

1. SCOPE

This Whistleblowing Policy (“**Policy**”) relates to Supply Network Limited (“**Supply Network**”) and its related bodies corporate (together “**Supply Network**”, “**we**”, “**our**” and “**us**”).

This Policy forms part of Supply Network’s risk management and corporate governance framework and has been approved by the Supply Network Board of Directors.

Supply Network is committed to ensuring employees (and non-employees) can report issues in an environment free from victimisation. This Policy is designed to ensure that wrongdoing is uncovered and to give individuals the confidence to speak up.

We are committed to identifying and addressing wrongdoing as early as possible and protecting and supporting the dignity, wellbeing, career and good name of anyone with reasonable cause for reporting an issue.

2. PURPOSE OF THIS POLICY

The purpose of this Policy is to:

- support individuals to make eligible disclosures about wrongdoing safely, securely and with confidence they will be protected;
- ensure disclosures are dealt with appropriately and on a timely basis;
- provide transparency around Supply Network’s framework for receiving, handling and investigating disclosures;
- ensure Supply Network’s officers and key management personnel understand their obligations when they receive a report from a whistleblower;
- ensure thorough, objective, fair and independent investigation of disclosures;
- outline how this Policy is to be made available to officers and employees of Supply Network; and
- comply with the Corporations Act 2001 (Cth), *Taxation Administration Act 1953* (Cth), ASIC Regulatory Guide 270 (“**RG 270**”) and ASX Corporate Governance Principles and Recommendations.

3. TO WHOM THIS POLICY APPLIES: “ELIGIBLE WHISTLEBLOWERS”

The Corporations Act 2001 (Cth) (“**the Act**”) gives certain people legal rights and protections as whistleblowers.

To be eligible for protection under the Act, an “**eligible whistleblower**” is an individual who is (or has been) any of the following in relation to Supply Network:

- an officer (a director or company secretary);
- an employee (including, but not limited to, employees who are permanent, part-time, fixed term or temporary);
- a supplier of services or goods to Supply Network (whether paid or unpaid), including their employees (this includes current and former contractors and consultants);
- an associate of Supply Network; and

- a relative or dependant of one of the individuals referred to above or a dependant or spouse of one of those individuals.

To qualify for protection, an 'eligible whistleblower' must make the disclosure directly to:

- a director or company secretary of Supply Network, any other Key Management Personnel (as defined in Supply Network's most recent Annual Report), the Human Resources Manager of Supply Network or any other person authorised under this Policy to receive a disclosure;
- Supply Network's external auditor, or member of the audit team;
- the Australian Securities & Investments Commission ("ASIC"), the Australian Prudential Regulation Authority ("APRA") or another Commonwealth body prescribed by regulation; or a lawyer (for the purposes of obtaining legal advice relating to whistleblower provisions in the Act).

An 'Emergency disclosure' or 'public interest disclosure' also qualify for protection (further information is detailed in Attachment A).

While disclosures must be made to one of the above people or organisations, concerns can be raised anonymously and still be eligible for protection.

Tax whistleblower regime

Protections also apply in the tax whistleblower regime i.e. to individuals who disclose information to the Australian Taxation Office on tax avoidance behaviour and other tax issues. Further information on this regime is available from <https://www.ato.gov.au/general/gen/whistleblowers/>

4. MATTERS THAT CAN BE REPORTED: "DISCLOSABLE MATTERS"

Set out below are the types of wrongdoing that can be reported under this Policy. These are referred to as "disclosable matters".

Disclosable matters involve information that the discloser has **reasonable grounds**¹ to suspect:

- concerns **misconduct**²;
- concerns an **improper state of affairs or circumstances**³, or

¹ 'Reasonable grounds' means that a reasonable person in the same position would also suspect the information indicates misconduct, improper state of affairs or circumstances or a breach of the law. This means that even if a disclosure turns out to be incorrect, the protections will still apply, provided the eligible whistleblower had 'reasonable grounds' to suspect.

² 'Misconduct' is defined in s9 of the Act to include 'fraud, negligence, default, breach of trust and breach of duty'.

