NEXSYS

POLICY

Reporting Misconduct and Non-Retaliation Policy

2026

NEXSYS

Contents

1. Overview

NexSys IT Pty Ltd is committed to maintaining a workplace culture built on accountability, transparency, integrity and respect. Speaking up early helps identify misconduct, prevent harm, protect clients and workers, and maintain trust in the way NexSys IT conducts business.

This policy replaces the 2024 Reporting Misconduct / Non-Retaliation Policy and strengthens the framework for 2026 by clarifying reporting channels, non-retaliation protections, confidentiality requirements, investigation principles, external reporting pathways and governance responsibilities.

NexSys IT recognises that misconduct reports can involve sensitive personal, commercial, employment, legal and client information. Reports will be handled carefully, confidentially and fairly, with support for people who raise concerns in good faith.

2. Purpose and objectives

The objectives of this policy are to provide clear, accessible and trusted pathways for reporting suspected misconduct and to ensure all reports are assessed and addressed appropriately.

In practice, this means NexSys IT will:

- promote ethical conduct and early reporting of concerns;
- protect people who report concerns in good faith from retaliation or detriment;
- support confidentiality, privacy and procedural fairness;
- ensure reports are assessed, investigated and resolved consistently;
- comply with applicable Australian whistleblower, employment, workplace, privacy, safety and anti-discrimination laws;
- identify root causes and improve systems, controls, training and culture.

3. Scope and application

This policy applies to all NexSys IT directors, officers, employees, contractors, consultants, temporary workers, suppliers, vendors, service providers, business partners and other people who perform work for or interact with NexSys IT

It applies to conduct occurring in the workplace, remotely, online, at client sites, during work-related travel, at work functions and in any business context connected with NexSys IT operations, systems, clients or suppliers.

Where a law, client contract or regulator requirement imposes a higher standard than this policy, the higher standard must be followed.

4. Key legal framework

NexSys IT will comply with applicable obligations and will interpret this policy consistently with the following legal and regulatory frameworks where relevant.

Law / framework	Relevance to NexSys IT
Corporations Act 2001 (Cth) - whistleblower protections	Protects eligible whistleblowers who make qualifying disclosures about misconduct or an improper state of affairs or circumstances in relation to a company. Includes protections for confidentiality, identity, victimisation, detriment and compensation rights.
Taxation Administration Act 1953 (Cth) - tax whistleblower protections	Protects eligible disclosures about tax affairs and tax misconduct, including disclosures to eligible recipients and taxation authorities.
Fair Work Act 2009 (Cth)	Contains general protections, workplace rights and adverse action provisions relevant to workers who raise workplace concerns, complaints or enquiries.
Sex Discrimination Act 1984 (Cth) and positive duty	Requires businesses to take proactive and meaningful action to prevent and respond to sexual harassment, sex discrimination, sex-based harassment, hostile work environments and related victimisation.
Work health and safety legislation	Requires safe systems of work and supports reporting and management of psychosocial, physical, safety and conduct risks.
Privacy Act 1988 (Cth) and Australian Privacy Principles	Applies when collecting, using, storing or disclosing personal information during misconduct reports, investigations and record keeping.
Anti-discrimination, equal opportunity and human rights laws	Relevant to discrimination, harassment, bullying, victimisation, vilification and workplace conduct concerns.
Criminal, cyber, corporations, competition and consumer laws	Relevant where reported conduct may involve fraud, bribery, corruption, theft, cyber misuse, data misuse, cartel conduct, misleading conduct or other unlawful behaviour.

5. Definitions

Term	Meaning
Misconduct	Behaviour that may be illegal, unethical, unsafe, dishonest, fraudulent, corrupt, discriminatory, harassing, retaliatory, negligent, grossly improper, in breach of NexSys IT policy or otherwise inconsistent with NexSys IT standards.
Reportable conduct	Conduct that should be reported under this policy, including suspected legal breaches, fraud, corruption, workplace harassment, discrimination, retaliation, privacy breaches, safety risks, cyber or information security misuse, serious policy breaches and conduct that may harm clients, workers or NexSys IT
Whistleblower	A person who reports suspected misconduct and may qualify for legal protections depending on who they are, what they report, who they report to and whether the disclosure meets legal requirements.
Eligible recipient	A person or body authorised by law or NexSys IT to receive certain protected disclosures. This may include officers, senior managers, auditors, actuaries, authorised whistleblower contacts and relevant regulators, depending on the type of disclosure.
Retaliation / detriment	Any actual or threatened disadvantage because a person made, may make, proposes to make or is suspected of making a report. This includes dismissal, demotion, harassment, intimidation, discrimination, disciplinary action, damage to reputation, reduced duties, exclusion, threats or other adverse treatment.
Good faith report	A report made honestly and on reasonable grounds, even if the concern is not ultimately substantiated.
Personal work-related grievance	A grievance about an individual employment matter that has implications only for the person making the complaint, unless it also involves misconduct, breach of law, victimisation, systemic issues or significant risk to NexSys IT or others.

