The Sanctions Compliance Programme must be approved by the Board of Directors or equivalent governance body and must be reviewed at least annually or upon any material change in the regulatory environment or the entity's business model.

The Sanctions Compliance Programme must, at a minimum, include:

- Written sanctions policies and procedures aligned with applicable UNSC resolutions, domestic legislation, and SECP regulations.
- Appointment of a designated Compliance Officer with specific authority and system access to implement immediate freezing and reporting.
- Screening systems capable of real-time or near-real-time identification of sanctioned persons at onboarding and on a continuous basis.
- Clear escalation and decision-making procedures for confirmed matches, partial matches, and false positives.
- Regular staff training on TFS obligations, sanctions screening processes, and reporting requirements.
- Annual internal audit of the Sanctions Compliance Programme, with findings reported to the Board Audit Committee.

SECTION 7. SCREENING AND FALSE POSITIVE MANAGEMENT

Screening must use fuzzy matching to detect spelling variations, aliases, and transliterations. Potential matches must be verified using secondary identifiers.

7.1 Confirming a Match

Individual Customer	Corporate Customer
Full name and aliases CNIC / passport number Date of birth Nationality Father's name	Full corporate / legal name Aliases and trading names Registered office address Business operation locations Directors, shareholders, and beneficial owners

Regulated persons must also screen associates of customers — meaning persons and entities acting on behalf of, at the direction of, or for the benefit of any designated/proscribed individual or entity. Associates may be identified through screening of sanctions lists, nominee/beneficiary disclosures, publicly available information, Government or regulatory sources, or reliable media sources. Refer to Regulation 25 (Section 5.1) for the full definition of associates.

7.2 Match Classification and Required Actions

Match Type	Action Required	Reporting
Confirmed Match	Freeze assets without delay (existing customer). Reject application (new customer).	Asset Freeze Report to SECP immediately. STR to FMU via goAML.
Partial Match	Suspend all transactions without delay pending further verification.	Report to SECP. Escalate internally for resolution.
False Positive	No action required. Continue normal screening.	Document in False Positive Log for SECP inspection.

Where there is not a full match but sufficient grounds for suspicion, the regulated entity should consider filing a STR with FMU.

7.3 Minimum Standards for Automated Screening

- Daily updates of UN consolidated lists including 1267 and 1373 and domestic SROs.
- Fuzzy-matching with configurable thresholds and documented tuning rationale.

- Audit logs for every match and decision.
- Capability to ingest aliases and transliterations.
- Demonstrable false-positive reduction metrics.

SECTION 8. RED FLAGS AND COMPLIANCE MONITORING

8.1 Red Flags Under SRO 920(I)/2020

SRO 920(I)/2020 issued by the SECP prescribes the following additional red flags that all regulated entities must incorporate into their TFS screening and transaction monitoring systems. These indicators are applicable across all regulated sectors:

- Customer refuses or is unable to provide the information required for sanctions screening or CDD without a plausible explanation.
- Customer requests that screening records, match decisions, or freeze actions be kept off formal records or communicated only verbally.
- Customer or beneficial owner shares an address, phone number, date of birth, or identification number with a person or entity appearing on any applicable sanctions list.
- Transaction involves a jurisdiction identified in NACTA's or MOFA's high-risk country circulars, or a country subject to UNSC arms embargo.
- Transactions structured to fall just below reporting or screening thresholds, suggesting deliberate layering to avoid detection.
- Customer insists on the use of cash, cryptocurrency, or informal value-transfer systems (hawaladars) for high-value transactions, particularly involving a counterparty in a conflict or sanctions-risk jurisdiction.
- Payments to or from a non-profit organisation (NPO) that are inconsistent with the NPO's stated charitable objects, donor base, or geographic programme area.
- Use of complex corporate structures, trusts, or nominee arrangements that obscure the identity of the ultimate beneficial owner, especially in combination with a high-risk jurisdictional nexus.
- Any transaction where the counterparty, intermediate beneficiary, or end recipient has a name, address, or identifier similar (but not identical) to a designated person or proscribed entity, requiring enhanced verification before proceeding.
- Customer or transaction involves a virtual asset service provider (VASP) or digital asset exchange that is unregistered, operates in a high-risk jurisdiction, or cannot demonstrate sanctions screening controls.

- Frequent changes to customer details (name, address, or identification numbers) without adequate explanation, particularly where changes result in the customer no longer appearing to match a previously flagged entry.

8.2 Compliance Assessment Checklist Submission — Annual and Quarterly Obligations

In accordance with SRO 920(I)/2020 and SECP's supervisory framework, regulated entities are required to submit a Compliance Assessment Matrix and Information on ML/TF/PF Risks to SECP on the following schedule:

Frequency	Return / Report	Description
Annual	Institutional Risk Assessment Report (IRAR)	Covers TFS risk assessment, inherent vulnerabilities, and residual risk scoring. Submitted to SECP AMLD by 30th April of each year.
Annual	Compliance Assessment Matrix (CAM)	Self-assessment of compliance with all AML/CFT/CPF obligations including TFS. Submitted with the IRAR.
Quarterly	Six-Monthly / Quarterly Data Return	Quantitative data on number of sanctions screenings conducted; confirmed matches and false positives; total value of frozen assets; STRs filed related to TFS; NIL reports submitted against each SRO.
Per Event	Asset Freeze Report	Submitted to SECP AMLD immediately upon confirming a sanctions match. Must include customer details, matched list, assets frozen, and actions taken.
Per SRO	NIL Report	Where no match is found against a particular SRO or notification, a NIL report must be submitted to SECP within the timeline specified in the SRO.