³ The phrase 'improper state of affairs or circumstances' is not defined and is intentionally broad. Internal matters, including breaches of policy, could constitute an improper state of affairs or circumstances if those breaches are systemic and relate to matters of interest to a particular regulator such as ASIC.

- Supply Network or any of their officers or employees has engaged in conduct that constitutes an offence against, or a contravention of, the Act or other specified financial services legislation or an offence against any other law of the Commonwealth punishable by imprisonment for 12 months or more or conduct that represents a danger to the public or the financial system.

The misconduct or an improper state of affairs may also be in respect of tax affairs.

The information can be about Supply Network, a related body corporate of Supply Network (including any subsidiary) or an officer or employee of Supply Network.

Examples of disclosable matters are:

- illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;
- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities;
- failure to comply with, or breach of, legal or regulatory requirements; and
- engaging in or threatening to engage in detrimental conduct against a person who has made a disclosure or is believed or suspected to have made or be planning to make a disclosure.

Disclosable matters also include conduct that may not involve a contravention of a particular law. For example:

- ‘misconduct or an improper state of affairs or circumstances’ may indicate a systemic issue that ASIC should know about to perform its functions properly;
- dishonest or unethical behaviour and practices or conduct that may cause harm, or conduct which is contrary to the Supply Network’s Directors Code of Conduct; and
- information that indicates a significant risk to public safety or the stability of, or confidence in, the financial system.

Deliberate false reports

You should not make false or vexatious reports where you know your report to be untrue. Individuals who submit a deliberate false report will not have access to the whistleblower protections under the Act. If any investigation of a disclosure demonstrates that it was not made on objectively reasonable grounds, this disclosure will not be protected.

Depending on the circumstances, it may be appropriate for Supply Network to take disciplinary action against a person who does not have objectively reasonable grounds for their disclosure. Such action may include termination of employment.

Supply Network encourages reporting where you reasonably suspect misconduct, even if those suspicions are later determined to be unfounded. As detailed in Regulation 270 of the Act, a discloser can still qualify for protection even if their disclosure turns out to be incorrect.

Matters that are not “disclosable matters”

Disclosures that are not about “disclosable matters” do not qualify for protection under the Act (or the *Taxation Administration Act 1953* (Cth) where relevant) and are not covered by this Policy.

For example, disclosures that relate solely to personal work-related grievances (i.e. grievances about matters relating to the eligible whistleblower's employment or former employment, having (or tending to have) implications for the eligible whistleblower personally), and that do not relate to detriment or a threat of detriment to the discloser, do not qualify for protection.

Examples are:

- interpersonal conflict between you and another employee; and
- decisions that do not involve a breach of workplace laws:
 - about your engagement, transfer or promotion;
 - about the terms and conditions of your engagement; or
 - to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

Importantly though, some personal work-related grievances still qualify for protection if:

- the grievance includes information about misconduct or an improper state of affairs, or information about such matters includes or is accompanied by a personal work-related grievance (mixed report);
- Supply Network has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public, or the disclosure relates to information that suggests misconduct beyond the discloser's personal circumstances;
- the discloser suffers from or is threatened with detriment for making a disclosure (see section 8 below); or
- the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Act.

Personal work-related grievances and other types of issues or concerns that are not covered by this Policy should be referred to the Human Resources Manager or relevant Manager, consistent with the Supply Network's Employment Policies and Procedures. In some cases, such grievances may be protected under other legislation, such as the Fair Work Act 2009 (Cth).

5. WHO CAN PROVIDE ADVICE OR RECEIVE A DISCLOSURE

In order to qualify for protection as a whistleblower under the Act, a disclosure must be made directly to:

- ‘eligible recipients’;
- legal practitioners;
- authorised regulatory bodies and other external parties (see Section 3);

and in certain circumstances:

- journalists; and
- members of Commonwealth, State or Territory parliaments (“**parliamentarians**”) (see Attachment A).

A discloser qualifies for protection from the time they make their disclosure, regardless of whether the person or the recipient recognises that the disclosure qualifies for protection at that time.

