Schedule D — Security

Version 1.0 · Effective 16 November 2026 · Last updated 16 November 2026 · Legal bundle DRIP-LEGAL-2026-11-16

ITEM	VALUE
Document	Schedule D to the DeRISK™ Intelligence Platform EULA — Security
Version	1.0
Effective date	16 November 2026
Published at	denexus.ai/legal/security

This Schedule summarizes how DeNexus protects the platform and Customer Data. More detail, including security questionnaires and audit reports, is available under confidentiality terms from security@denexus.ai.

1. How we protect your data

AREA	CONTROLS
Hosting	Customer Data is held in DeNexus's cloud environment, segregated by tenant, with no access between customers
Encryption	Data encrypted in transit and at rest
Access	Single sign-on support; staff access on a least-privilege basis, with multi-factor authentication and periodic review
AI processing	AI Models process data in inference only and do not retain it. Controls at the model boundary mask credentials and payment-card numbers, screen documents for prompt-injection attempts, and filter personal data from generated reports. Customer Data is never used to train AI Models (EULA 7.3)
Application security	Secure development practices, dependency and vulnerability management, regular patching
Monitoring	Security events logged and monitored; usage monitored to detect abuse
Data lifecycle	Retention and deletion by tier (EULA 7.5 to 7.7); backups deleted within 35 days of deletion
Resilience	Backups and documented recovery procedures
People	Confidentiality obligations and security training for all staff
Suppliers	Security due diligence and contractual data protection terms for sub-processors

2. Assurance and incidents

2.1 Independent assurance. DeNexus maintains a SOC 2 Type II report at company level, available to customers and prospects under confidentiality terms.

2.2 Security reviews. Customers may ask for completed security questionnaires and further documentation under confidentiality terms. Audit rights for personal data are set out in the DPA (Schedule C, Section 5).

2.3 Incident notification. If DeNexus confirms a personal data breach affecting Customer Data, it notifies the customer within 48 hours, or any shorter period agreed in an MSA (Schedule C, Section 3.3).

3. Shared responsibility

Security is shared. DeNexus secures the platform; you secure how your organization uses it. You are responsible for:

- managing your Authorized Users and keeping their credentials secret, preferably through single sign-on with multi-factor authentication;
- removing access promptly when people leave;
- the security of your systems and of data before it reaches the platform;
- submitting only the data you need, and no special categories of personal data;
- telling security@denexus.ai promptly if you suspect a compromise.

4. Vulnerability disclosure policy

DeNexus welcomes reports of security vulnerabilities from researchers acting in good faith. Send reports to **security@denexus.ai**. This policy is also referenced in denexus.ai/.well-known/security.txt.

4.1 Scope.

IN SCOPE	OUT OF SCOPE
The DeRISK™ Intelligence Platform application; denexus.ai	Denial-of-service testing; social engineering or phishing of DeNexus staff or customers; physical attacks; third-party services and providers we use; findings from automated scanners without a demonstrated impact

4.2 Rules. When testing, you must:

- access, change or keep no data beyond the minimum needed to show the issue, and never other customers' data;
- stop testing and report as soon as you find a vulnerability;
- not disrupt the platform or degrade it for others;
- keep the issue confidential until DeNexus has fixed it, or for 90 days after your report, whichever comes first;
- comply with applicable law.

4.3 Safe harbour. If you follow this policy, DeNexus will not take legal action against you for your research, and considers it authorized under the EULA (Section 5.3).

4.4 What to expect. DeNexus acknowledges reports within 3 business days and completes triage within 10 business days. It will keep you informed and may credit you publicly with your consent.

4.5 No bug bounty. DeNexus does not offer payment for reports.

Questions about these terms: legal@denexus.ai · Current version: denexus.ai/legal