6. What should be reported

NexSys IT encourages prompt reporting of suspected misconduct. Reportable conduct may include:

- fraud, theft, bribery, corruption, money laundering, financial misconduct or misuse of company assets;
- dishonest, misleading, deceptive or unethical business practices;
- breaches of competition, consumer, corporations, tax, employment, safety, privacy, cyber security or other laws;
- discrimination, sexual harassment, bullying, victimisation, vilification or unsafe workplace behaviour;
- retaliation or threatened retaliation against someone for raising a concern;
- serious breaches of NexSys IT policies, procedures, client obligations or contractual requirements;
- misuse of confidential information, personal information, client systems, credentials, AI tools, data or intellectual property;
- cyber security incidents, unauthorised system access, data loss, compromised accounts or concealment of security incidents;
- modern slavery, unethical labour practices or serious supplier misconduct;
- conduct that creates a substantial risk to health, safety, the environment, clients, the public, NexSys IT or its reputation;
- deliberate concealment, destruction of evidence or interference with an investigation.

7. Matters generally outside this policy

Some matters may be more appropriately handled under other NexSys IT processes, such as performance management, employment grievances, leave disputes, payroll queries or interpersonal disagreements. These matters should generally be raised with a manager, People & Culture / HR contact or the appropriate internal contact.

However, a personal work-related grievance may still be handled under this policy where it involves legal breach, victimisation, retaliation, discrimination, harassment, systemic misconduct, unsafe conduct, significant risk, concealment or conduct that may qualify for whistleblower protection.

8. Who can make a report

Reports may be made by current or former directors, employees, contractors, consultants, suppliers, service providers, business partners, secondees, volunteers, associates and relatives or dependants of eligible whistleblowers where applicable under law.

NexSys IT will also consider reports from clients, prospective clients, regulators and other third parties where the concern relates to NexSys IT, its personnel, systems, suppliers or business conduct.

9. How to report misconduct

Reports can be made through multiple channels. A person may choose the channel they feel most comfortable using.

Channel	Use
Manager or supervisor	Raise the concern with a direct manager, senior manager or project lead where appropriate.
Nominated misconduct / whistleblower contact	Human Resources Manager
Email	hr@nexsysit.com.au
Phone	1300 733 010
External eligible recipient	Where applicable, reports may be made to eligible recipients such as auditors, legal practitioners or relevant regulators in accordance with legal requirements.
Emergency or immediate risk	Call emergency services or notify the appropriate safety, security or management contact immediately.

When making a report, include as much detail as possible, such as what happened, when and where it occurred, who was involved, any witnesses, supporting documents, systems or records, and whether there is any immediate risk.

10. Anonymous reporting

Reports may be made anonymously where permitted by law and practical for the circumstances. Anonymous reports will be assessed and investigated where sufficient information is available.

A person who reports anonymously may choose to maintain ongoing anonymous communication through a safe channel. Providing a way to ask follow-up questions can help NexSys IT assess and investigate the concern while preserving anonymity.

11. Confidentiality and information handling

NexSys IT recognises the sensitivity involved in reporting misconduct. Reports will be handled confidentially and information will only be shared with people who need to know for the purpose of assessment, investigation, support, legal advice, remediation, regulatory reporting or risk management. Where legal whistleblower confidentiality protections apply, NexSys IT will not disclose the whistleblower's

identity, or information likely to identify them, except where permitted by law. This may include disclosure with consent, disclosure to a legal practitioner for advice, disclosure to certain regulators, or disclosure where reasonably necessary to investigate the matter and reasonable steps are taken to reduce the risk of identification.

All personnel involved in receiving, assessing or investigating reports must preserve confidentiality, protect records, avoid unnecessary discussion and comply with privacy, employment, client and legal obligations.

12. Non-retaliation commitment

NexSys IT strictly prohibits retaliation against anyone who raises a concern in good faith, assists with a report, participates in an investigation or is suspected of doing so.

Retaliation may include dismissal, demotion, disciplinary action, threats, intimidation, harassment, exclusion, bullying, discrimination, reduced work opportunities, changes to duties, reputational damage, adverse performance treatment, damage to business relationships or any other disadvantage connected to a report.

