NEXSYS

POLICY

Privacy Policy

2026

NEXSYS

Contents

1. Overview
2. Scope and application
3. Key legal framework
4. Definitions
5. Privacy governance responsibilities
6. What personal information we collect
7. How personal information is collected
8. Collection notices and transparency
9. Purposes for using personal information
10. Use and disclosure limits
11. Disclosure to third parties
12. Overseas disclosure and cross-border handling
13. Marketing, cookies and analytics
14. Security of personal information
15. Data breach response
16. Access and correction
17. Retention and destruction
18. Employee, contractor and workplace privacy
19. Health information and sensitive information
20. Government identifiers
21. Artificial intelligence, automation and emerging technology
22. Client systems and managed service environments
23. Third-party and supplier privacy due diligence
24. Privacy complaints and enquiries
25. Training and awareness
26. Breaches of this policy
27. Review and maintenance
28. Practical privacy rules for all personnel

Appendix A: Data breach quick reference
Appendix B: Privacy impact assessment checklist

1. Overview

NexSys IT Pty Ltd is an Australian owned and operated technology integrator providing IT solutions and services to the architectural, engineering, construction and manufacturing sectors across Australia and the Asia Pacific region. In delivering these services, NexSys IT may collect and handle personal information relating to clients, prospective clients, suppliers, contractors, job applicants, employees, website users and other business contacts.

This Privacy Policy sets out how NexSys IT manages personal information in accordance with Australian privacy law, including the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Notifiable Data Breaches scheme, applicable telecommunications, spam and consumer laws, and relevant Victorian privacy, health records and surveillance obligations.

NexSys IT is committed to handling personal information lawfully, fairly, transparently and securely. Privacy is not only a legal obligation; it is part of maintaining trust with our clients, employees, suppliers and partners.

2. Scope and application

This policy applies to:

- all NexSys IT directors, officers, employees, contractors, consultants and temporary workers;
- all business units, offices, remote working arrangements and systems used by NexSys IT;
- all third parties that collect, access, store, process, host or transmit personal information for or on behalf of NexSys IT;
- all personal information handled in Australia, including Victoria; and
- personal information disclosed to, accessed from, stored in or processed by overseas recipients.

Where a law, client contract or regulatory requirement imposes a higher privacy, security or confidentiality standard than this policy, the higher standard must be followed.

3. Key legal framework

NexSys IT will comply with applicable privacy and data protection obligations, including the following.

Law / framework	Relevance to NexSys IT
Privacy Act 1988 (Cth) and Australian Privacy Principles	Core national privacy framework for handling personal information, including transparency, collection, use, disclosure, access, correction, direct marketing, overseas disclosure and security.
Notifiable Data Breaches scheme	Requires assessment and notification of eligible data breaches involving likely serious harm.
Privacy and Other Legislation Amendment Act 2024 (Cth)	Introduced major privacy reforms, including a statutory tort for serious invasions of privacy commencing in 2025 and new doxxing-related criminal offences.
Spam Act 2003 (Cth)	Regulates commercial electronic messages, including consent, sender identification and unsubscribe requirements.
Do Not Call Register Act 2006 (Cth)	Regulates certain telemarketing calls and marketing faxes.
Competition and Consumer Act 2010 (Cth) / Australian Consumer Law	Requires accurate, non-misleading statements about privacy, data handling, security and marketing practices.
Telecommunications Act 1997 (Cth) and Telecommunications (Interception and Access) Act 1979 (Cth)	Relevant where NexSys IT handles telecommunications-related information, communications metadata, network support or managed IT services.
Privacy and Data Protection Act 2014 (Vic)	Applies primarily to Victorian public sector information handling but may affect NexSys IT when providing services to Victorian public sector clients or contractually adopting Information Privacy Principles.
Health Records Act 2001 (Vic)	May apply if NexSys IT handles health information in Victoria, including employee health and safety records or client-related health information.
Surveillance Devices Act 1999 (Vic)	Relevant to use of listening, optical, tracking and data surveillance devices, including workplace monitoring and recordings.
Records, taxation, employment and work health and safety laws	May require retention of certain employee, payroll, financial, contract and safety records.

