SAFE REPORTING SERVICE PROVIDER STANDARD: DIGITAL EXTERNAL

>> SafeLine – DigEX <<

The best practice standard for digital safe reporting service providers.
Developed by The Ethics Institute.

Input provided by industry experts

INTRODUCTION

The Safe Reporting Service Provider Standard Digital External (SafeLine-DigEX) is a best practice standard which specifies requirements for a quality digital safe reporting system managed by independent safe reporting service providers. Independent safe reporting service providers of digital platforms use the standard to demonstrate their ability to consistently provide quality services that protect whistle-blowers. The standard should be seen as a business management tool that independent digital safe reporting service providers can use to drive value, improve operations and reduce operational and reputational risks.

SCOPE OF APPLICATION

SafeLine-DigEX is a set of best practice norms for professional and ethical conduct for external digital safe reporting service providers (hereafter 'service providers') that enable client organisations (hereafter 'clients') to report observed or perceived unethical conduct confidentially and anonymously.

OBJECTIVES OF SafeLine-DigEX

The objectives of SafeLine-DigEX are:

- To strengthen the external digital safe reporting industry by establishing a best practice industry standard;
- To provide quality assurance to organisations requiring external digital safe reporting services;
- To create conditions in which would-be whistle-blowers can report misconduct with confidence;
- To differentiate legitimate from non-legitimate service providers;
- To discourage sub-standard service providers from entering the market; and
- To certify service providers as a "TEI-Certified External Digital Safe Reporting Service Provider".

BENEFITS OF SafeLine-DigEX CERTIFICATION

Complying with SafeLine-DigEX will help service providers to:

- Organise their internal systems and processes;
- Improve the efficiency of their internal systems and processes;
- Continually improve their service delivery;
- Create conditions in which would-be whistle-blowers can report misconduct with confidence and anonymously; and
- Provide assurance to client organisations in terms of:
    - confidentiality of information,
    - protection of whistle-blowers' identity,
    - professional service delivery, and

- quality of reports to clients.

NORMS OF SafeLine-DigEX

This Standard is based on five guiding norms for service providers, which balance client needs, whistle-blower interests, and digital platform requirements. A description of each norm, the standards supporting it, and the conditions for compliance with it, are provided below.

>> Norm 1: INTEGRITY

A commitment to integrity requires that the service provider is honest, adheres to clear moral principles, and is professional. In order to demonstrate commitment to the norm of integrity, service providers must comply with three standards, namely (1) being honest, (2) ensuring that safe reporting service provider staff are of a high ethical and professional standing, and (3) ensuring complete, accurate and truthful reporting.

INTEGRITY	
Standard 1.1	**Having integrity means that service providers are honest and will, therefore:** i. Honour the letter and spirit of their contractual agreements; ii. Be transparent about the services they are able to provide; iii. Make no misrepresentations; iv. Ensure the service provider pays all relevant fees; v. Pro-actively inform clients of problems relating to the delivery of, or changes in, the service; vi. Accept new clients only if the service provider has sufficient capacity to provide new clients with agreed-upon services; and vii. Possess the capacity to provide all services advertised.
Standard 1.2	**Having integrity means that service providers ensure that safe reporting service provider staff are of a high ethical and professional standing. They will therefore:** i. Perform background checks on prospective employees which include, as a minimum, qualifications and certificates, criminal records, past employer references, to ensure that applicants' claims are honest and truthful; and ii. If contracted to interact with whistle-blowers, conduct continual reviews of the quality of service provider staff's interactions with whistle-blowers in order to obtain complete and accurate information.
Standard 1.3	**Having integrity means that service providers ensure complete, accurate and truthful reporting. They will therefore ensure that:** i. All relevant information provided by a whistle-blower is included in the submission; ii. Reporting is objective and unbiased; iii. Staff do not solicit any other services related to the submission; iv. Reporting is accurate; v. Submissions are professionally presented; and vi. The anonymity and confidentiality of the whistle-blower is respected, in accordance with the whistle-blower's preference.

>> Norm 2: EFFICIENCY

A commitment to efficiency requires that the external safe reporting service provider delivers high-quality information to clients in a timely manner. In order to demonstrate commitment to the norm of efficiency, service providers must comply with five standards, namely, (1) performing services in a timely manner, (2) ensuring that safe reporting service provider staff and client staff are properly trained on the use of the digital whistle-blowing tool, (3) providing clients with customised service options, (4) assisting clients with awareness and communications initiatives, and (5) continually improving service.

