



HiTech Group Australia Limited

Whistleblowing Policy



Our Purpose

Our Goals & Commitment

The purpose of this document is to demonstrate HiTech Group's ('HiTech') commitment to ethical and professional standards in all that we do and be accountable for our conduct.

Together with our values, we want to have feedback and encourage people to speak up when they see activity or behaviour that they feel is wrong or does not match our values. The goal of this policy is to provide very clear guidelines on how we approach and manage this feedback. With our whistleblowing policy, we aim to ensure:

- Every employee will have the chance to speak up anonymously when they feel employees of HiTech are not adhering to our corporate values. They should have a place to report misconduct and every report will be heard and acted on. In turn, we will make improvements based on the results of investigations.
- The HiTech Group believes everyone should be able to make reports anonymously should they wish. We commit to protecting informant's identities and they only need to reveal themselves if they choose to.
- We will investigate every report of misconduct. At the end of the investigation, we will document the results and provide feedback when appropriate.

What Conduct Should Be Reported

We want to hear from you if you witness or know about any behaviour that is:

- Fraudulent.
- Illegal.
- Corrupt.
- Unethical.
- Violates the law or any legal code.
- Is creating an unsafe environment.
- Breaches any of our company's policies.
- Discrimination.
- Harassment and/or bullying of any kind.
- Any conduct which is detrimental to HiTech and could cause financial or non-financial loss.

Process for Making a Report

If an employee or eligible person would like to make a report, they have different channels available where they can do this:

- Speak with a senior manager at HiTech.
- Whistleblowing/Anonymous Reporting via email to secretary@hitechaust.com.
- Phone +612 9241 1919.
- Via post to PO BOX R182, Royal Exchange NSW 1225.



It is important for HiTech to be transparent with our employees and outline what is the process for us to investigate a report submitted through our whistleblowing channels. Below, we have provided the different steps a case manager or member of our whistleblowing team will go through once a report is received until the case is closed.

- Report (anonymous or otherwise) is received and logged with the HiTech Board.
- A case manager is assigned to the report to assess it and confirm its receipt.
- The case manager will do an initial assessment to confirm it is a valid report and request permission to investigate.
- The case manager will begin their investigation. This can include corresponding with the informant if there is a channel to do this.
- The case manager will investigate and update management and the informant per policy guidelines.
- Once the case manager has finalised their investigation and report, senior management and the informant will be updated.

Any information that could potentially identify an anonymous informant will be held in the strictest confidence and will not be shared, unless HiTech is compelled by law.

The Informant and the relevant protection

HiTech will strive to provide relevant stakeholders as much feedback on the investigation as possible. However, due to HiTech's privacy guidelines, information that cannot be shared with the informant will be suppressed.

As part of our investigative process, HiTech will update the informant of the progress of the investigation. These updates can include the following:

- HiTech has confirmed the receipt of a report from the informant.
- HiTech has commenced the investigative process.
- The investigation is currently ongoing.
- The investigation has been closed.

After submitting a report, the following policies around anonymity are in place to protect an informant's identity:

- The informant has the right to remain anonymous and does not need to identify themselves at anytime during the investigation process.
- HiTech uses tools and platforms that help protect an informant's identity during and after submitting a report.
- The informant can refuse to answer questions they feel could identify themselves. If the informant reveals themselves at any time, you will document who will have access to their identity. This can include the case manager, whistleblowing program owner.

Potential Retaliation

An informant may be concerned that staff, management, or the organisation might retaliate against them. In this case, HiTech will protect the informant from:

- Being terminated or having their employment ceased.
- Harassment on the job or workplace bullying.
- Warnings or disciplinary actions.
- Discrimination.



- Any other action that can be perceived as retaliation for making a report.

Considered Risk of Retaliation

In cases of considered retaliation, the informant should contact their immediate manager or the GM or CEO of HiTech. Relevant action will follow thereafter so that the informant feels protected as well as come up with recommendations for how the situation can be resolved. Potential steps to protect the informant from a considered risk of retaliation can include:

- The informant taking leave.
- The informant being reassigned to other duties.
- The informant being reassigned to another location.

Protection & Immunity for Others

Other parties that might have to bear witness or are involved in the investigation will be protected from retaliation in the same manner as the informant.

Legislative/Regulation Protection & Assistance

If in any jurisdictions or locales where HiTech operates has whistleblowing protection laws that provide a higher level of protection than what is included in this policy, the local legislation will take precedence.