WHISTLEBLOWER CHANNEL USER MANUAL

Cintas Adhesivas UBIS, S.A.

February 2024

CONTENTS

VERSION	PARTY RESPONSIBLE	REMARKS
v.1		

INTRODUCTION

The internal information channel is established as an obligation to be fulfilled by companies in accordance with the provisions of Act 2/2023, of 20 February 2023, governing the protection of persons reporting regulatory breaches and the combating of corruption.

The implementation of an internal information channel at an organisation entails fulfilment of one of the basic tools comprising an organisational and management model as referred to in the Spanish legislative system.

This channel must offer guarantees of confidentiality and anonymity for both the whistleblower and the accused, in addition to a secure means of communication, access and storage of information, and the generation of evidence. Whistleblowing channels or ethical channels are seen as the most effective means of control among anti-fraud and anti-corruption mechanisms.

WHAT IS UNDERSTOOD BY 'INTERNAL INFORMATION CHANNEL'?

The Internal Information Channel is the means via which employees, executives and members of the governing body of Cintas Adhesivas UBIS, and any third party with which the company might have a relationship (suppliers, customers, external consultants, etc.), can inform the Supervisor of the Internal Information System of any irregular conduct or breaches of our internal and external regulations, or any that could constitute a criminal act.

The Cintas Adhesivas UBIS Channel is intended to ensure a positive and harmonious working environment at the company, which is vital for its development and growth.

CINTAS ADHESIVAS UBIS has an Internal Information Channel in place, in accordance with its legitimate basis in fulfilling a legal obligation and a mission undertaken in the public interest, namely the protection of legal rights, in addition to our legitimate interest in avoiding conduct which could give rise to criminal liability for the company. This is accessible via the corresponding online form for the reporting of any conduct which could constitute a criminal offence.

WHEN MUST IT BE USED?

It must be used in all situations in which anyone learns of any conduct or act which could constitute any serious breach of criminal or administrative provisions, a breach of company regulations, or any other unlawful activity that goes against the interests of CINTAS ADHESIVAS UBIS.

The aim of this User Manual is to foster among all workers a duty to use the tool in good faith, with reports being based on acts or evidence which could reasonably indicate that the aforementioned conduct has taken place. The reporting of false information must therefore be avoided.

The Channel is not the appropriate means to address matters connected with your employment conditions. In this case you will need to follow the policies established at your organisation. If

any such matter is received, it will be immediately shelved by the Supervisor of the CINTAS ADHESIVAS UBIS Internal Information System.

HOW DO WE PROCESS THE DATA, AND WHO CAN ACCESS THE INFORMATION?

The Channel will use a form to gather the data. This may also take place anonymously.

The confidentiality of the whistleblower's data is guaranteed (email address), maintaining their anonymity unless there is a necessary and proportionate obligation to identify them, imposed by EU or domestic law within the context of an investigation conducted by national authorities or as part of court proceedings, in which case the data must be communicated to the authorities responsible for the matter.

As these data are anonymous for the Supervisor of the Internal Information System, the inherent design of the application itself prevents any type of retaliation being brought against the whistleblower.

In any event, the data of the data subjects in question will be confidential, and will be processed in accordance with the data protection regulations in force.

HOW LONG DO WE STORE THE DATA FOR?

All information that could serve as evidence of the conduct or acts reported must be stored for as long as a legal obligation exists to store such documents.

In any event, the provisions of the Internal Information System Policy will be fulfilled, and the information will thus be stored for as long as is essential to decide whether or not to initiate an investigation into the events.

In any event, 3 months after the report is received, if no investigative actions have begun, the information must then be deleted, unless the purpose of storage is to retain evidence of the functioning of the system. Those reports which are not acted upon may only be recorded in anonymous form, without the obligation to block access established in the Spanish Data Protection Act being applicable.Information regarding complaints that have been acted upon and are in the process of investigation will be as stored for as long as relevant for the process corresponding to the commission of criminal offences outside the channel.