EFFICIENCY	
Standard 2.1	**Being efficient means that service providers will perform services in a timely manner. They will therefore ensure:** > Reports are sent to the authorised client representative(s) within 24 hours of receiving information from a whistle-blower, except for weekends; > Have in place a channel for immediate emergency reporting of incidents; and > Perform other contracted services within agreed-upon timeframes.
Standard 2.2	**2.2.a Being efficient means that service providers will ensure that their staff are properly trained on the use of the digital whistle-blowing tool. They will therefore ensure that service provider staff and / or the digital platform:** > Are trained / or programmed to: o Provide information regarding the functioning of the safe-reporting solution; o Create professional and comprehensive reports; o Reflect the business of the client (for example, core operations, regions, subsidiaries and client-specific terminology); > Link submissions to previous submissions about the same incident; **2.2.b Being efficient means that service providers will ensure that client staff are properly trained on the use of the digital whistle-blowing tool. They will therefore ensure that client staff:** > Are trained to: o Interact effectively with whistle-blowers (who, what, where, when and how); o Request pertinent information from whistle-blowers; o Follow-up with whistle-blowers within legislative timeframes; > Are provided with relevant learning opportunities on an annual basis.
Standard 2.3	**Being efficient means that clients are provided with customised service options. Service providers will therefore customise to agreed-upon requirements with regard to:** > Questions for whistle-blowers; > Whistle-blower submissions; > Other reports (such as monthly reports); and > Awareness and training material.
Standard 2.4	**Being efficient means that clients are assisted with awareness and communication initiatives. Service providers will therefore:**

	> Provide customised training to client staff about the safe reporting solution; > Provide customised awareness material suitable to the client on or before the digital platform is launched and thereafter annually; > Follow up annually in writing or in person with the client to offer training and awareness material and/or services; and > Advise clients at least annually in writing or in person on the importance of awareness and communication initiatives and on methods to maximise the efficiency and effectiveness of the safe reporting digital platform. These methods include: o Obtaining endorsement of the digital whistle-blowing tool by the client company's top leadership; o Publicising the functioning of the safe reporting solution, with specific emphasis on measures to protect whistle-blowers' anonymity; o Setting out the respective responsibilities of the service provider, client, and whistle-blower; and o Publicising that the safe reporting solution is hosted independently from the client organisation, and that the client or third party cannot alter information on the digital platform.
Standard 2.5	**Being efficient means that service providers shall continually improve their services. They will therefore:** > Request bi-annual written feedback from clients about the quality of their service; > Stay abreast of technological developments in data management systems and advances in digital reporting; and > Act on client feedback to improve service delivery to clients.

>> Norm 3: INDEPENDENCE

A commitment to independence requires that the service provider remains free from conflicts of interest with their clients, clients' stakeholders and other service providers. Independence includes two standards that service providers must comply with, namely, (1) identifying, declaring and avoiding conflicts of interest, and (2) hosting an independent safe reporting digital platform.

INDEPENDENCE	
Standard 3.1	**Being independent means that service providers must identify, declare and avoid conflicts of interest. Protecting the interest of the whistle-blower is of prime importance and supersedes the interest of the client. Thus, the interest of the whistle-blower is the ultimate consideration in determining whether a situation presents a conflict of interest. Service providers will therefore:** > Require annual declarations of independence from service-provider monitors and third-party monitors; > Identify, declare and avoid any contracts, agreements, arrangements or situations that could negatively affect the service provided to clients and whistle-blowers; and > Identify, declare and avoid any contracts, agreements, arrangements or situations that could create a perception of not being independent from clients.

Standard 3.2	**Being independent means that service providers must host an independent safe reporting digital platform. They will therefore:** > Host a safe reporting digital platform independently from the client organisation to ensure that the client or third parties cannot alter information on the platform.

>> Norm 4: PROTECTION

A commitment to protection requires that the service provider respects whistle-blowers' anonymity, as well as the confidentiality of their information, as applicable and appropriate, in order to prevent victimisation. Protection includes five standards, namely, (1) ensuring the security of the safe reporting digital platform, (2) ensuring that the location of the safe reporting service provider is discreet, (3) guaranteeing whistle-blowers' anonymity, (4) assuring the confidentiality of communications received and submissions delivered and (5) ensuring that information received through all communication channels is documented and securely stored.

