XPOSER.AI

EXECUTIVE GUIDE · ARABIC + ENGLISH

Building A Whistleblowing Unit Under The SAMA Policy.

A practical implementation guide for financial institutions supervised by the Saudi Central Bank — the obligations, the unit, the eight processing stages, and where the Kingdom's whistleblower protection framework changes the picture.

Published	September 2026
Edition	1.0
Languages	English (part one) · العربية (part two)
Audience	Compliance, internal audit, board audit committees
Author	XPOSER.AI

Not legal advice. This guide summarises the Whistle Blowing Policy for Financial Institutions issued by the Saudi Central Bank and related Saudi instruments, and offers an implementation view. Obligations are stated as we read the published policy; the authoritative text is SAMA's. Confirm the current version in the SAMA Rulebook and take your own legal advice before relying on anything here.

CONTENTS · المحتويات

Section 01

Who The Policy Binds

The Whistle Blowing Policy for Financial Institutions is a minimum standard, not a model document. An institution is expected to build its own policy on top of it, approved by the board.

Institutions in scope

Banks and branches of foreign banks, insurers and reinsurers, insurance service providers, finance companies and credit bureaus supervised by SAMA.

People in scope

The policy reaches further than employment. **Financial institution employees** covers board members, executives, permanent and contract staff, consultants and third-party workers. **Stakeholders** covers shareholders, creditors, customers, suppliers and other third parties with an interest in the institution.

> **The scoping mistake to avoid**
>
> A channel restricted to employees with corporate credentials does not meet this scope. Customers, suppliers and contractors must be able to report — which means the channel has to work without a corporate login, on a personal device, in Arabic and in the languages your workforce actually speaks.

Section 02

The Eight General Obligations

MINIMUM OBLIGATIONS ON THE INSTITUTION

#	Obligation	What it takes in practice
1	Board-approved whistleblowing policy, reviewed annually	A dated policy, minuted board approval, and a diarised annual review that actually happens
2	Periodic reports to the board and audit committee on cases and actions	A standing agenda item with a defined reporting pack, not an ad-hoc escalation
3	Encourage employees and stakeholders to report	Active communication, not a link buried in an intranet
4	Assure confidentiality of the whistleblower’s identity and information	Access control, restricted handler circle, and a channel that does not force identification
5	Protect whistleblowers against retaliation	An anti-retaliation policy with a named owner and a route to enforce it
6	Make clear that good-faith reports later found unsubstantiated carry no penalty	Stated in the policy and repeated at the point of reporting, where it is actually read
7	Provide, as a minimum, telephone, website, postal and email channels	Four channels, all monitored, all feeding one case record
8	Run awareness programmes on reporting responsibilities	Training with attendance records, refreshed, and extended to third parties in scope

On obligation 7

“As a minimum” is the operative phrase. Four channels are the floor, and a voice channel that accepts a spoken report in the reporter’s own language satisfies the telephone requirement while producing a structured case record rather than a call note. What SAMA cares about is that every channel reaches the same unit, under the same confidentiality, with the same audit trail — fragmenting intake across four unconnected inboxes technically complies and practically fails.

Section 03

The Violation Report Processing Unit

The policy requires an **independent administrative unit** to receive and process reports, reporting to the compliance department.

What independence has to mean

- The unit does not sit under a function it will routinely investigate. Reports about finance cannot be triaged by finance.
- Conflict-of-interest routing exists in advance: a documented rule for what happens when a report names the head of the unit, the CCO, an executive or a board member.
- The unit has direct access to case data without depending on the implicated function’s systems.
- Resourcing is sufficient for 24/7 intake — misconduct is not reported during business hours only.

Segregation of duties within the unit

Receiving, assessing, investigating and deciding should not collapse into one person, however small the institution. Where headcount makes full separation impossible, the compensating control is documentation: every decision recorded with its rationale, reviewed by compliance, and reportable to the audit committee.

Section 04

What May Be Reported

The policy enumerates fourteen categories. They are broader than fraud, and a channel scoped only to financial crime under-delivers against the policy.

