

WHISTLEBLOWER POLICY

1. Purpose

This Whistleblowing Policy has been published to supplement Ingram Micro's global Sunshine Rule, Non-Retaliation Policy and Hotline Reporting Policy in order to meet local Australian whistleblowing laws (including the *Corporations Act 2001* and the *Taxation Administration Act 1953*).

We are committed to the highest standards of legal and ethical conduct. This policy is designed to help you report concerns you have about illegal, unethical or improper conduct you encounter at work. Rather than allowing these problems to stay hidden, we encourage you to bring these issues into the light of day.

2. Who does this policy applies to?

This is a policy of Ingram Micro Pty Ltd ("Ingram Micro"). It applies to all current and former directors, officer, associates and contractors of Ingram Micro along with its suppliers (including their employees). It also protects disclosures made by a relative, dependence or spouse of these individuals.

3. What is Reportable Conduct?

You can make a disclosure under this policy if you have reasonable grounds to believe that you have information about illegal, unethical or improper conduct by someone connected with Ingram Micro, or an improper state of affairs in relation to Ingram Micro (including about Ingram Micro's tax affairs) (**Reportable Conduct**).

Reportable Conduct may include the following type of conduct:

- Collusion, fraud or theft (e.g. falsifying credit applications, misappropriating funds);
- corrupt behaviour (e.g. accepting or offering a bribe, money-laundering);
- serious criminal offences (eg assault, theft, forgery);
- a serious or material breach of internal policy, including the Ingram Micro Code of Conduct
- potential breaches of human rights standards;
- a misuse of sensitive or confidential customer information;
- unsafe work practices or an environmental hazard;
- Price fixing and financial misreporting;
- indicates a significant risk to public safety or the stability of (or confidence in) the financial system;
- attempts to conceal any of the above.

The disclosure of a Reportable Conduct is known as a "protected disclosure" and qualifies for protection under the relevant Legislation (**Protected Disclosure**).



We strongly encourage individuals to disclose the wrongdoing where a person has reasonable grounds to suspect misconduct, or an improper state of affairs or circumstances, in relation to Ingram Micro or a related body. We will not tolerate retaliation for reporting made by an eligible whistleblower where there are reasonable grounds to suspect such matters.

4. What types of concerns are not Reportable Conduct?

Personal work-related grievances are generally not classified as Reportable Conduct. These are concerns relating to your employment (e.g. remuneration, performance reviews, transfers, promotions or disciplinary action) or grievances relating to an interpersonal conflict between you and another employee or manager. These issues can be reported to HR or managed in accordance with our [Grievance Procedure](#).

Your personal work-related grievance may still be Reportable Conduct if:

- it relates to treatment you face because you have made a protected disclosure;
- the grievance relates to a breach of employment (or other) laws punishable by imprisonment for a period of 12 months or more, or conduct representing a danger to the public or the financial system; or
- it includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance (mixed report).

Customer complaints are another type of concern that are generally not classified as Reportable Conduct unless there is misconduct or an improper state of affairs.

You must have reasonable grounds to suspect the misconduct, improper state of affairs or circumstances that constitute the relevant Reportable Conduct in order for it to be a Protected Disclosure. If a whistleblower is found to have intentionally made a false or vexatious report, they may be subject to disciplinary or legal action.

5. Who can I make a disclosure to?

Independent hotline: We have also set up a confidential independent hotline for whistleblowers (EthicsPoint) which you can use to make disclosures anonymously:

- [Webform](#),
- By phone 1 800 551 155 (Optus) or 1 800 881 011 (Telstra)
 (AT the prompt dial **(877) INGRAM2 (464-7262)**).

Ingram Micro contact: You can make disclosures to:

- a director or senior manager of Ingram Micro or a related body corporate. An Ingram Micro senior manager is a person who makes or participates in decisions that substantially affect the business including members of the Executive Leadership Team, APAC Head of Compliance and general managers;
- internal or external auditor (including a member of an audit team conducting an audit) of Ingram Micro.