PROTECTION	
Standard 4.1	**Protecting whistle-blowers means that service providers will ensure the security of the safe reporting service provider digital platform. They will therefore ensure that:** > Access to the digital platform is always strictly monitored; > Appropriate logistical and physical access controls are in place to protect infrastructure, networks, hardware and software; > Appropriate logistical, digital and physical access controls protect information received from whistle-blowers, as well as reports to relevant client recipients; and > Visitors (including cleaning and security staff) and/or suppliers of services to the digital platform are monitored and supervised.
Standard 4.2	**Protecting whistle-blowers means that service providers will ensure that the location of the safe reporting service provider is discreet. They will therefore ensure that:** > The safe reporting service provider is not identifiable with overt signage; and > External stakeholders, such as service providers and contractors, sign a register confirming their presence in in the area where the digital platform is located.
Standard 4.3	**Protecting whistle-blowers means that service providers will guarantee whistle-blowers' anonymity and confidentiality. They will therefore ensure that:** > There is no IP address or IMEI number identification mechanisms in place to identify the whistle-blower; > Whistle-blowers can be provided with the choice of: o Remaining anonymous to the service provider and / or the client; or o Revealing their identity to the service provider and / or the client; > Reports to client's respect and protect whistle-blowers' anonymity by voiding them of any identification data, including gender and position; > Whistle-blowers' confidentiality is protected in respect of third parties should they expressly request that their identity be revealed to the client, thus waiving their anonymity; > Whistle-blowers receive unique reference numbers; and

	> Whistle-blowers receive case or user codes, choose anonymous nicknames, that are not stored at the backend.
Standard 4.4	**Protecting whistle-blowers means that service providers must assure the confidentiality of communications received and reports delivered. Service providers will therefore ensure that:** > All submissions are delivered to the authorised client representative(s) only; > Appropriate logistical, digital and physical access controls protect infrastructure, networks, hardware and software; > Appropriate logistical, digital and physical access controls protect information received from whistle-blowers, as well as reports to clients; > Changes to authorised client recipient(s) of reports are verified in writing; and > The confidentiality of information is secured by password protection or encryption of all submissions sent via email to authorised client representative(s). > The confidentiality of information contained in monthly reports to authorised client representative(s)is secured by password protection.
Standard 4.5	**Protecting whistle-blowers means that information received through all communication channels is recorded and securely stored. Service providers will therefore:** > Invest in, and maintain, infrastructure to ensure that all information received is stored securely; > Ensure that all information received is stored securely; and > Ensure that an audit trial is available of all communication with whistle-blowers.

>> Norm 5: AVAILABILITY

A commitment to availability requires that the service provider ensures easy and reliable access to the external safe reporting digital platform, 24 hours per day, 365 days per year. Being available includes the following two standards that service providers must adhere to, namely, (1) ensuring the maximum up-time, and (2) providing a choice of user-friendly communication channels 24 hours a day, 365 days a year.

AVAILABILITY	
Standard 5.1	**Being available means that the service provider must provide assurance that the digital platform has maximum up-time. Third parties and service providers will therefore:** > Maintain continuity / disaster plans that are regularly tested; > Have appropriate and comprehensive insurance to protect the digital platform and related infrastructure; and > Conduct regular testing of all systems at the back- and front end.
Standard 5.2	**Being available means that service providers provide a user-friendly communication channel 24 hours a day, 365 days a year. They will therefore:** > Provide clients with a digital platform for whistle-blowers to report misconduct; > Ensure that the digital platform is easily accessible and free of charge, if possible; > Provide services in the languages agreed-upon with the client; > Translate submissions received in agreed-upon languages before sending reports to the client; and

	> Provide for response to whistle-blowers via the digital platform 24 hours a day, 365 days a year.

SafeLine-DigEX CERTIFICATION

1. TEI will provide the Standard to any eligible service provider who wishes to apply for certification.

2. On submission of a completed application form, which entails a self-assessment against the Standard, TEI will conduct a preliminary assessment of the information. Additional information may be requested from the service provider.

3. Upon completion of the preliminary evaluation, TEI will conduct a site visit to the service provider and any other relevant physical or digital site(s). During this visit, the assessor will interview staff, observe operations, and review and inspect documentation to determine if the service provider complies with the Standard.

4. On completion of the assessment, the assessor will submit the final report for the service provider's attention. Recommendations for improvements will be included where necessary.

5. Service providers who adhere to all the norms and standards will receive a certificate of compliance, as well as the relevant logo banner from TEI. The certification will be valid for one year.

ABOUT THE ETHICS INSTITUTE

The Ethics Institute is an independent public institute producing original thought leadership and offering a range of services and products related to organisational ethics.

Visit our website at **www.tei.org.za**.

For enquiries about SafeLine – DigEX or any other services, contact Liezl Groenewald at liezl@tei.org.za.

building an ethical SOCIETY