Eligible recipients

The role of eligible recipients is to receive disclosures that qualify for protection. At Supply Network, eligible recipients are:

- an officer of Supply Network (being any Director or the Company Secretary of Supply Network), any other Key Management Personnel (as defined in Supply Network’s most recent Annual Report) and the Human Resources Manager of Supply Network; and
- the external auditor (HLB Mann Judd (NSW Partnership)), including a member of the audit team.

Disclosures outside of Supply Network

We encourage you to make disclosures internally in the first instance.

A disclosure can, however, be made directly to regulatory bodies (e.g. ASIC), or other external parties such as lawyers (for the purpose of obtaining legal advice or legal representation in relation to the Act), about a disclosable matter and still qualify for protection under the Act without a prior disclosure being made to us.

Whistleblowing information is provided by ASIC in Information Sheet 239 How ASIC handles whistleblower reports (INFO 239):

<https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/how-asic-handles-whistleblower-reports/>

Public interest disclosures and emergency disclosures

Disclosures can be made to a journalist or parliamentarian under certain circumstances and qualify for protection. These circumstances are detailed in Attachment A.

6. ROLES AND RESPONSIBILITIES

Board of Supply Network

The Board of Supply Network is responsible for the ongoing oversight and monitoring of and approving updates to this Policy and related processes and procedures.

Whistleblower Protection Officer

The role of the Whistleblower Protection Officer is to:

- respond to queries about how Supply Network's Whistleblowing Policy works, what it covers and how a disclosure might be handled (including to disclosers who wish to seek additional information before formally making their disclosure); and
- protect disclosers and potential disclosers and ensure the integrity of the reporting mechanism.

An eligible recipient should notify the Whistleblower Protection Officer (subject to the discloser's consent) so that Supply Network's mechanisms for protecting and safeguarding disclosers can commence as soon as possible.

Whistleblower Investigation Officer

The Whistleblower Protection Officer will, for each disclosure, appoint a Whistleblower Investigation Officer responsible for assessing whether the disclosure falls within this Policy and for investigating the disclosure.

Supply Network may engage external investigation officers or legal advisers to assist with investigating the disclosure.

7. HOW TO MAKE A DISCLOSURE

Disclosures can be made to any one of Supply Network's eligible recipients in person or by phone, post or email. Disclosures may be made anonymously, and/or confidentially, securely and outside of business hours. In the first instance, disclosures should be made to a Whistleblower Protection Officer:

Contact: Peter Gill
Email: petergill@supplynetwork.com.au
Tel: +61 2 8624 8077
Address: Supply Network Limited
1 Turnbull Close
Pemulwuy NSW 2145

A disclosure can instead be made to another eligible recipient within Supply Network, being any officer of the company (defined as any Director or the Company Secretary of Supply Network), any other Key Management Personnel (as defined in Supply Network's most recent Annual Report) or the Human Resources Manager of Supply Network.

A disclosure can also be made to Supply Network's auditor:

Contact: HLB Mann Judd (NSW Partnership)
Email: mailbox@hlbnsw.com.au
Tel: +61 2 9020 4000
Address: Level 19, 207 Kent Street
[Sydney NSW 2000]

The person disclosing any matter should inform the recipient that they wish to make a disclosure under this Policy.

Anonymous disclosures

Disclosures made anonymously are still protected under the Act.

Anonymous disclosures can be made securely and outside of business hours by, for example, leaving a voicemail or using an email address which does not disclose your identity. You may choose to adopt a pseudonym for the purposes of the disclosure, rather than your real name.

An individual can choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalised. A discloser can refuse to answer questions that could reveal their identity during follow-up conversations. However, reporting anonymously may hinder Supply Network's ability to investigate fully a disclosed matter. For this reason, ongoing two-way communication is encouraged (such as via an anonymous email address), so that follow-up questions can be asked and/or feedback provided.

8. LEGAL PROTECTIONS FOR DISCLOSERS

The protections available to a discloser who qualifies for protection as a whistleblower are:

- identity protection (confidentiality);
- protection from detrimental acts or omissions;
- compensation and remedies; and
- civil, criminal and administrative liability protection.

These protections apply not only to internal disclosures, but also to external disclosures to lawyers, regulatory and other external bodies, and public interest and emergency disclosures that are made in accordance with the Act.