Any employee, contractor, manager or business partner who retaliates, threatens retaliation, encourages retaliation or fails to address known retaliation may face disciplinary action, contract termination or other corrective action.

13. Whistleblower protections

Some reports may qualify for legal whistleblower protections under the Corporations Act 2001 (Cth), the Taxation Administration Act 1953 (Cth) or other laws. Whether legal protections apply depends on the reporter's relationship to NexSys IT, the subject matter of the disclosure and the person or body to whom the disclosure is made.

Where protections apply, a whistleblower may have rights to confidentiality, protection from detriment, immunity from certain civil, criminal or administrative liability for making the disclosure, and access to compensation or other remedies if they suffer loss, damage or injury because of detrimental conduct.

This policy is intended to support those legal protections but does not replace them. A person may seek independent legal advice about their rights and reporting options.

14. Roles and responsibilities

Role	Responsibility
Directors / senior leadership	Set expectations, allocate resources, monitor high-risk matters, ensure non-retaliation and approve major corrective actions.
Nominated misconduct / whistleblower contact	Receive and triage reports, coordinate confidentiality, assess protection needs, maintain records and escalate matters appropriately.
Managers	Create a speak-up culture, receive concerns respectfully, escalate promptly, prevent retaliation and preserve evidence.
Employees and contractors	Report suspected misconduct, cooperate honestly with investigations, maintain confidentiality and avoid retaliation.
Investigation lead	Plan and conduct fair, impartial and timely investigations, document findings and recommend corrective action.
Third-party providers	Comply with contractual, legal, confidentiality and reporting obligations when handling NexSys IT information or concerns.

15. Assessment, triage and investigation process

Reports will be assessed promptly to determine the nature of the concern, whether immediate action is required, who should manage the matter, whether external advice is needed, and whether legal whistleblower protections may apply.

Step	Action
1. Receive and acknowledge	Record the report, acknowledge receipt where possible and explain next steps and support options.
2. Triage risk	Assess immediate safety, client, privacy, cyber, legal, employment, retaliation and evidence-preservation risks.
3. Appoint appropriate owner	Allocate the matter to an impartial person or investigation lead with suitable independence and capability.
4. Plan investigation	Define issues, evidence sources, witnesses, confidentiality requirements, timelines and communication approach.
5. Gather information	Collect documents, system logs, communications, interviews and other relevant information lawfully and fairly.
6. Assess findings	Evaluate evidence objectively and determine whether allegations are substantiated, unsubstantiated, partly substantiated or unable to be determined.
7. Take action	Implement corrective, disciplinary, remedial, training, control, contractual or reporting actions as appropriate.
8. Close and review	Document outcomes, communicate appropriately, check retaliation risks and identify lessons learned.

16. Support and protection measures

NexSys IT may implement support and protection measures based on the circumstances, including:

- protecting identity and limiting information access;
- changing reporting lines or work arrangements by agreement where appropriate;
- monitoring retaliation risks;
- providing an internal support contact;
- referring workers to employee support services where available;
- taking steps to prevent interference with evidence or witnesses;
- separating people involved in a matter where necessary and lawful;
- providing updates where appropriate and legally permitted.

17. Outcomes and corrective action

Where a report is substantiated, NexSys IT may take corrective action proportionate to the issue. This may include coaching, training, process improvement, control changes, system access changes, disciplinary action, termination of employment or contract, supplier review, client notification, regulatory reporting, remediation or legal action.

Where a report is not substantiated, NexSys IT may still take steps to address risks, misunderstandings, communication issues, training gaps or process weaknesses identified during the review.

18. Records, privacy and data security

Misconduct reports and investigation records must be handled securely, confidentially and in accordance with NexSys IT privacy, information security, employment, legal and client obligations.

Records may include reports, notes, evidence, emails, interview records, system logs, investigation plans, findings and outcome records. Access must be restricted to authorised personnel with a legitimate need to know.

Records must not be stored in personal email accounts, unauthorised drives, unapproved AI tools or unmanaged systems. Retention and destruction must follow legal, employment, audit, insurance, contractual and business requirements.

19. External reporting and emergency disclosures

This policy does not prevent any person from reporting to a regulator, law enforcement body, legal adviser, auditor, tax authority or other external body where they are legally entitled to do so.

Where a person is considering an external disclosure and wants to understand whether legal whistleblower protections may apply, they should consider obtaining independent legal advice. Certain public interest or emergency disclosures may only be protected if strict legal conditions are met.

