GIS-Pax Pty Ltd

Security & Privacy Statement

Public website policy

Version 1.0

Effective date: 15 June 2026

Document information

Document	Security & Privacy Statement
Owner	Commercial Manager, GIS-Pax Pty Ltd
Effective date	15 June 2026
Version	1.0
Audience	Customers, procurement teams, partners and prospective customers
Security contact	security@gis-pax.com

Version	Date	Author	Revision details
1.0	15 June 2026	GIS-Pax	First published version.

GIS-Pax Pty Ltd (**GIS-Pax**) develops, and licenses specialist geoscience software used by energy companies, government agencies, universities, research organisations and consultants worldwide. We understand that, from time to time, our customers may entrust us with their information, and we take a practical and considered approach to protecting it. This statement provides an overview of our security and privacy practices. This information is intended to provide customers and partners with confidence in our operational practices and is provided for informational purposes only. It does not form part of any contract.

1. Security commitment

Security is an ongoing priority that is supported by our management team. We maintain documented information security policies and procedures, manage security risks through a defined risk management process. We review our practices periodically, and as our business and the threat environment change. Our objective is to protect the confidentiality, integrity and availability of any information we may hold.

2. Information protection

We apply controls that are appropriate to the level of sensitivity of the information we handle. Information is encrypted in transit using industry-standard protocols, and we use secure, reputable cloud-hosted services for relevant systems where applicable. We classify and handle information according to its sensitivity and apply the principle of least privilege so that information is only accessible to those who need it.

3. Access controls

Access to our systems and information is governed by role-based access controls and the principle of least privilege. Access is granted based on business need, is reviewed periodically, and is revoked promptly when personnel change roles or leave the organisation, in line with our onboarding and offboarding procedures.

4. Authentication practices

We require individual user accounts and use multi-factor authentication where it is supported by the relevant system. We apply sensible credential management practices and discourage the sharing of accounts and passwords.

5. Secure development and change management

Changes to our software, systems and services are managed through a documented change management process that includes assessment, testing and appropriate approval before changes are released. We consider security as part of our development and change activities and aim to address security issues in a timely and risk-based manner.

6. System maintenance and patch management

We keep our systems and software reasonably up to date and apply security updates and patches on a risk-prioritised basis, giving priority to higher-severity issues. We maintain an inventory of key software and systems to support this activity.

7. Backup and recovery

We maintain backup and recovery procedures for key systems and data so that information can be restored in the event of data loss or system failure. Backups are configured according to the importance of the relevant system, and recovery processes are reviewed from time to time.

8. Business continuity

We have arrangements in place to help us continue or restore key business operations following a disruptive event. These arrangements are reviewed periodically and are designed to be proportionate to the size and nature of our business.

9. Employee security awareness

Our personnel are responsible for protecting the information they handle. We provide security awareness guidance covering topics such as recognising phishing and social engineering, good password and multi-factor authentication practices, secure handling of data, and reporting suspected security events. Personnel are made aware of their security responsibilities as part of their engagement with GIS-Pax.

10. Third-party service providers

We rely on a number of reputable third-party providers, including cloud hosting, email and other supporting services. We select providers with regard to their security posture and, where appropriate, address security and confidentiality expectations through our contracting arrangements. Some providers may store or process information outside Australia; further detail on overseas handling of personal information is set out in our Privacy Policy.

11. Responsible disclosure and vulnerability reporting

We welcome reports from researchers, customers and members of the public who identify a potential security vulnerability in our website, products or services. If you believe you have found a vulnerability, please contact us at **security@gis-pax.com** with sufficient detail to allow us to reproduce and assess the issue. We ask that you act in good faith, avoid accessing or modifying

data that is not your own, and give us a reasonable opportunity to investigate and respond before any public disclosure. We will acknowledge legitimate reports and work to address confirmed issues on a risk-prioritised basis. We periodically review and assess our systems for security weaknesses; such reviews are conducted on a periodic basis and are not a guarantee that all vulnerabilities will be identified.

12. Privacy commitment

We handle personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles. We collect only the personal information we reasonably need, use it for the purposes for which it was provided, and take reasonable steps to protect it. Full details of how we collect, use, disclose and protect personal information are set out in our Privacy Policy, available on our website.

13. Security contact

For security enquiries, or to report a suspected vulnerability or security incident involving GIS-Pax, please contact:

GIS-Pax Security

Email: security@gis-pax.com

Website: www.gis-pax.com