Regulators: By law, you may also receive protection if you chose to raise disclosable matter with regulators including:

- ASIC – please see [How ASIC handles whistleblower reports | ASIC](#)
- ATO – please see [Tax whistleblowers | Australian Taxation Office \(ato.gov.au\)](#)
- another prescribed Commonwealth regulatory authority.

Public interest disclosure and emergency disclosures: Disclosures can be made to a journalist or parliamentarian under certain circumstances and qualify for protection (see the criteria in [Attachment A](#)).

Independent Legal Advice: Before you decide whether to make a disclosure, you can seek advice from a lawyer and the disclosure and advice will be protected by legal professional privilege. You should contract an independent legal adviser before making a public interest disclosure or an emergency disclosure.

6. Confidentiality and anonymous disclosures

Protected Disclosures can be made anonymously and still be protected under the relevant legislation. A whistleblower can choose to remain anonymous while making a Protected Disclosure, over the course of the investigation and after the investigation is finalised. The whistleblower can refuse to answer questions that they feel could reveal their identity at any time, including during follow-up conversations. We encourage whistleblowers who wish to remain anonymous to maintain ongoing two way communication with us so we can ask follow-up questions or provide feedback. It may not be possible to investigate a matter thoroughly if there are insufficient details and questions cannot be followed up.

We will not identify a whistleblower, or disclose information that is likely to lead to the identification of the whistleblower, outside the following exceptions:

- a person can disclose the identity of the whistleblower to: (a) to ASIC, APRA, or a member of the Australian Federal Police; (b) to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Corporations Act); (c) to a person or body prescribed by law; or (d) with the consent of the whistleblower.
- a person can disclose the information contained in a Protected Disclosure with or without the whistleblower's consent if: (a) the information does not include their identity; (b) we has taken all reasonable steps to reduce the risk that the whistleblower will be identified from the information; and (c) it is reasonably necessary for investigating the issues raised in the Protected Disclosure.

The reasonable steps we will take to protect your identity and information in your Reportable Disclosure that is likely to identify you, may include:

- securely storing all paper and electronic documents and other materials relating to the Protected Disclosure;
- where possible, communicating with you to help identify the aspects of your concerns that could inadvertently identify you;
- potentially using a pseudonym or gender neutral terminology to refer to you; and



- reminding those involved in receiving, handling and investigating Protected Disclosures about the confidentiality requirements and consequences of breaching confidentiality to those.

Despite the above measures, it may be difficult to protect your identity if;

- you have mentioned to another person that you are considering making a disclosure
- you are one of a small number of people with access to the disclosed information.
- the disclosure relates to information that you have previously been told privately and in confidence.

If you believe that anyone in Ingram Micro has breached confidentiality in relation to a disclosure, you can lodge a complaint to the Manager of Legal ANZ or to a regulator such as ASIC or the ATO.

7. Protections from detrimental acts or omissions

We are committed to supporting and protecting people who make Protected Disclosures under this policy and has adopted a Non-Retaliation Policy in relation to any employee that discloses Reportable Conduct. This means that you will not be subject to retaliatory or disciplinary action or other adverse employment consequences (Detrimental Conduct) because someone believe that you have (or suspects you may have) made a Protected Disclosure within the scope of this policy or under applicable legislation.

You may also be protected under the relevant legislation from any of the following in relation to a Protected Disclosure:

- (a) civil liability (e.g. any legal action for breach of an employment contract, duty of confidentiality or another contractual obligation);
- (b) criminal liability (e.g. prosecution for unlawfully releasing information, or other use of the disclosure in a prosecution (other than for making a false disclosure); and
- (c) administrative liability (e.g. disciplinary action for making the disclosure).

Further under legislation, you can seek compensation and other remedies through the courts if:

- (a) you suffer loss, damage or injury because of a disclosure; and
- (b) we have failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

The protections under the relevant legislation do not grant immunity for any misconduct by you that is revealed in your disclosure. Not all conduct will amount to Detrimental Conduct, such as managing poor work performance in line with our performance management procedures, disciplinary action in response to misconduct by you, where you intentionally make a Whistleblower Report that you know isn't true or is misleading, or action that is reasonable to protect you from Detrimental Conduct.

If you believe you have been subjected to or threatened with Detrimental Conduct you should contact the APAC Director of Compliance who will review the allegation.