Category	Category
1 · Financial and administrative corruption	8 · Conflicts of interest in business arrangements
2 · Breach of laws, regulations, instructions or policies	9 · Misuse of granted powers, including password sharing
3 · Environment, health and safety violations	10 · Obtaining undeserved benefits
4 · Conduct contrary to public order and Islamic ethics	11 · Unlawful disclosure of confidential information
5 · Misuse of institution property or assets	12 · Destroying documents or concealing fraudulent reports
6 · Abuse of power by employees	13 · Serious negligence causing damage to the institution
7 · Illegal operations or circumvention of regulation	14 · Concealment of any of the above

Category 14 deserves attention when designing intake: it makes the covering-up of misconduct independently reportable, which means your taxonomy needs a way to record it without forcing the reporter to first prove the underlying act.

Obligations the policy places on whistleblowers

Reciprocally, a reporter is expected to ensure credibility rather than repeat rumour, to avoid malicious reports aimed at defamation or retaliation, to exercise due diligence and provide accurate detail and supporting documents where available, to report promptly, to maintain confidentiality over the report, and to bear responsibility for malicious allegations. Communicating these obligations at the point of reporting — alongside the good-faith protection in obligation 6 — improves report quality measurably.

Section 05

Protection, And Its One Significant Limit

Three protection obligations apply:

1. Protect whistleblowers who report without malice from retaliatory action by employees.
2. Disclose whistleblower information only to competent authorities — investigation and judicial authorities.
3. Confirm that a good-faith report later found unsubstantiated attracts no penalty.

> **The limit programmes most often get wrong**
>
> Under the SAMA policy, **a whistleblower who reports anonymously cannot claim the institution's protective obligations.** This is not a reason to remove anonymous reporting — anonymous channels surface reports that would otherwise never arrive. It is a reason to say so honestly at the point of submission, so a reporter can make an informed choice between anonymity and protection, rather than discovering the trade-off after retaliation has begun.

The practical design answer is to offer both and explain the difference in one sentence each: an identified report carries the institution's protection; an anonymous report carries stronger concealment but not that protection. A channel with a secure two-way follow-up thread narrows the gap, because the investigative disadvantage of anonymity — the inability to ask a follow-up question — largely disappears.

Section 06

The Eight Processing Stages

The policy requires documented procedures with detailed steps for each stage of report processing. These are the stages, with the control that makes each auditable.

STAGES AND THEIR EVIDENCE

#	Stage	Control that makes it auditable
1	Report reception	Timestamped record, channel of origin captured, acknowledgement issued where possible
2	Initial assessment	Category and seriousness recorded with the reasoning, by a named assessor
3	Identification of a verification plan	Written plan and scope before investigation begins
4	Documentation of the processing rationale	Why this route was chosen — the step most often skipped
5	Processing decision	Decision, decision-maker and date, with conflicts declared
6	Follow-up on implementation	Corrective actions tracked to completion, not to assignment
7	Record keeping	Reports and documents retained for the legally required duration
8	Reporting	Periodic pack to board and audit committee on instances and procedures

Alongside these, the institution must treat every report seriously regardless of its nature or the adequacy of its detail, take protective measures for the whistleblower, notify the whistleblower of receipt and of the decision where possible, take corrective action where a violation is proven, consider the interests of employees and stakeholders, and refer reports to the responsible control or investigation department.

> **“Regardless of… the adequacy of its detail”**
>
> Thin reports cannot be discarded as unactionable. This is where a two-way follow-up channel stops being a convenience and becomes a compliance control: it is the mechanism by which a thin report is made adequate rather than closed.

Section 07

The Automated Reporting System

The policy expects controls to review report content and a system that tracks specific fields, and it expects the institution to be able to generate a report at any processing stage **on SAMA’s request**. That last clause sets the real requirement: the data must be queryable on demand, not reconstructable from spreadsheets in a week.

TRACKED FIELDS

Field	Why SAMA wants it
Channel through which the report was received	Shows whether all four required channels are genuinely in use
Total reports received	Volume trend; unusually low volume is itself a finding
Reports by subject	Concentration by category or business line
Processed versus in-progress	Backlog and ageing
Type of processing applied	Consistency of treatment across similar cases
Status at any processing stage, on request	Supervisory examination readiness

Section 08

Key Performance Indicators

The policy requires an indicator for each procedure stage, measuring compliance with the requirements. Indicators that measure activity rather than compliance satisfy the letter and miss the point.