Supply Network takes contraventions of these protections very seriously and will take disciplinary action against anyone for breaching these protections. If an eligible whistleblower has any concerns about this, they can raise them with Supply Network's Whistleblower Protection Officer (or a director of Supply Network).

Civil and criminal sanctions also apply for breaches of these protections.

Identity protection (confidentiality)

It is illegal to identify a discloser, or disclose information that is likely to lead to the identification of the discloser except, in very limited circumstances detailed below.

The identity of the discloser can be disclosed:

- to ASIC, APRA, the Commissioner of Taxation (in relation to tax matters) or a member of the Australian Federal Police;
- to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Act);
- another person or entity to which Supply Network is legally compelled to disclose (including a body prescribed by the Corporations Regulation); or
- with the consent of the discloser.

If an eligible whistleblower's disclosure qualifies for protection set out in this Policy, it is likely that the eligible whistleblower will be asked to provide consent to the disclosure of their identity or information that is likely to lead to their identification. This would be to facilitate any investigation and/or resolution of the matter. If consent is withheld, it may not be possible to adequately investigate and respond (if at all) to the disclosure.

However, the discloser's consent is not required if:

- the information does not include the discloser's identity;
- Supply Network has taken all reasonable steps to reduce the risk that the discloser will be identified from the information; and
- it is reasonably necessary for investigating the issues raised in the disclosure.

ASIC, APRA or the Australian Federal Police can disclose the identity of the discloser, or information that is likely to lead to the identification of the discloser, to a Commonwealth, State or Territory authority to help the authority in the performance of its functions or duties.

Supply Network seeks to ensure confidentiality by:

- storing all paper and electronic documents and other materials relating to disclosures securely with access limited as reasonably possible to only those directly involved in managing and investigating the disclosure;
- ensuring communications and documents relating to the investigation of a disclosure are not sent to a group email address;
- ensuring that only the people who are directly involved in handling and investigating a disclosure are made aware of a discloser's identity or information that is likely to lead to the identification of the discloser; and
- reminding each person who is involved in handling and investigating a disclosure that they should keep the identity of the discloser and the disclosure confidential and that an unauthorised disclosure of a discloser's identity may be a criminal offence.

In practice, it is important to recognise that a whistleblower's identity may still be determined if the person has previously mentioned to other people that they are considering making a disclosure, the whistleblower is one of a very small number of people with access to the information or the disclosure related to information that an eligible whistleblower has previously been told privately and in confidence.

A discloser can lodge a complaint about a breach of confidentiality with:

- Supply Network's Whistleblower Protection Officer (or a Director of Supply Network); or
- a regulator e.g. ASIC.

Protection from detrimental acts or omissions

The Act makes it illegal (through a criminal offence and civil penalty) for someone to cause or threaten detriment to a person because they believe (or suspect) that the other person or third party has made, may have made, or could make a whistleblower disclosure, no matter if it is accurate. Threats of detriments will be unlawful if the person making the threat intended to cause fear that a detriment would be carried out or was reckless as to whether the person against who it was directed would fear the threatened detriment being carried out. Threats may be express or implied, conditional or unconditional. An eligible whistleblower (or another person) who has been threatened in relation to a disclosure does not have to actually fear that the threat will be carried out.

Detrimental conduct includes:

- dismissal of an employee;
- alteration of an employee's position or duties to their disadvantage;
- discriminating between an employee and other employees;
- harassment or intimidation of a person;
- harm or injury to a person, including psychological harm;
- damage to a person's property;
- damage to a person's reputation, business or financial position; or
- any other damage to a person.

The following actions are **NOT** detrimental conduct:

- administrative action that is reasonable to protect a discloser from detriment (e.g. when the disclosure relates to wrongdoing in the discloser's immediate work area); or
- managing a discloser's unsatisfactory work performance, if the action is in line with Supply Network's performance management framework.

Compensation and remedies

A discloser (or any other employee or person) can seek compensation and other remedies through the courts if they are subject to detriment or threatened detriment. These include injunctions, compensation orders (including against individual employees and their employer), reinstatement, exemplary damages

and the making of apologies. Civil and criminal sanctions also apply to breaches of the Whistleblower Protection Scheme. We encourage a discloser to seek independent legal advice to understand protections or rights to compensation that may apply.

