Inwido Group Whistleblowing Policy

Document history			
Date:	Changed by:	Version:	Comments
April 2026	Malin Cullin	1.0	Update in line with legislation, approval by BoD.

1. Document information

Policy

The Inwido Group is committed to high standards of ethical business conduct and recognises the importance of that breaches and reasonably suspected breaches of law that are harmful to the public interest are reported in order to allow the business to take appropriate actions.

This whistleblowing policy (the "**Whistleblowing Policy**" or the "**Policy**") establishes Inwido Group's internal reporting channels and procedures for whistleblowing (the "**Internal Reporting Channel**"). The Internal Reporting Channel can be used by reporting persons to report breaches internally.

Target group

This Whistleblowing Policy applies to [Inwido AB (publ), 556633-3828, and all group companies listed in Appendix 1] ("**Relevant Inwido Group Company**") and the target group is all individuals (reporting persons) who may report breaches through the Internal Reporting Channel.

Approval and policy owner

The Board of Directors have on April 27, 2026 approved this Whistleblowing Policy.

The CEO of Inwido Group is the owner of the Whistleblowing Policy, and responsible for ensuring that the Policy is compliant with applicable laws and regulations and internal policies, routines and procedures. The owner shall also ensure that the Policy is reviewed on a regular basis to ensure that it is up to date.

2. Background and purpose

Directive 2019/1937 on the protection of persons who report breaches of Union law (the "**Whistleblowing Directive**") and local laws implementing the Whistleblowing Directive (the "**Whistleblowing Act**) e.g. includes provisions on establishment of internal reporting channels.

The Whistleblowing Directive requires companies that have at least 50 employees to establish internal reporting channels and procedures for internal reporting and follow-up of reported breaches. Moreover, the Whistleblowing Directive provides that reporting persons shall be protected against retaliation and from liability for breach of confidentiality as a result of a reported breach.

The purpose of this Whistleblowing Policy is to outline who can use the Internal Reporting Channel, which types of breaches that can be reported, how breaches can be reported and the measures to be taken review and investigate reports, including assessing the accuracy of a report, submitted by a reporting person through the Internal Reporting Channel.

Moreover, the Whistleblowing Policy outlines when a reporting person can report breaches externally to appointed public authorities and describes the protection afforded to reporting persons under the Whistleblowing Act against retaliation and from liability for breach of confidentiality.

3. internal reporting channel for whistleblowing

Who can use the Internal Reporting Channel

The Internal Reporting Channel can be used by a reporting person, who have acquired information on a breach in a work-related context, and is:

- an employee of Relevant Inwido Group Company or a person otherwise engaged to perform work (for example temporary agency worker) on behalf of Relevant Inwido Group Company,
- contractors (for example consultants) engaged by Relevant Inwido Group Company,
- a job applicant who inquires, applies or has applied for a position with Relevant Inwido Group Company,
- a person who seeks or performs voluntary work for Relevant Inwido Group Company,
- an intern who carries out an internship with Relevant Inwido Group Company,
- a member of the Board of Directors of Relevant Inwido Group Company, or
- an active shareholder of Relevant Inwido Group Company, who are available or otherwise perform work for Relevant Inwido Group Company.

Other categories of individuals, for example customers, contact persons of suppliers and business partners, are referred to and encouraged to use ordinary reporting channels to report breaches or reasonable suspected breaches.

Which type of breaches that can be reported through the Internal Reporting Channel

The Internal Reporting Channel may be used, and you are encouraged to use the Internal Reporting Channel, to report breaches in a work-related context as outlined below.

A "**breach**" is defined as information on (i) actual or suspected wrongdoings that are of public interest, and (ii) actual or suspected breaches of law within certain areas, including – among others – the following areas:

- financial services, anti-corruption, and prevention of money laundering,
- product safety and compliance,
- protection of health and environment,
- consumer protection,
- data protection and privacy, and
- information security.

Examples of breaches that may be reported through the Internal Reporting Channel include fraud, bribery, serious work environment breaches, serious cases of discrimination or harassment, and unlawful uses of personal data.

In order to report a breach through the Internal Reporting Channel, you must have reasonable grounds for believing that the information concerning the breach is true. However, there is no requirement that you submit any evidence or supporting information for the breach. If you have reasonable grounds for believing that the information regarding the breach is true, you will still be protected under this Policy, even if it turns out that the suspected breach was incorrect upon further investigation of the report, please see Section 4 of the Policy (*Protection for Reporting Persons*) below.