Stage	Weak indicator	Indicator that evidences compliance
Reception	Number of reports received	% acknowledged within the committed period, by channel
Initial assessment	Number assessed	Median and p95 time to assessment; % with recorded reasoning
Verification plan	Number of investigations opened	% with a written plan before work began
Rationale	—	% of decisions with documented rationale
Decision	Number closed	Ageing profile of open cases; % closed with declared conflicts checked
Follow-up	Actions assigned	% of corrective actions verified complete
Records	—	% of cases with complete retained documentation on sample test
Programme health	—	Employee awareness and willingness-to-report survey results

Section 09

The Wider Saudi Framework

The SAMA policy does not operate alone, and a unit designed only against it will have gaps.

Personal Data Protection Law (PDPL)

A whistleblowing case file is dense personal data about at least three parties — the reporter, the reported person and any witnesses — and often includes allegations of criminal conduct. Purpose limitation, minimisation, retention limits and the restrictions on transferring personal data outside the Kingdom all apply. For most SAMA-supervised institutions the practical consequence is that case data should reside in the Kingdom, and any cross-border access by a vendor or its subprocessors must rest on a ground the PDPL and its transfer regulation permit. SDAIA is the competent supervisory authority.

Whistleblower, witness, expert and victim protection

Saudi Arabia has developed a dedicated protection framework, with a national programme supervised by the Public Prosecution and administered by a committee drawing on the Public Prosecution, the Ministry of Interior, the Presidency of State Security and the Oversight and Anti-Corruption Authority (Nazaha). Where a report concerns a public official, Nazaha is the competent body to investigate and prosecute. An internal unit therefore needs a documented referral route to external authorities and a rule for when internal handling must stop.

Rights of the reported person

People named in reports have data protection rights too. Responding to them must not reveal, directly or indirectly, the identity of a reporter — which means access requests in this context require a redaction protocol written before the first request arrives, not after.

Section 10

A 90-Day Implementation Plan

SAMA required institutions to implement the policy within three months of issuance, with a compliance plan submitted within one month. The same shape works for an institution rebuilding a unit that has drifted.

Days	Workstream	Output
1–15	Gap assessment against the eight obligations	Written gap register with owners
1–30	Draft policy and compliance plan	Board-ready policy; plan submitted
15–45	Stand up the unit; define independence and conflict routing	Charter, reporting line, segregation of duties
20–50	Channels: telephone, website, postal, email into one case record	Four live channels, one queue
30–60	Document the eight processing stages	Procedure manual with templates
35–65	Configure the tracking system and reporting fields	On-demand supervisory report
45–70	Define KPIs and the board reporting pack	KPI definitions, first pack drafted
50–80	Awareness programme and handler training	Materials, sessions, attendance records
60–85	PDPL alignment: residency, retention, redaction protocol	Records of processing; DPA with any vendor
75–90	Test the channel end to end, including anonymously	Test report and remediation list
90	Board approval and go-live	Minuted approval; annual review diarised

Section 11

Board And Audit Committee Questions

1. When did the board last approve the whistleblowing policy, and when is the next annual review?
2. How many reports arrived through each of the four required channels last period? A channel at zero is either unknown or untrusted.
3. What is the median and 95th-percentile time from receipt to initial assessment?
4. How many cases are open, and what is the age of the oldest?
5. Can we produce a report on any case at any processing stage today, if SAMA asked this afternoon?

6. Who investigates a report naming an executive or a board member, and where is that written down?
7. Do we tell anonymous reporters that anonymity forfeits the institution’s protective obligations?
8. Have we surveyed whether staff know the channel exists and would trust it?
9. Does case data reside in the Kingdom, and who outside it can access the system?
10. Has anyone who reported internally been disciplined or managed out since the last review?

Section 12

References

1. **Whistle Blowing Policy for Financial Institutions**, Saudi Central Bank (SAMA), August 2019. rulebook.sama.gov.sa — the authoritative source for sections 1 to 8.
2. **Personal Data Protection Law** and the **Regulation on Personal Data Transfer Outside the Kingdom**, Kingdom of Saudi Arabia. sdaia.gov.sa
3. **Law for the Protection of Whistleblowers, Witnesses, Experts and Victims**, Kingdom of Saudi Arabia, and the national protection programme supervised by the Public Prosecution.
4. **Oversight and Anti-Corruption Authority (Nazaha)** — competent authority where a report concerns a public official. nazaha.gov.sa
5. **XPOSER.AI Anonymity Whitepaper** — the anonymity architecture referenced in section 5.