4. Definitions

Term	Meaning
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in material form or not.
Sensitive information	A higher-risk category of personal information, including health information, biometric information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record, union membership and other categories protected by law.
Health information	Personal information about an individual's health, disability, health services, medical history, injuries, workers compensation or health-related identifiers.
Employee records	Records directly related to current or former employment. Some employee records may be exempt from parts of the Privacy Act, but NexSys IT will still handle them responsibly, securely and in accordance with employment, workplace, health and safety and confidentiality obligations.
Data breach	Unauthorised access, unauthorised disclosure, loss, theft, misuse, alteration or compromise of personal information.
Overseas disclosure	Disclosing or making personal information accessible to a recipient outside Australia, including offshore support teams, cloud hosting providers and overseas contractors.

5. Privacy governance responsibilities

Privacy compliance is a shared responsibility across the business. NexSys IT will maintain clear accountability for privacy management, including executive oversight, operational controls, incident response and regular review.

Rose	Responsibility
Directors / senior leadership	Set privacy expectations, allocate resources, approve major risk decisions and ensure privacy is embedded in governance.
Privacy Officer / nominated responsible person	Maintain this policy, coordinate privacy enquiries, manage access and correction requests, support data breach response and maintain privacy registers.
Managers	Ensure teams follow privacy requirements, complete training, report incidents and manage third-party privacy risks.
Employees and contractors	Collect and handle personal information only as authorised, keep information secure, report suspected breaches immediately and complete privacy training.
Third-party service providers	Handle NexSys IT information only under approved instructions, contractual confidentiality, privacy and security controls.

6. What personal information we collect

NexSys IT collects information reasonably necessary for its business functions and activities. The types of personal information collected may include:

- contact details such as name, business address, email address, telephone number, job title and organisation;
- client and supplier relationship information, including account records, communications, proposals, quotes, contracts, purchase history, support requests and meeting notes;
- technical support information, including device, system, licence, user account, configuration, network, log, diagnostic and access information where required to deliver IT services;
- website, marketing and event information, including enquiry forms, newsletter preferences, webinar registrations, analytics and cookie-related information;
- billing, payment, procurement and finance information;
- recruitment information such as CVs, references, qualifications, interview notes and right-to-work information;
- employment and contractor records, including payroll, leave, performance, training, safety and access records;
- security and access information such as building access logs, CCTV images, authentication logs and identity verification information where applicable; and
- complaints, incident reports, investigation records and compliance records.

NexSys IT will not collect sensitive information unless the individual consents and the collection is reasonably necessary, or another lawful basis applies. Sensitive information must be handled with additional care and access restrictions.

7. How personal information is collected

Where practicable, NexSys IT collects personal information directly from the individual. Information may be collected when a person:

- contacts NexSys IT by phone, email, website form, social media, event registration or in person;
- requests information, support, quotations, demonstrations, proposals, licences or services;
- enters into a client, supplier, contractor or employment relationship with NexSys IT;
- uses NexSys IT systems, networks, managed services, support portals or collaboration platforms;
- attends NexSys IT premises, events, webinars or meetings;
- applies for a role with NexSys IT; or
- interacts with marketing communications or website analytics tools.

NexSys IT may also collect personal information from authorised representatives, employers, suppliers, recruitment agencies, referees, publicly available sources, regulators, professional advisers, software vendors, platform providers and clients where it is lawful and reasonable to do so.

8. Collection notices and transparency

At or before collection, or as soon as practicable afterwards, NexSys IT will take reasonable steps to make individuals aware of:

- NexSys IT's identity and contact details;
- the purposes of collection;
- whether collection is required or optional;
- the consequences if information is not provided;
- the types of third parties to whom information may be disclosed;
- whether information may be disclosed overseas and, where practicable, likely countries;
- how individuals may access and correct their information;
- how to make a privacy complaint; and
- where this Privacy Policy can be accessed.