HOW DO WE ACCESS THE WHISTLEBLOWING CHANNEL?

The Whistleblowing Channel may be accessed via the following link:

https://cybersecurity.telefonica.com/sandasgrc/?organization=CCD057D1-7F62-47CD-BC2E-463B5BC738B0

This link provides access to the platform of an external service provider in order to guarantee the anonymity and protection of the data of the whistleblower, the accused, and any persons named in the communication.

The platform may be used to complete a form which, if this is entered, may record the email address used to receive notification of receipt of the communication and the subsequent decision stating the actions taken by the organisation. Neither the third-party service provider nor the organisation itself will be aware of this email address, since all notifications will be contained within the platform.

You may use the form to provide any information you wish and to upload any files constituting evidence of the events reported.

Once you have completed the form, you will receive notification of receipt and a communication tracking number.

Within a maximum of 3 months, you will receive notification via the same mechanism, including the decision issued by CINTAS ADHESIVAS UBIS, and will be informed of the actions conducted.

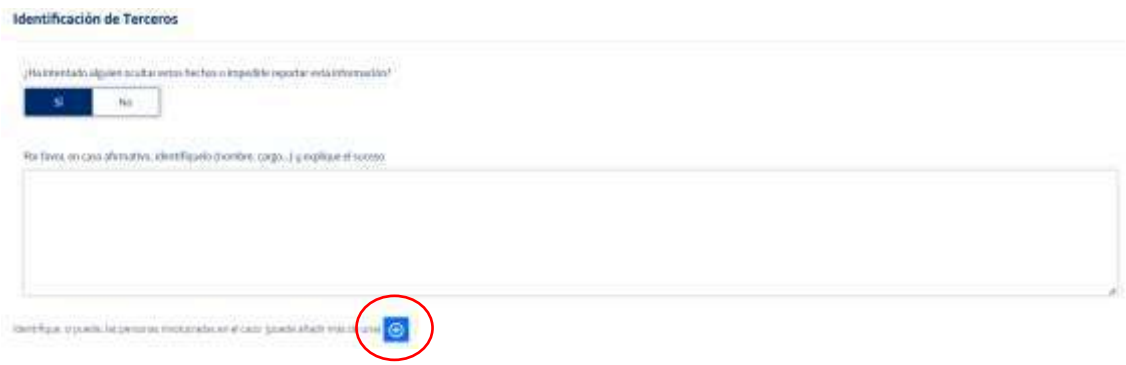
WHAT WILL WE DO WHEN WE RECEIVE A COMMUNICATION?

Following receipt of the communication, the Supervisor of the Internal Information System will proceed to analyse the events in order to determine whether the case should be shelved, or otherwise whether an investigation should be opened into the events reported.

The Supervisor is responsible for ordering the initiation of an investigation, if they deem this necessary, and may use the same tool to request any additional information or evidence to confirm the circumstances required and proceed to open the corresponding investigation file.

The data of those referred to in the communication will never be revealed if this could constitute a conflict of interest with the System Supervisor or the management team of the organisation.

If the information communicated could accuse the person acting as Supervisor of the Internal Information System, then the form would need to place on record their full name and the following email address: p.ibarbia@ubis.es in the space indicated on the form below in order to prevent this person from accessing it:



The Supervisor is obliged to maintain the confidentiality of all information they may access as a result of the communication sent.

Lastly, the service provider responsible for maintaining the channel will periodically check that the tool is functioning properly.

WHAT IS THE DIFFERENCE BETWEEN AN ALERT AND A CONSULTATION?

You can, as a whistleblower, use an alert to communicate any matter that you believe could be a serious violation in administrative or criminal terms.

You can use a consultation to raise any question as to the functioning of the channel, anti-retaliation measures or the deadlines for your alert to be resolved, or any other question that could be derived from or originate in use of the channel.

It must not under any circumstances be used to submit consultations that do not concern the internal information system itself.