الجزء الثاني

الدليل التنفيذي — بناء وحدة الإبلاغ عن المخالفات

هذه نسخة عربية موجزة من الدليل. النص الإنجليزي في الجزء الأول هو النسخة الكاملة، والمرجع المُعتمد في جميع الأحوال هو سياسة الإبلاغ عن المخالفات للمؤسسات المالية الصادرة عن البنك المركزي السعودي.

نطاق التطبيق

تسري السياسة على البنوك وفروع البنوك الأجنبية وشركات التأمين وإعادة التأمين ومقدّمي خدمات التأمين وشركات التمويل وشركات المعلومات الائتمانية الخاضعة لإشراف البنك المركزي. ويشمل نطاق الأشخاص أعضاء مجلس الإدارة والتنفيذيين والموظفين الدائمين والمتعاقدين والاستشاريين والعاملين من أطراف ثالثة، إضافة إلى أصحاب المصلحة من مساهمين ودائنين وعملاء وموّردين.

> **خطأ شائع في تحديد النطاق**
>
> القناة المقصورة على الموظفين الذين يملكون حسابات مؤسسية لا تفي بالنطاق المطلوب. يجب أن يتمكن العملاء والموّردون والمتعاقدون من الإبلاغ، أي أن تعمل القناة دون تسجيل دخول مؤسسي، ومن جهاز شخصي، وباللغة العربية واللغات التي يتحدثها منسوبو المنشأة فعلياً.

الالتزامات العامة الثمانية

1. إعداد سياسة للإبلاغ عن المخالفات معتمدة من مجلس الإدارة، ومراجعتها سنوياً.
2. رفع تقارير دورية إلى مجلس الإدارة ولجنة المراجعة عن الحالات والإجراءات المتخذة.
3. تشجيع الموظفين وأصحاب المصلحة على الإبلاغ عن المخالفات.
4. ضمان سرية هوية المُبلّغ والمعلومات المتعلقة به.
5. حماية المُبلّغين من الإجراءات الانتقامية.
6. توضيح أن البلاغات المقدَّمة بحسن نية ولم تثبت صحتها لا تترتب عليها عقوبات.
7. توفير قنوات إبلاغ لا تقل عن: الهاتف، والموقع الإلكتروني، والبريد، والبريد الإلكتروني.
8. إعداد برامج توعوية بمسؤوليات الإبلاغ.

وحدة معالجة بلاغات المخالفات

تتطلب السياسة إنشاء وحدة إدارية مستقلة لاستقبال البلاغات ومعالجتها، ترتبط بإدارة الالتزام. والاستقلالية هنا تعني عملياً ألا ترتبط الوحدة بإدارة يُتوقع أن تحقق فيها، وأن توجد قاعدة موثقة مسبقاً لمسار البلاغات التي تخص رئيس الوحدة أو مسؤول الالتزام أو أحد التنفيذيين أو أعضاء المجلس، وأن تتوافر موارد كافية لاستقبال البلاغات على مدار الساعة.

الحماية وحدودها

> **حدٌّ جوهري كثيراً ما يُغفل**
>
> بموجب السياسة، **لا يستطيع المُبلّغ الذي يُبلّغ بصفة مجهولة المطالبة بالتزامات الحماية المقررة على المنشأة**. وليس هذا سبباً لإلغاء الإبلاغ المجهول — فهو يكشف بلاغات ما كانت لتصل — بل سبب لتوضيح ذلك بصراحة عند تقديم البلاغ، حتى يختار المُبلّغ بين إخفاء الهوية والحماية عن بيّنة، لا أن يكتشف الفارق بعد وقوع الانتقام.

ولا يجوز الإفصاح عن معلومات المُبلّغ إلا للجهات المختصة، أي جهات التحقيق والجهات القضائية. كما تلتزم المنشأة بحماية المُبلّغين غير الكيديين من أي إجراء انتقامي من قِبل منسوبيها.