Civil, criminal and administrative liability protection

The Act protects a discloser against certain legal actions including:

- criminal prosecution (e.g. attempted prosecution of the discloser for unlawfully releasing information. The disclosure cannot be used against the whistleblower in a prosecution, unless the disclosure is false);
- civil litigation (e.g. legal action against the discloser for breach of an employment contract, duty of confidentiality, or other contractual obligation), or
- administrative action (including disciplinary action for making the disclosure).

This protection does not grant immunity to a whistleblower for any misconduct that they were involved in that is revealed in the disclosure.

9. SUPPORT AND PRACTICAL PROTECTION FOR DISCLOSERS

Supply Network has appointed a Whistleblower Protection Officer who is committed to protecting the confidentiality and welfare of a discloser and who will be available to contact at any time. On receiving a disclosure, the Whistleblower Protection Officer will, as soon as practicable, assess and monitor the risk of detriment to the discloser and develop strategies to deal with any such risk and take appropriate steps to manage confidentiality and support an investigation.

Support offered to a discloser by Supply Network may also include:

- an independent support person appointed by the Whistleblower Protection Officer to support the discloser; and/or
- referring the discloser to external independent support providers.

In the situation where a discloser believes they have suffered detriment, a complaint can be lodged with any other eligible recipient (a person not involved in dealing with disclosures) and investigation findings will be provided to the Board of Supply Network.

Where detriment is present, Supply Network will consider the following courses of action:

- allowing the discloser to take extended leave or perform duties from another location (if practicable); or
- offering an alternative career development plan for the discloser, including new training and career opportunities.

Alternatively, a discloser may seek independent legal advice or contact regulatory bodies, such as ASIC, if they believe they have suffered detriment.

10. HANDLING AND INVESTIGATING A DISCLOSURE

Receipt of disclosure

On receipt of a disclosure, subject to the consent of the whistleblower, the eligible recipient must inform the Whistleblower Protection Officer as soon as practicable (subject to applicable confidentiality requirements) who will appoint an appropriate Whistleblower Investigation Officer.

If a disclosure relates to serious misconduct, the Supply Network Board shall be notified immediately.

If a disclosure relates to the eligible recipient, such disclosure should be immediately directed to an alternative eligible recipient.

The Whistleblower Investigation Officer will acknowledge receipt of the disclosure (if the discloser can be contacted).

Investigation

The Whistleblower Investigation Officer will assess:

- whether the disclosure falls under this Policy; and
- if a formal, in-depth investigation is required, each disclosure will be considered on a case by case basis and will consider:
 - the nature and scope of the investigation;
 - the person(s) within and/or outside Supply Network that should lead the investigation. Any investigation will be independent of the discloser, the individuals who are the subject of the disclosure, and the department involved;
 - the nature of any technical, financial or legal advice that may be required to support the investigation; and
 - the timeframe for the investigation. Each investigation will be different, which will impact the applicable timeframe. However, our intent is to complete an investigation as soon as practicable.

Maintaining confidentiality

The Whistleblower Investigation Officer and Whistleblower Protection Officer will take steps to protect the confidentiality of the investigation process by, for example:

- reminding the eligible recipient/s of the disclosure of the requirement to maintain confidentiality; and
- maintaining all electronic records in a private, confidential folder or drive.

Without the discloser's consent, information contained in a disclosure will not be disclosed to any other party (including to another Supply Network employee or Director) as part of Supply Network's investigation process unless:

- the information does not include the discloser's identity;

- information relating to the discloser's identity or other information that is likely to lead to the identification of the discloser is removed (e.g. the discloser's name, position title and other identifying details);
- it is reasonably necessary for investigating the issues raised in the disclosure; and
- it is to one of the parties listed in section 8 of this Policy.