Please note, however, that abuse of the Internal Reporting Channel constitutes a serious violation of this Whistleblowing Policy and, if you are an employee, your employment obligations in accordance with your employment agreement and could result in employment actions being taken, up to an including termination of employment.

The Internal Reporting Channel is a supplementary channel to ordinary internal reporting channels. This means that the Internal Reporting Channel should only be used for reporting breaches that may be reported through the Internal Reporting Channel as outlined above.

This also means that ordinary reporting channels shall be used for raising issues or concerns that do not qualify as a breach under the Policy, for example issues that concern your own employment or employment conditions. Such issues and concerns shall, unless they are sufficiently serious to qualify as a breach that may be reported using the Internal Reporting Channel, be reported to your line manager, HR or the legal team, as appropriate.

Please also note that the Whistleblowing Act may not be applicable to certain information. For example, security classified information under the Protective Security Act (2018:585) is exempted under Swedish law.

How you report breaches or reasonably suspected breaches

Reporting by using the Internal Reporting Channel

You can report breaches by using the Internal Reporting Channel in the following ways:

- **Web-reporting tool**: submit a report in our secure and confidential web-reporting tool, which is available at https://report.whistleb.com/sv/portal/inwido.
- **Meeting**: you can also request a meeting with a person of the Investigation Team, which shall be held within a reasonable time following your request. You request a meeting by using the contact details set out in Appendix 1.
- **Telephone**: you can also report to the Investigation Team via telephone by using the telephone number set out in Appendix 1.

If you submit your report verbally, your report will (i) be recorded, if you consent to such recording, (ii) documented in writing by way of meeting minutes, which you will be given the opportunity to review, rectify and approve by way of your signature, or if the report is not made in a meeting (for example by telephone, (iii) documented by way of a transcript or note summarising your report.

To facilitate the investigation of your report, you are encouraged to provide a detailed description of the breach, including the type and nature of the breach, time and place of the breach (if possible), and by providing any supporting information that you have access to.

It is possible to use the web-reporting tool to submit anonymous reports. However, you are encouraged to include your contact information in the report in order to allow the Investigation Team to reach out to you directly for obtaining further information or follow-up questions. This being said, if you choose to be anonymous, measures will be taken to, to the extent possible, protect your identity and we will not take any measures to discover your identity.

You will receive a notification with a confirmation that your report has been received within seven (7) days from the date of the receipt of your report, unless (i) you have stated that you do not want to receive such confirmation, or (ii) there is reason to assume that such confirmation cannot be made without disclosing your identity.

Reporting externally to specific public authorities

We encourage you to report breaches internally by using the Internal Reporting Channel, but it is also possible to report externally to specific public authorities which have been appointed to receive reports of breaches within their respective designated areas of responsibility. As such, which public authority that you should submit your report to depends on the type of the breach. The report to the public authority should be made using the relevant authority's established external reporting channel.

Links to the appointed public authorities and their respective areas of responsibility are included in Appendix 1.

Investigation of reports submitted through the Internal Reporting Channel

Investigation Team

Relevant Inwido Group Company has appointed a team of persons responsible for reviewing and investigating reports submitted through the Internal Reporting Channel, (the "**Investigation Team**"). The Investigation Team currently consists of the, EVP People & Culture, Business unit/plant HR manager or in the smaller units of Inwido group the Managing director.

Reports submitted through the Internal Reporting Channel will be investigated by the relevant persons of the Investigation Team. The persons of the Investigation Team are authorised to take appropriate measures to investigate and review a report to assess the accuracy of the reported breach, including to communicate with and provide feedback to the reported person regarding the reported breach. The Investigation Team shall operate independently and in an impartial way.

Investigation of reports

Once a report has been received by the Investigation Team, a person of the Investigation Team will review the report to evaluate and assess whether the reported breach qualify as a breach under this Policy.

If the Investigation Team, following a review of your report, makes the assessment that the reported breach should not be managed in the Internal Reporting Channel, you will be informed of this within a period of seven (7) days following the receipt of your report and referred to your line manager or the appropriate function, for example HR, if you wish to maintain your report.

If the reported breach falls within the scope of the Policy, the Investigation Team will take appropriate actions to investigate the report in order to assess the accuracy of the reported breach.

You will normally receive reasonable feedback within three (3) months following the receipt of the report of the measures or actions taken or envisaged to be taken as a result of the report. If possible and appropriate, you will also be informed of the status of the investigation and any actions taken as a result of your report on a continuous basis.