9. Purposes for using personal information

NexSys IT uses personal information for purposes connected with its business, including to:

- provide IT integration, managed services, software, hardware, licensing, support and consulting services;
- respond to enquiries and provide client support;
- manage client, supplier, contractor and partner relationships;
- prepare proposals, quotes, tenders, contracts, invoices and reports;
- deliver implementation, troubleshooting, account administration, training, renewals and professional services;
- operate, secure, monitor and improve NexSys IT systems, platforms, premises and services;

- conduct marketing, communications, events and business development where lawful;
- recruit, employ, manage and support staff and contractors;
- meet legal, regulatory, taxation, employment, work health and safety, insurance and audit obligations;
- investigate complaints, misconduct, fraud, security incidents, data breaches and policy breaches;
- protect NexSys IT's legal rights and commercial interests; and
- conduct analytics, forecasting, service improvement and business planning using de-identified or aggregated data where practicable.

10. Use and disclosure limits

NexSys IT will use and disclose personal information only for the primary purpose for which it was collected, a related secondary purpose that the individual would reasonably expect, with consent, or where otherwise permitted or required by law.

Personal information must not be accessed out of curiosity, used for personal purposes, copied to unauthorised systems, disclosed to unauthorised recipients, or used in a way inconsistent with a collection notice, contract or this policy.

11. Disclosure to third parties

NexSys IT may disclose personal information to third parties where reasonably necessary for business purposes, including:

- software vendors, distributors, cloud providers, data centre operators, telecommunications providers and managed service partners;
- payment processors, banks, insurers, auditors, accountants, lawyers and professional advisers;
- recruitment agencies, referees, background checking providers and payroll providers;
- event platforms, email marketing platforms and customer relationship management providers;
- clients, suppliers and contractors where needed to deliver services or manage contracts;
- regulators, law enforcement, courts, tribunals, government agencies and dispute resolution bodies where required or authorised by law; and
- successors or prospective purchasers in connection with a restructure, merger, acquisition or sale of all or part of the business, subject to confidentiality and lawful handling requirements.

12. Overseas disclosure and cross-border handling

NexSys IT works with clients, suppliers, contractors and technology providers outside Australia. Personal information may be accessed from, stored in or disclosed to overseas recipients where this is necessary for service delivery, support, hosting, security, procurement, business administration or client requirements.

Before disclosing personal information overseas, NexSys IT will take reasonable steps to ensure the recipient handles the information consistently with the APPs, unless an exception under Australian privacy law applies. This may include contractual privacy clauses, confidentiality obligations, security requirements, access controls, data processing instructions, audit rights and breach notification obligations.

Where practicable, NexSys IT will identify likely overseas locations in collection notices, client contracts, supplier records or system documentation. Potential countries may include jurisdictions where NexSys IT's cloud, software, support or vendor services operate, including Australia, New Zealand, the United States, the United Kingdom, countries in the European Economic Area and the Asia Pacific region.

13. Marketing, cookies and analytics

NexSys IT may use personal information to communicate about products, services, events, webinars, updates and insights relevant to clients and prospects. Direct marketing will be conducted in accordance with the Privacy Act, Spam Act and Do Not Call Register requirements.

Commercial electronic messages must include sender identification and a functional unsubscribe facility. NexSys IT will honour unsubscribe and opt-out requests within a reasonable time and in accordance with legal requirements.

NexSys IT websites and digital services may use cookies, pixels, analytics tools and similar technologies to operate websites, remember preferences, understand usage and improve marketing relevance. Where required, NexSys IT will provide clear notices and preference options.

14. Security of personal information

NexSys IT will take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. Security controls will be proportionate to the nature of the information, the risk of harm and the business context.

- role-based access and least-privilege permissions;
- multi-factor authentication where appropriate;
- secure password and credential management;
- network, endpoint, email and cloud security controls;
- encryption in transit and at rest where appropriate;
- secure backup, logging and monitoring practices;
- physical access controls and secure disposal processes;
- contractual security requirements for vendors and contractors;
- privacy and cyber security training;
- incident response procedures and breach escalation pathways; and
- periodic review of systems, suppliers and controls.