Keeping the discloser informed

After the initial acknowledgement, the Whistleblower Investigation Officer will keep the discloser informed of the progress and outcome of the investigation, wherever possible. However, the extent of the information provided, the frequency and timeframe of any updates, or whether it will be provided at all, will be subject to applicable confidentiality considerations, legal obligations and any other factors Supply Network considers relevant in the particular situation. This process will also be limited in the case of an anonymous disclosure with no means of contacting the discloser.

Our preferred communication method is via email.

Reporting findings

The results of the investigation will be reported to the Board of Supply Network (having regard to relevant confidentiality requirements) together with a summary of the matter and the actions taken to date. The method for documenting and reporting the findings of an investigation will depend on the nature of the disclosure – but may include a summary report of the findings.

Where appropriate, the discloser will be notified of the outcome of the review (but not be provided with a copy of the investigation report).

A flowchart of Supply Network's typical whistleblowing process is shown in Attachment B.

11. ENSURING FAIR TREATMENT

Supply Network is committed to fair treatment of its employees who are mentioned in a disclosure, including those who are the subject of a disclosure.

In all cases:

- disclosures will be handled confidentially, when it is practical and appropriate in the circumstances;
- each disclosure will be assessed and may be the subject of an investigation;
- the objective of an investigation is to determine whether there is enough evidence to substantiate or refute the matters reported; and
- an employee who is the subject of a disclosure will be advised about:
 - the subject matter of the disclosure as and when required by principles of natural justice and procedural fairness, and prior to any actions being taken - for example, if the disclosure is to be the subject of an investigation or if the disclosure is serious and needs to be referred to ASIC, APRA or the Federal Police; and

- where appropriate, the outcome of the investigation (but not be provided with a copy of the investigation report).

12. ACCESSIBILITY OF THIS POLICY

A copy of this Policy is made available to all officers and employees of Supply Network on the Supply Network website. An electronic communication has been sent to all officers and employees of Supply Network to alert them to the implementation of the Policy from 1 January 2020 and a Policy Summary is included in the Induction Pack for all new employees.

Supply Network's internal eligible recipients, who include the Whistleblower Protection Officer, understand and have received training on the requirements of this Policy and Regulation 270.

A full copy of this Policy is provided in the Governance section of Supply Network's website allowing disclosers outside of Supply Network to access our Policy.

13. REVIEW AND UPDATE

This Policy will be reviewed by the Board of Supply Network (at least every 2 years) to check that it is operating effectively and consider whether any changes are required.

14. OTHER MATTERS

This Policy is not intended to go beyond the legislation. This Policy is not a term of any contract, including any contract of employment and does not impose any contractual duties, implied or otherwise, on Supply Network. This Policy may be varied by Supply Network from time to time, including as part of any review.

ATTACHMENT A - PUBLIC INTEREST AND EMERGENCY DISCLOSURES

A **'public interest disclosure'** is a disclosure of information to a journalist or a parliamentarian, where:

- at least 90 days have passed since the discloser made the disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;
- the discloser does not have reasonable grounds to believe that action is being or has been taken in relation to their disclosure;
- the discloser has reasonable grounds to believe that making a further disclosure of the information is in the public interest;
- before making the public interest disclosure, the discloser has given written notice to the body to which the previous disclosure was made that:
 - includes sufficient information to identify the previous disclosure; and
 - states that the discloser intends to make a public interest disclosure; and
- the extent of the information disclosed in the public interest disclosure is no greater than to inform the journalist or parliamentarian of the misconduct or improper state of affairs or circumstances, or other conduct falling within the scope of the whistleblower protection scheme under the Act.

An **'emergency disclosure'** is the disclosure of information to a journalist or parliamentarian, where:

- the discloser has previously made a disclosure of the information to ASIC, APRA or another Commonwealth body prescribed by regulation;
- 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;
- before making the emergency disclosure, the discloser has given written notice to the body to which the previous disclosure was made that:
 - includes sufficient information to identify the previous disclosure; and
 - states that the discloser intends to make an emergency disclosure; and
- 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.

You may wish to contact an independent legal adviser to ensure you are aware of the criteria for making a public interest or emergency disclosure that qualifies for protection.

ATTACHMENT B – FLOWCHART OF SUPPLY NETWORK’S TYPICAL WHISTLEBLOWING PROCESS