The Investigation Team shall comply with the procedure for the Internal Reporting Channel when investigating a reported breach.

Measures as a result of an investigation

Following the conclusion of an investigation of a report, the Investigation Team shall present recommendations for appropriate measures to be taken a result of the investigation.

Confidentiality of reporting persons and other persons involved in an investigation

The Investigation Team is obligated under law to observe confidentiality and secrecy with respect to the identity of the reporting person, regardless of whether you have reported anonymously or not, and the identity of any other individuals involved in the investigation.

4. Protection for reporting persons

Protection against retaliation etc.

If you have reported a breach or a suspected breach using the Internal Reporting Channel, which you had reasonable grounds for believing is true, you will be protected against any form of retaliation as a result of the reporting.

Retaliation means any, direct or indirect, act or omission which occurs in a work-related context, which is prompted by internal reporting using the Internal Reporting Channel or external reporting to the relevant public authorities, and which causes or may cause unjustified detriment to the reporting person. Examples of retaliation include, but is not limited to, suspension, termination of employment or an assignment, demotion, transfer of working duties, unfair treatment etc.

The protection against retaliation does not, however, apply if you have committed a criminal offence as a result of the reporting or in connection with obtaining information for the report (for example due to unlawful hacking).

Moreover, provided that you have reasonable grounds for believing that a breach is true, you are also protected against measures which prevents or tries to prevent you from reporting the breach using the Internal Reporting Channel or externally to relevant public authorities.

Protection against liability for breach of confidentiality

If you have reported a breach or a suspected breach using the Internal Reporting Channel, which you had reasonable grounds for believing is true, you will also be protected against liability for breach of confidentiality obligations, for example confidentiality undertakings in your employment agreement if you are an employee. However, you have no right to disclose documents (*Sw: handlingar*).

5. processing of personal data in the internal reporting channel

Only authorized persons, including the Investigation Team, will have access to personal data in the Internal Reporting Channel.

For more information on the processing of personal data in the Internal Reporting Channel, please see www.inwido.com/WhistleblowingPrivacyNotice

* * * * *

APPENDIX 1

Contact details of the Inwido companies which are subject to this policy.

Inwido company (name & registration number)	**Postal address**	**E-mail address to request a meeting**	**Telephone number to make a verbal report**
Klas 1, 0981161-9	Nissinjokimutka 2, FI-93600 Kuusamo, Finland	Marko.Kohvakka@pihla.fi	+358504015023
Pihla Group 1882624-9	Konikuja 7, 85800 Haapajärvi, Finland	Marko.Kohvakka@pihla.fi	+358504015023
MV Center 0545266-3	Pikkukorventie 14, 37150 Nokia, Finland	Marko.Kohvakka@pihla.fi	+358504015023
JABS Group 37416258	Kratholmvej 27B, 5260 Odense S, Denmark	Martin.Murrekilde@jabsgroup.com	+4524200545
CWG 5686121	Pywell Road, Willowbrook Industrial Estate, Corby, Northamptonshire, NN17 5XJ, UK	maryanne.edmonds@cwgchoices.com	+44(0)1536 271940
Westcoast 556528-1200	Kardanvägen 42, 461 38 Trollhättan	anna.akerfeldt@westcoastwindows.se	+46 0720 -704472
Outrup Vinduer Og Døre 72381211	Outrupstræde 31, 7900 Nykøbing M, Danmark	pia.elkaer@inwido.dk	45 23654497
Lyssand Frekhaug AS 988381063	Ulsmågvegen 7 5224 NESTTUN BERGEN Norge.	henry.krohnstad@lf-as.no	+47 47912949 / 56 30 33 00
Artickaihdin 3434551-7	Linjatie 14, 80140 Joensuu, Finland	Marko.Kohvakka@pihla.fi	+358504015023
Elitfönster 556007-3073	Box 153, 574 22 Vetlanda	Victoria.Ersson@elitfonster.se	0730711855
Winbas 111775687	Žalgirio g. 90, LT-09303 Vilnius, Litauen	Indre.Eigminiene@winbas.eu	+37052051212
KPK Døre og Vinduer	Rogalandsvej 3, DK-7900	brian.frimor@inwido.dk	+4522100302

