Thales Internal Alert System

Thales promotes a culture of trust, integrity and compliance, and encourages employees to share their doubts and concerns about any situation or behavior that could contravene the Code of Ethics and/or the Code of Conduct – Prevention of Corruption and influence peddling, any of the Group's policies and/or instructions or any applicable law or regulation.

- The Group has defined and implemented an internal alert system that allows employees to **report internally** such situations or behaviors.

- If authorized by local regulations, the employee (or third-party individual) may also file an **external report** with the competent public authorities in accordance with the procedures provided for by local regulations.

Why reporting internally?

By making an internal alert report, the author of the alert report (the "Reporting Person") contributes to:

- the detection of conduct or situations contrary to the laws and internal rules of the Group and by allowing the implementation of corrective actions;
- the sustainability of our business by reducing, in particular, the risk of reputation and financial loss;
- the protection of the Group and the interests of its stakeholders.

In most countries, making an internal report is not an obligation and no employee can be sanctioned if he/she does not report such conduct or situations.

Who can make an alert report via the Alert Platform?

Thales Internal Alert Platform is intended to receive internal alert reports concerning any of the conduct or situations listed below, transmitted by an individual acting in good faith and without direct financial compensation:

- A staff member of the entity concerned,
- A person whose employment relationship with the entity concerned has ended, when the information was obtained within the framework of this relationship,
- A person who has applied for a job within the entity concerned, when the information was obtained in the context of this application;
- A shareholder, a partner and a holder of voting rights in the general meeting of the entity;
- A member of the administrative, management or supervisory body;
- An external or occasional collaborator (temporary or service provider);
- A co-contractor of the entity concerned, a subcontractor or, when the co-contractor or subcontractor is a legal person, a member of the administrative, management or supervisory body of these co-contractors and subcontractors, as well as a member of their staff.

Please note that if the Reporting Person is an employee, depending on her preference and the circumstances, she may also choose to report via the **hierarchical channel** or the relevant **Referent** depending on the issue raised in the report under the conditions provided for in the Group's Internal Alert System instruction.

At the informant's request, it will also be possible to arrange a face-to-face meeting within a maximum period of 7 days.

How to report via the Internal Alert Platform?

The Alert Platform is available *here*.

You can also log in 24/7:

- via the following url: https://thales.integrityline.org

- by clicking on the link entitled Thales Alert Line available from the **Group intranet home page** (My Applications / Group Applications section) **or** from the page of the **Ethics and Integrity Department** (Alert section);

- by clicking on the link entitled Thales Alert Line available from the **Group's website** (Go to Corporate responsibility/governance/Quick access: Thales Alert Line alert platform).

The Internal Alert Platform allows alert report to be issued 24 hours a day, 7 days a week, via an online form available in several languages (French, English, German, Dutch, Italian, Portuguese and Spanish).

What types of situations can be reported?

An alert report may concern any conduct or situation that contravenes the Thales Code of Ethics or the Code of Conduct "Prevention of Corruption and Influence Peddling", as well as any other breach (or an attempt to conceal a breach) of laws and regulations, particularly in the following areas:

- Bribery or influence peddling
- Fraud
- Money laundering, financial and accounting crimes
- Conflicts of interest
- Anti-competitive practices
- Trade compliance
- Personal Data protection issues
- Product Safety
- Health and Safety
- Information Security and Privacy
- Harassment/Discrimination/Workplace Violence
- Human Rights abuse
- Environmental Issues

Please note that facts, information or documents covered by **national defense secrecy**, **medical secrecy, secrecy of judicial deliberations, secrecy of investigation or judicial investigation or attorney-client privilege** are **excluded from the whistleblowing regime** regardless of their form.

How does it work?

When the Reporting Person submits a report via the Alert Platform, she is asked to fill in an electronic form, including the country where the events leading to the report occurred, the category of the alleged facts and her identity (if she agrees to identify herself).
Upon submission of the alert report, **the Internal Alert Platform automatically generates a random alert report reference**. This alert report reference that is personal to the Reporting Person, together with the password that the Reporting Person has chosen, gives her **access to a secure dialog box ("Inbox")** allowing her to exchange information and documents with the members of the Alert Monitoring Committee in charge of collecting and processing the alert report.

The Reporting Person shall receive an acknowledgement of receipt of the communication within 7 calendar days of its receipt, unless this could jeopardize the confidentiality of such communication.

Important: **In order to access the secure dialog box (Inbox) of the Internal Alert Platform, the Reporting Person must carefully keep this random alert report reference as well as the password that she has chosen.** Otherwise, she will no longer be able to access the alert submitted and will have to submit the alert report once again.

Which are the different alert lines available in the Alert Platform?

Thales Internal Alert Platform actually hosts several reporting lines:

- A **Group alert line**: This alert line is managed by the members of the Group Alerts Monitoring Committee. This Committee is set up within the Group's parent company and is composed of the Group Legal and Contracts Director, the Ethics and Integrity Director and the Human Resources Legal Director.

  To submit an alert report to the Group Alert Line, please select the Group option in the drop-down list associated to the Country Section of the online reporting form.

- Alert lines dedicated to **Major Countries** (under the meaning of Thales organization, i.e. **Australia, Germany, North America (Canada + USA), the Netherlands, Great Britain).** Each Major Country Alert Monitoring Committees is composed of the Compliance Officer and the Human Resources Director of the Major Country.