15. Data breach response

All suspected or actual data breaches must be reported immediately to the Privacy Officer, IT/security team or nominated manager. A data breach may include misdirected emails, lost devices, compromised accounts, malware, unauthorised access, accidental disclosure, stolen credentials, ransomware, loss of files or improper use of personal information.

NexSys IT will assess suspected eligible data breaches promptly and take steps to contain, investigate and remediate the incident. If a breach is likely to result in serious harm to affected individuals and remedial action has not prevented that risk, NexSys IT will notify affected individuals and the Office of the Australian Information Commissioner as required under the Notifiable Data Breaches scheme.

Step	Action
1. Identify and contain	Secure systems, disable compromised access, recover lost information where possible and preserve evidence.
2. Assess	Determine what happened, what information is involved, who is affected and whether serious harm is likely.
3. Remediate	Reduce harm, patch vulnerabilities, recover services, update controls and provide support to affected individuals.
4. Notify	Notify affected individuals, regulators, clients, insurers or other parties where legally or contractually required.
5. Review	Document lessons learned, update policies and improve controls.

16. Access and correction

Individuals may request access to personal information NexSys IT holds about them or ask NexSys IT to correct inaccurate, out-of-date, incomplete, irrelevant or misleading information. Requests should be made using the contact details in this policy.

NexSys IT will respond within a reasonable period and may need to verify the individual's identity before releasing information. Access may be refused or limited where permitted by law, for example where release would unreasonably affect another person's privacy, prejudice an investigation, reveal commercially sensitive information, or be unlawful.

17. Retention and destruction

NexSys IT will retain personal information only for as long as reasonably necessary for the purpose for which it was collected, or as required for legal, regulatory, employment, taxation, contractual, insurance, audit or dispute management purposes.

When personal information is no longer required, NexSys IT will take reasonable steps to securely destroy or de-identify it, unless retention is required or permitted by law. Disposal methods may include secure deletion, certified destruction, media sanitisation, de-identification or archiving with restricted access.

18. Employee, contractor and workplace privacy

NexSys IT handles employee and contractor information to manage recruitment, employment, onboarding, payroll, performance, security, workplace safety, training, conduct, investigations, leave, benefits, separation and legal compliance. Even where employee record exemptions may apply under the Privacy Act, NexSys IT will treat employee and contractor information responsibly and in accordance with workplace, confidentiality and security obligations.

Workplace monitoring, including system logs, email security tools, endpoint management, building access, CCTV and similar controls, will be used only for legitimate business, security, safety, compliance and operational purposes. Monitoring must be proportionate, transparent and consistent with Victorian surveillance and workplace laws.

19. Health information and sensitive information

NexSys IT may handle health information in limited circumstances, such as workplace injury, safety incidents, fitness-for-work matters, leave management, emergency contacts, reasonable adjustments or client-related support where health information is incidentally involved. Health information will be handled with additional safeguards, including restricted access and purpose limitation.

NexSys IT will not collect biometric information, facial recognition templates, government identifiers, criminal history checks or other sensitive information unless the collection is necessary, lawful, transparent and subject to appropriate approvals and controls.

20. Government identifiers

NexSys IT will not use Australian government identifiers, such as Tax File Numbers, Medicare numbers, passport numbers or driver licence numbers, as its own identifiers. Government identifiers will be collected, used and disclosed only where lawful and reasonably necessary, such as payroll, identity verification, right-to-work checks or legal compliance.

21. Artificial intelligence, automation and emerging technology

NexSys IT may use automation, analytics or AI-enabled tools to improve operations, cyber security, support, service delivery and business administration. Personal information must not be entered into public AI tools or external automated systems unless approved by NexSys IT and subject to appropriate privacy, confidentiality, security and client contractual controls.

Where AI or automated tools are used to handle personal information, NexSys IT will consider privacy-by-design, data minimisation, security, accuracy, transparency, human oversight and vendor risk controls.

22. Client systems and managed service environments

In providing IT services, NexSys IT personnel may access client systems that contain personal information controlled by the client. NexSys IT personnel must access client personal information only where authorised and necessary to perform services, and must comply with client instructions, contractual requirements, confidentiality obligations and applicable laws.