A/S 15646101	Nykøbing M, Danmark		
Dekko Window Systems Ltd 5686121	Dekko House, Margaret Street, Ashton Under Lyne, Ol7 0qq, Uk	dkelly@dekkowindows.com	0161 406 0055
Inwido AB 556633-3828	Engelbrektgatan 15, 211 33 Malmö, Sweden	Malin.Cullin@inwido.com	+46734196286
Outline Vinduer A/S 29 18 91 10	Fabriksvej 4, 9640 Farsø, Denmark	Sarah.Nauer-Newstead@inwido.dk	+45 60820531
Profin OY 2461589-4	Tulotie 2, 93100 Pudasjärvi, Finland	Marko.Kohvakka@pihla.fi	+358504015023
AJM okna-vrata-senčila d.o.o 5391610000	Kozjak nad Pesnico 2A, 2211 Pesnica pri Mariboru, Slovenia	ivan.marusic@ajm.si	++386 51 342 205
A-lackering AB 556120-8827	Box 142, 576 23 Sävsjö, Sweden	marianne.steene@alackering.se	+46 724 67 33 05
Alakiernia Sp.zo.o 220169272	ul. Bolesława Krzywoustego 1, 84–300 Lębork, Poland	katarzyna.franczak@alakiernia.pl	+48 506640907
Diplomat Dörrar AB 556606-8234	Tallvägen 30, 564 35 Bankeryd, Sweden	mari.eriksson@diplomatdorrar.se	+46703222955
Allan Brothers Ltd 5829849	Allan House, Ord Road, Berwick-upon-Tweed, TD15 2 XU, UK	Christine.rafferty@allanbrothers.co.uk	01289 334652

Sidey Solutions Ltd 9613925	71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, UK	cath.macaulay@sidey.co.uk	07387 140923
Walker Profiles Ltd SC173084	57 Feus Road, Perth PH1 2AX, UK	cath.macaulay@sidey.co.uk	07387 140923
ERA Fönster i Sverige AB 556124-2768	Slottsmöllan 17F, 302 31 Halmstad, Sweden	martin.mollborn@erafonster.se	+46 72 099 53 10
Hajom Skjutdörrar AB 556304-8098	Kvarnbacken 2, 511 97 Hajom, Sweden	christofer.rosberg@elitfonster.se	+46104514451
SnickarPer AB 556136-4158	Furuvägen 1 331 94 Värnamo, Sweden	christofer.rosberg@elitfonster.se	+46104514451
Steelform Scandinavia AB	Värendsgatan 30, 363 45 Lammhult, Sweden	Michael.blom@steelform.se	+46 708 18 36 90
Elitfönster på plats AB 556391-7078	Mogölsvägen 6, 555 93 Jönköping, Sweden	martin.ternsjo@elitfonsterpaplats.se	+46725151659
RM Snickerier AB 556335-8679	Södra Industrigatan 8, 598 40 Vimmerby, Sweden	helene@rm.se	+46736232550
FastFrame (Europe) Ltd 5477831	Amber Drive, Bailey Brook Ind Estate, Langley Mill Nottingham, NG16 4BE, UK	swoodworth@dekkowindows.com	0161 406 0055
Victorian House Window Group Ltd 7259617	Victorian House, Capel Hendre Business Park, Capel Hendre, Ammanford, SA18 3FA, UK	Luci.Coles@vhwg.co.uk	07805 475344

Frovin Vinduer og Døre A/S 20 89 44 31	Rogalandsvej 3, 7900 Nykøbing Mors, Denmark	brian.frimor@inwido.dk	+4522100302
Bøjsø Døre & Vinduer A/S 12 22 44 94	Højagervej 5-7, 6623 Vorbasse, Denmark	Sarah.Nauer-Newstead@inwido.dk	+45 60820531
Hyvinkään Puuseppien Oy 0940027-0	Lukonmäentie 26, 05950 Hyvinkää, Finland	Marko.Kohvakka@pihla.fi	+358504015023
Sydänpuu Ikkunat Oy 2581890-9	Yrittäjäntie 8, 19650 JOUTSA, Finland	Marko.Kohvakka@pihla.fi	+358504015023
Carlson and Co Ltd 227444	G11 & G12 Calmount Park Ballymount, Dublin D12 F9P1, Ireland	Julie@carlson.ie	01-9121307
Sokolka Okna i Drzwi SA 82682	Lotników Lewoniewskich 1, 16-100 Sokółka, Poland	Marek.Anisko@sokolka.com.pl	+48 691 990 213

Contact details to appointed public authorities for external reporting.

Country	*Contact details*
Sweden	A list of the appointed public authorities and their respective areas of responsibility is included in the appendix to the Ordinance on Protection of Persons who Report Breaches (2021:949), which is available online and this information can also be found here.