20. Training and awareness

NexSys IT will provide misconduct reporting, ethics and non-retaliation awareness appropriate to each person's role. Personnel who receive reports, manage teams, investigate matters, administer systems, manage suppliers or handle sensitive information may receive additional guidance.

21. Breaches of this policy

Breaches of this policy may result in disciplinary action, suspension of access, contract termination, supplier review, client notification, regulator notification, legal action or other corrective measures. Serious breaches may include retaliation, maliciously false reports, concealment of misconduct, destruction of evidence, unauthorised disclosure of confidential report information or failure to escalate serious concerns.

A report that is not substantiated is not considered false or malicious merely because the concern could not be proven. However, deliberately false, dishonest or vexatious allegations may result in disciplinary action.

22. Review and maintenance

This policy will be reviewed at least annually and sooner if there are significant changes to NexSys IT operations, laws, regulator guidance, client requirements, supplier arrangements, workplace risk profile, reporting channels or incident trends.

23. Practical reporting rules for all personnel

- Speak up early when something appears illegal, unethical, unsafe or inconsistent with NexSys IT standards.
- Do not investigate serious matters yourself unless authorised. Preserve evidence and escalate.
- Treat all reports and investigations confidentially. Do not gossip or speculate.
- Do not retaliate, threaten, exclude, disadvantage or pressure anyone connected to a report.
- Use approved reporting channels and secure systems.
- Report cyber, privacy, safety or client-impacting concerns immediately.
- Be honest and cooperative during any assessment or investigation.
- Ask a manager or nominated contact if unsure how to raise a concern.

24. Contact and reporting channels

Contact point	Details
Nominated misconduct / whistleblower contact	HR Manager
Email	hr@nexsysit.com.au
Phone	1300 733 010
Website	www.nexsysit.com.au
Postal address	Level 27, 101 Collins Street Melbourne Victoria 3000 Australia
Emergency	Call 000 for immediate threats to life, safety or property.

Appendix A: Reporting misconduct quick reference

Report immediately if you become aware of:

- fraud, theft, bribery, corruption or serious dishonesty;
- sexual harassment, discrimination, bullying, victimisation or unsafe workplace conduct;
- retaliation or threats against someone for raising a concern;
- privacy breach, compromised account, cyber incident or unauthorised system access;
- client data copied, altered, deleted, exported or accessed without authority;
- serious breach of policy, law, contract or client requirement;
- attempts to conceal misconduct, destroy evidence or mislead an investigation.

Appendix B: Investigation principles

- Confidentiality: information is shared only with authorised people who need to know.
- Independence: investigators should be impartial and free from conflicts of interest.
- Procedural fairness: people involved should be treated fairly and given appropriate opportunity to respond.
- Timeliness: matters should be progressed without unnecessary delay.
- Evidence-based findings: outcomes should be based on relevant and reliable information.
- Protection: retaliation risks should be monitored throughout and after the process.
- Documentation: key decisions, evidence, findings and actions should be recorded securely.

Appendix C: Retaliation risk checklist

Managers and investigation owners should consider whether the reporter, witnesses or other participants have experienced or may experience:

- dismissal, demotion, suspension or disciplinary action;
- changes to duties, hours, rosters, reporting lines or work location;
- exclusion from meetings, projects, communications or opportunities;
- negative performance treatment, threats, intimidation, ostracism or bullying;
- reputational damage, gossip, pressure to withdraw a report or interference with evidence;
- contract, supplier, client or commercial disadvantage;
- any other adverse treatment that may be connected to the report.

Policy owner	CEO / Senior Management
Applies to	Employees, directors, officers, contractors, consultants, suppliers, agents, resellers, implementation partners and anyone performing services for or on behalf of NexSys IT
Jurisdiction	Australia, with specific application to the State of Victoria; global application to NexSys IT business dealings
Effective date	15 May 2026
Version	Reporting Misconduct and Non-Retaliation Policy 2026
Replaces	Reporting Misconduct and Non-Retaliation Policy 2024
Approved	Sean Zare CEO 14 May 2026

NEXSYS

1300 733 010
INFO@NEXSYSIT.COM.AU
NEXSYSIT.COM.AU

LEVEL 27
101 COLLINS STREET
MELBOURNE

LEVEL 29
2 CHIFLEY SQUARE
SYDNEY

LEVEL 19
10 EAGLE STREET
BRISBANE

LEVEL 28
140 ST GEORGES TERRACE
PERTH

LEVEL 24
91 KING WILLIAM STREET
ADELAIDE

LEVEL 31
48 SHORTLAND STREET
AUCKLAND