If NexSys IT discovers a suspected data breach, security weakness or privacy incident involving a client environment, the matter must be escalated immediately in accordance with incident response procedures and client notification obligations.

23. Third-party and supplier privacy due diligence

Before engaging third parties that handle personal information for NexSys IT, the responsible manager must consider privacy and security risks. Depending on the nature and risk of the arrangement, due diligence may include:

- reviewing the supplier's privacy policy, security documentation and data locations;
- checking whether the supplier uses subcontractors or offshore processing;
- confirming breach notification, confidentiality and access control obligations;
- ensuring contracts include appropriate privacy, cyber security, audit, return/deletion and assistance clauses;
- assessing whether sensitive information or large volumes of personal information are involved; and
- documenting approvals and residual risk.

24. Privacy complaints and enquiries

Individuals may contact NexSys IT with privacy questions, access or correction requests, complaints, unsubscribe requests or concerns about how personal information has been handled.

NexSys IT will acknowledge privacy complaints within a reasonable period, investigate the matter fairly, and provide an outcome or update as soon as practicable. If an individual is not satisfied with NexSys IT's response, they may be able to complain to the Office of the Australian Information Commissioner or another relevant regulator.

Contact Point	Details
Privacy contact	NexSys Privacy Officer
Email	info@nexsysit.com.au
Phone	+61 1300 733 010
Website	www.nexsysit.com.au
Postal address	Level 27, 101 Collins Street Melbourne Victoria 3000 Australia

25. Training and awareness

NexSys IT will provide privacy and information security awareness appropriate to each person's role. Personnel handling higher-risk information, client systems, recruitment records, employee records, support tickets, remote access tools, marketing systems or supplier integrations may receive additional training.

26. Breaches of this policy

Breaches of this policy may result in disciplinary action, contract termination, suspension of access, client notification, regulator notification, legal action or other corrective measures. Deliberate misuse, unauthorised disclosure, concealment of a data breach or failure to report a suspected incident may be treated as serious misconduct.

27. Review and maintenance

This policy will be reviewed at least annually, and sooner if there are significant changes to NexSys IT's operations, technology, legal obligations, regulator guidance, data handling practices, service offerings, overseas arrangements or security risk profile.

28. Practical privacy rules for all personnel

1. Collect only the personal information needed for a legitimate business purpose.
2. Be clear and transparent about why information is collected and how it will be used.
3. Use personal information only for approved purposes.
4. Do not share personal information with unauthorised people or systems.
5. Use approved NexSys IT systems, not personal email, personal drives or unauthorised AI tools.
6. Check recipients before sending emails or files containing personal information.
7. Apply extra care to sensitive, health, identity, payroll, recruitment and access information.
8. Report suspected data breaches immediately, even if the issue seems minor.
9. Do not download or copy client data unless necessary and authorised.
10. Ask the Privacy Officer or manager before doing anything new, high-risk or unclear with personal information.

Appendix A: Data breach quick reference

Immediate escalation triggers

- Personal information sent to the wrong recipient.
- Lost or stolen laptop, phone, storage device, printout or access card.
- Compromised email, remote access, administrator or cloud account.
- Suspicious login, malware, ransomware or unauthorised access.
- Client data copied, exported, deleted or accessed without authority.
- Supplier or cloud provider reports a security or privacy incident.
- Any incident involving health, identity, payroll, financial, child-related or sensitive information.

Appendix B: Privacy impact assessment checklist

A privacy impact assessment or privacy review should be considered before starting new activities that involve significant or changed handling of personal information, especially where the activity involves sensitive information, automated decision-making, AI tools, surveillance, offshore processing, large data sets, new integrations or client data access.

- What personal information will be collected, used or disclosed?
- Is the information necessary and proportionate?
- What notice or consent is required?
- Will information be disclosed overseas?
- Who can access the information and why?
- What security controls apply?
- How long will the information be retained?
- How will individuals exercise access, correction or complaint rights?
- What happens if there is a data breach?
- Do contracts and supplier controls match the risk?

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	Privacy Policy 2026
Replaces	Privacy Policy 2025
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