  To submit an alert report to a Major Country Alert Line, please select the relevant Major Country in the drop-down list associated to the Country Section of the online reporting form.

- **Alert lines dedicated to certain entities with ≥ 50 employees** registered **in certain EU Countries**. In most cases, the Entity Alert Monitoring Committee is composed of the Compliance Officer and the Human Resources Director of the relevant entity;

  To submit an alert report to the Alert Line dedicated to a Spanish entity reaching 50 or more employees: First select Spain in the drop-down list associated with the Country section, then choose the Category of alleged facts and then select the relevant entity.

- **An Alert line dedicated to "other countries":** i.e. other than a country listed in the drop-down list associated to the Country Section of the online reporting form. This alert line is also managed by the members of the Group Alerts Monitoring Committee.

  To submit an alert report to the Other Country Alert Line: please select the Other Country option in the drop-down list associated to the Country Section of the online reporting form.

In which situations, is it recommended to submit an alert report via the Group alert line?

The Group Alert Line is aimed to enable the Reporting Person to the Group Alerts Monitoring Committee set up within the Group's parent company, **an alert report that concerns** facts likely to characterize a **Fraud**, or an act of **Corruption** or of **Influence Peddling**, **and more generally**, when the alert report:

- **Reveals a structural problem within the Group** or that **several Group entities are affected** by the facts reported;
- **Cannot be treated impartially** at the level of the entity or the Major Country concerned due to a risk of conflict of interest and/or retaliation. For example, because the alert report involves local management, the human resources manager or the Compliance Officer of the entity;

By choosing the Group option (instead of selecting the country in which the facts covered by the report are located), the Reporting Person ensures that the alert report is sent directly to the Group Alerts Monitoring Committee set up within the Group's parent company.

Is it possible to submit an anonymous report?

The Internal Alert Platform allows anonymous reporting.
Thanks to the secure dialog box ("Inbox") dedicated to each alert report, the Internal Alert Platform allows for further exchanges with the Reporting Person while allowing her to remain anonymous if she so wishes.

Who is in charge of collecting and analyzing the alert?

Within a maximum of 15 calendar days from the date of receipt, the members of the Alert Monitoring Committee collegially assess whether the alert report is actionable or not.

If the members of the Alert Monitoring Committee collegially assess that the alert report is not actionable, they inform the Reporting Person of the reasons why the alert report is declared not actionable.

If the members of the members of the Alert Monitoring Committee collegially assess that the alert report is actionable, they appoint a Case Manager who will conduct the checks.

At any time, the Alert Monitoring Committee concerned or the appointed Case Manager reserve the right to ask the Reporting Person to provide or complete the information and documents necessary for the analysis of the actionability or the processing of her alert report.

In certain circumstances (*) the Alert Monitoring Committee receiving the alert report may request the consent of the Reporting Person to bring the alert report to the attention of the members of the Group Alerts Monitoring Committee, who will collegially determine the procedure for processing this report.

(*) Alert report concerning facts likely to characterize a Fraud, acts of Corruption or Influence Peddling, or report Revealing a structural problem within the Group or facts affecting several Group entities, impossibility to treat the alert report with impartially, alert report requiring to have the resources and support of the parent company).

Within a reasonable period not exceeding 3 months from the acknowledgment of receipt of the alert report, the members of the relevant Alerts Monitoring Committee inform the Reporting Person of the measures planned or taken, to assess the accuracy of the allegations and, if necessary, remedy the subject of the alert report.

The objective is to process the alert report within 3 months (increased to 6 months for the most complex cases).

Once the alert report is processed, the relevant Alerts Monitoring Committee presents its recommendations to the management of the entity or function concerned. It is the responsibility of the management of the entity or function concerned to adopt appropriate remediation action and to monitor their implementation.

Which protection for the Reporting Person?

The Reporting Person benefits from the protections provided by the applicable regulations.

The person reporting in good faith, any person benefiting from the protection granted to whistleblowers cannot be the subject of reprisals, threats or attempted reprisals. Anyone falling into the above categories who believes they have been subject to retaliation, threats or attempted retaliation after reporting in good faith can report through the Internal Alert System.

What confidentiality measures apply?

Any person in charge of collecting or processing an alert report shall implement measures aimed at preserving the confidentiality of the identity of the Reporting Person, of the person(s)

involved, of any third party mentioned in the alert report and of the information collected while processing the alert report.

The use of the Internal Alert Platform is recommended. All exchanges and information collected on the platform are encrypted and only visible to authorized personnel specifically authorized to collect alerts and/or designated to process them.

The person(s) involved by the alert report and any third party mentioned in the alert report also have the right to respect for the confidentiality of their identity. The Reporting Person as well as the persons interviewed in the context of the checks must ensure that they do not disclose, outside the reporting procedure, elements that would allow these persons to be identified.

What personal data protection measures apply?

Personal data is collected and processed by Thales, the legal entity which collect and/or manage the alert report and the legal entity of the Thales Group where the alleged facts occurred, acting jointly as data controller, in order to communicate with the person reporting the incident for better management of the alert. The Reporting Person has the right to access, rectify and delete her data, as well as the right to object to the processing and to its limitation.

When submitting a report, the Reporting Person is provided with detailed information on the use of her personal data.

To exercise the rights related to her personal data, the Reporting Person may also contact the Group's Data Protection Officer by sending an e-mail to the following address: dataprotection@thalesgroup.com.

oOo