8. Support

Dealing with concerns about misconduct in the workplace can be difficult and stressful. You should feel free to call Ingram Micro's [Employee Assistance Program](#), which is a confidential counselling service to assist when work-related concerns are impacting your health or wellbeing. Ingram Micro will not be informed that you have contacted the service nor receive any information about the discussion you have.

9. Handling and investigating a disclosure

When a disclosure has been reported, the disclosure will be allocated to an independent Case Manager who will initially determine whether the disclosure needs to be investigated based on the criteria set out in this Whistleblowing Policy.

The Case Manager will carry out their investigation keeping in mind the obligation to maintain confidentiality and protecting you from retaliation in accordance with our [Non-retaliation Policy](#). The investigation will be conducted under the supervision of the Compliance Department. The investigation will consist of: 1) a review of the facts and any documents you communicated to us; 2) the collection of records and data, including interviews of the people who are aware of the issue and/or implicated in the disclosure; 3) the preparation of a report for the Ingram Micro Audit Committee that includes findings, conclusions and remediation/improvements, where appropriate.

The Case Manager will update you on the progress of the investigation (if you can be contacted). The length of the investigation will depend on the nature of disclosure. It may not be appropriate to provide you with specific details of the investigation or the measures that we have taken.

An associate who is alleged to have been involved in misconduct will be advised about the subject matter of a disclosure as and when required by principles of natural justice and procedural fairness and prior to any actions being taken.

10. Policy compliance

Breach of this policy may be regarded as misconduct, which may lead to disciplinary action (including termination of employment or engagement). An individual may also be exposed to criminal or civil liability for a breach of relevant legislation.

11. How this policy is made available

This policy is made available to Ingram Micro officers and associates on the [Ingram Micro intranet](#) and to the public via the [Ingram Micro web page](#).

Revision Table

Review Date	Version	Description of Revision	Version Revision By	Approved By
	1.0	New Policy implemented		Legal/HR/Compliance

Attachment A: Public Interest Disclosure and Emergency Disclosures

Public Interest Disclosure is the Disclosure of information to a journalist or a parliamentarian, where:

- (a) at least 90 days have passed since the Discloser made the Disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;
- (b) the Discloser has reasonable grounds to believe that no substantive action is being, or has been taken, in relation to their Disclosure;
- (c) the Discloser has reasonable grounds to believe that making a further Disclosure of the information is in the public interest; and
- (d) before making the public interest Disclosure, the Discloser has given written notice to the body referred to in paragraph (a) above (i.e. the body to which the previous Disclosure was made) that:
 - A. includes sufficient information to identify the previous Disclosure; and
 - B. states that the Discloser intends to make a public interest Disclosure.

Emergency Disclosure is the Disclosure of information to a journalist or parliamentarian, where:

- (a) the Discloser has previously made a Disclosure of the information to ASIC, APRA or another Commonwealth body prescribed by regulation;
- (b) the Discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;
- (c) before making the emergency Disclosure, the Discloser has given written notice to the body referred to in paragraph (a) above (i.e. the body to which the previous Disclosure was made) that:
 - A. includes sufficient information to identify the previous Disclosure; and
 - B. states that the Discloser intends to make an emergency Disclosure; and
- (d) the extent of the information disclosed in the emergency Disclosure is no greater than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

Key definitions

“discloser” means an individual who is, or has been, any of the following in relation to any member of the Group: (a) an officer, Contractor or Employee; (b) a supplier of services or goods to a member of the Group (whether paid or unpaid), including their employees; (c) an 'associate' of a member of the Group (as that term is defined in the Corporations Act 2001 (Cth)); (d) a relative, dependant or spouse of an individual referred to in (a) – (c) above, and includes current and former employees of any member of the Group including those who are permanent, part-time, fixed term or temporary, interns, secondees, managers, directors, current and former contractors, consultants, service providers and suppliers.

“disclosure” means a disclosure of information relating to, or allegedly relating to, a disclosable matter.

“disclosable matter” means Information to which the whistleblower protections apply (see RG 270.50–RG 270.57 and s1317AA of the Corporations Act.)