مراحل معالجة البلاغ الثماني

م	المرحلة	الدليل الذي يجعلها قابلة للتدقيق
١	استقبال البلاغ	سجل موثّق بالتاريخ والوقت وقناة الاستقبال، وإشعار بالاستلام متى أمكن
٢	التقييم الأولي	تصنيف البلاغ ودرجة جسامته مع تدوين المسوّغات ومَن قام بالتقييم
٣	تحديد خطة التحقق	خطة مكتوبة ونطاق محدد قبل بدء العمل
٤	توثيق مسوّغات المعالجة	سبب اختيار هذا المسار — وهي أكثر مرحلة يجري تجاوزها
٥	قرار المعالجة	القرار وصاحبه وتاريخه، مع الإفصاح عن تعارض المصالح
٦	متابعة التنفيذ	تتبّع الإجراءات التصحيحية حتى الإنجاز لا حتى الإسناد
٧	حفظ السجلات	الاحتفاظ بالبلاغات والمستندات للمدد النظامية
٨	رفع التقارير	تقرير دوري إلى المجلس ولجنة المراجعة عن الحالات والإجراءات

وتلتزم المنشأة عند تلقّي البلاغ بالتعامل معه بالجدية اللازمة أياً كانت طبيعته أو مدى كفاية معلوماته، واتخاذ إجراءات حماية المُبلّغ، وإشعاره بالاستلام وبالقرار متى أمكن، واتخاذ الإجراءات التصحيحية عند ثبوت المخالفة، وإحالة البلاغ إلى الإدارة الرقابية أو التحقيقية المختصة.

نظام التتبّع الآلي

تتطلب السياسة نظاماً يتتبّع قناة استقبال البلاغ، وإجمالي البلاغات، وتصنيفها بحسب الموضوع، والمعالَج منها وما هو قيد المعالجة، ونوع المعالجة، مع القدرة على إصدار تقرير عن أي مرحلة من مراحل المعالجة بناءً على طلب البنك المركزي. وهذا الشرط الأخير هو الجوهر: يجب أن تكون البيانات قابلة للاستخراج فوراً، لا أن تُعاد تركيبها من جداول خلال أسبوع.

الإطار السعودي الأوسع

لا تعمل سياسة البنك المركزي بمعزل عن غيرها. فملف البلاغ يحتوي بيانات شخصية كثيفة عن المُبلّغ والمُبلَّغ عنه والشهود، وغالباً ما يتضمن نسبة أفعال جرمية، ما يستوجب تطبيق نظام حماية البيانات الشخصية: تحديد الغرض،

وتقليل البيانات، ومدد الاحتفاظ، والقيود على نقل البيانات خارج المملكة. والجهة المختصة بالإشراف هي الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).

كما طوّرت المملكة إطاراً لحماية المُبلّغين والشهود والخبراء والضحايا، ببرنامج وطني تحت إشراف النيابة العامة تديره لجنة تضم النيابة العامة ووزارة الداخلية ورئاسة أمن الدولة وهيئة الرقابة ومكافحة الفساد (نزاهة). ومتى تعلّق البلاغ بموظف عام كانت نزاهة هي الجهة المختصة، ما يستوجب وجود مسار إحالة موثّق للجهات الخارجية وقاعدة تحدد متى تتوقف المعالجة الداخلية.

أسئلة لمجلس الإدارة ولجنة المراجعة

1. متى اعتمد المجلس سياسة الإبلاغ آخر مرة، ومتى موعد المراجعة السنوية القادمة؟
2. كم بلاغاً ورد عبر كل قناة من القنوات الأربع؟ القناة التي لم يرد عبرها شيء إما مجهولة أو غير موثوقة.
3. ما متوسط ونسبة الـ٩٥٪ للزمن بين الاستلام والتقييم الأولي؟
4. كم عدد الحالات المفتوحة، وما عمر أقدمها؟
5. هل نستطيع اليوم إصدار تقرير عن أي حالة في أي مرحلة لو طلبه البنك المركزي؟
6. من يحقق في بلاغ يخص تنفيذياً أو عضو مجلس إدارة، وأين ذلك موثّق؟
7. هل نُخطر المُبلّغ المجهول بأن إخفاء الهوية يُسقط التزامات الحماية؟
8. هل قِسنا مدى معرفة المنسوبين بالقناة وثقتهم بها؟
9. هل تُحفظ بيانات الحالات داخل المملكة، ومن يستطيع الوصول إليها من خارجها؟
10. هل تعرّض أي شخص أبلغ داخلياً لإجراء تأديبي منذ المراجعة الأخيرة؟