Failure to submit required returns on time, or submission of inaccurate or incomplete data, constitutes a violation of Regulation 27 of the SECP AML/CFT/CPF Regulations, 2020, and will be treated as a compliance deficiency. SECP may impose sanctions in accordance with the AML/CFT Sanctions Rules, 2020 for persistent non-submission or misreporting.

SECTION 9. ENTERPRISE-WIDE RISK ASSESSMENT

Regulated entities must explicitly quantify TFS risk (both terrorism financing and proliferation financing) within the enterprise-wide risk assessment (ERA). This includes:

- Mapping product, customer, and geographic exposures to UNSC and domestic lists.
- Scoring residual TFS risk after controls.
- Documenting mitigation plans with timelines and senior management sign-off.

SECTION 10. REPORTING AND RECORD KEEPING

When a true match is confirmed, regulated entities must take the following steps:

Step	Action	Timeline / Channel
1	Freeze all assets immediately without prior notice.	Without delay.
2	Submit Asset Freeze Report to SECP AML Department.	Immediately / without delay.
3	File Suspicious Transaction Report (STR) with FMU.	Via goAML portal.
4	Notify MOFA (if UNSC designated) or NACTA (if ATA proscribed).	Simultaneously with STR.
5	Report as per specific SRO requirements.	Per applicable SRO.

Attempted transactions involving designated persons must also be reported. All records must be maintained for a minimum of five years. Regulated entities must maintain up-to-date data and MIS of all frozen assets, funds, and attempted or rejected transactions, and make these available to SECP as required.

SECTION 11. INTERNAL CONTROLS AND GOVERNANCE

Entities must establish written sanctions policies, appoint a compliance officer, train staff, and maintain escalation procedures. Senior management and the Board are responsible for ensuring that the sanctions compliance framework is effective and adequately resourced. Refer to the SECP AML/CFT/CPF Regulations, 2020 for detailed requirements on internal controls and governance, in particular Regulations 27 and 28.

- Written sanctions compliance policies and procedures.
- Trained and qualified compliance staff.
- Screening systems capable of immediate freezing.
- Periodic audit and compliance checks.
- Compliance officer oversight with direct reporting to senior management.

SECTION 12. UNFREEZING AND DELISTING

Assets may only be unfrozen upon official notification that the person has been removed from the applicable sanctions list or upon written authorization from the competent authority. The same mechanism used for disseminating additions to proscribed and designated lists namely, SROs issued by MOFA and notifications issued by NACTA or the Ministry of Interior is also used to communicate removals and deletions from these lists. Upon receipt of such a notification confirming removal, regulated entities must promptly lift the freeze and restore access to the customer's assets, and must document the de-freezing action in their compliance records.

SECTION 13. ENFORCEMENT AND PENALTIES

Failure to comply with TFS obligations may result in regulatory action under the AML Act, Anti-Terrorism Act, and SECP laws. Penalties may be imposed on the institution as well as responsible officers.

Penalty Type	Details
Monetary Fines	Up to PKR 100 million depending upon the nature of the violation and type of Financial Institution.
Individual Liability	Penalty on CEO and Compliance Officer; potential disqualification from holding office.
Operational Sanctions	Suspension of license or business operations.
Criminal Referral	Referral to law-enforcement agencies.

Administrative Sanctions: In addition to monetary penalties, SECP may impose the following administrative sanctions for TFS violations: (a) issuance of written warning or reprimand; (b) direction to conduct internal inquiry and take disciplinary action against responsible officers; (c) imposition of conditions, limitations, or restrictions on business or product offerings; (d) suspension or revocation of licence; and (e) referral to law-enforcement agencies for criminal action. Where non-compliance is attributable to wilful conduct or gross negligence, sanctions may be imposed directly on the CEO, Compliance Officer, or other responsible individuals, including temporary or permanent prohibition from holding positions of responsibility.

Sanctions violations are treated as the highest-risk regulatory breaches. SECP publishes redacted enforcement orders on its website. Regulated entities retain the right to appeal against any sanction before the SECP Appellate Bench within 30 days of the order. The maximum time for the Appellate Bench to decide on an appeal shall not exceed 180 days from the date of receipt.

SECTION 14. FINAL PROVISIONS

All regulated entities must ensure strict compliance with these Guidelines and all sanctions requirements issued by the Government of Pakistan, the United Nations Security Council, and the SECP. Entities must ensure that their systems, procedures, and internal controls are capable of implementing targeted financial sanctions without delay and without exception.

[End of Guidelines]

GLOSSARY OF TERMS

AMLA —Anti-Money Laundering Act, 2010.

CDD — Customer Due Diligence

CFT — Countering financing of terrorism.

CPF — Countering proliferation financing

CTR —Cash transaction reporting

EDD — Enhanced due diligence

FATF — Financial Action Task Force

FBR — Federal Board of Revenue

FMU —Financial Monitoring Unit

IRAR — Internal Risk Assessment

LEA —Law Enforcement Agencies

MOFA — Ministry of Foreign Affairs

NACTA — National Counter Terrorism Authority.

NPO — Non-Profit Organization

RP — Regulated Person

STR/SAR — Suspicious Transaction Report

TF — Terrorist Financing

TFS — Targeted Financial Sanctions

UNSC — United Nation Security Council
