ITERONIX MSP PLATFORM

Security Questionnaire

Iteronix HelpDesk — pre-filled answers

Audience: Prospects & auditors · Version 2026-11-18

Pre-filled answers to the questions prospects most often ask about how **Iteronix LLC** protects client data. Contact security@iteronix.co for anything not covered here. Last updated: 2026-11-04.

1. Company & governance

Question	Answer
Who provides the service?	Iteronix LLC, cr 18a.
Is there a written information-security policy?	Yes — the Security Incident Policy, Data Retention Policy, Data Processing Agreement and Acceptable Use Policy are published at /legal.
Do staff sign confidentiality obligations?	Yes. Access is limited to staff and contractors who need it for the service.
Is there cyber / professional liability insurance?	Details available on request.

2. Data location & processing

Question	Answer
Where is client data stored?	Portal application and database: the hosting provider listed in the Sub-processor List (United States). Document Backup files: the storage provider configured for the service (Backblaze B2 or Cloudflare R2).
Do you sell or share client data?	No. Data is used only to provide the service, as set out in the Data Processing Agreement.
Which sub-processors are used?	See the Sub-processor List at /legal/subprocessors. Optional features (AI assistance, payments, sign-in) are only used when enabled.
GDPR / UK GDPR / CCPA?	A Data Processing Agreement with standard processor terms is available and accepted in the portal.

3. Encryption

Question	Answer
In transit?	TLS (HTTPS) for all portal, agent and storage traffic; HSTS enforced.

At rest — secrets?	Passwords in the documentation vault, 2FA seeds, BitLocker recovery keys and integration secrets are encrypted with AES-256-GCM.
At rest — backups?	Document Backup files are encrypted on the client's PC with a per-client AES-256-GCM key before upload; the storage provider only holds ciphertext. The nightly off-site database backup is compressed and encrypted with AES-256-GCM using a key derived from an offline passphrase.

4. Access control

Question	Answer
How do staff sign in?	Individual accounts with rate-limited sign-in; two-factor authentication for administrators; single sign-on for client users (Microsoft / Google).
Least privilege?	Role-based access (admin, IT, employee) plus per-client and per-site scopes; technicians only see clients they are assigned to.
Privileged actions?	Deleting customers, database exports and off-site backup downloads require a fresh sign-in; every privileged action is written to an audit log.
Client-side separation?	Every request that references a ticket, asset, device, invoice or document is checked against the user's client scope.

5. Endpoint agent

Question	Answer
What does the Windows agent do?	Inventory, monitoring, patching, security posture, document backup and technician-requested actions.
How is it authenticated?	Each device has its own random 192-bit key, stored with Windows DPAPI; keys can be revoked individually and are rotated when a device re-registers.
Can it be removed by users?	Uninstalling and closing the tray require an administrator password.
Remote access?	Only after the client accepts the Remote Access and Monitoring Authorization; console commands and file transfers are audit-logged.
Updates?	Agent updates are verified by SHA-256 (and optionally the code-signing certificate) and rolled out to a pilot group first.

6. Availability & recovery

Question	Answer
Backups of the platform?	Daily database backups on the server plus a nightly encrypted off-site copy (retained 30 days by default).
Deleted data?	Deleted records and removed devices are recoverable for 90 days, then permanently deleted.
Status and incidents?	Live service status and incident history at /status.

7. Secure development & testing

Question	Answer
Common web vulnerabilities?	Parameterised database queries (no string-built SQL), output escaping, formula-safe CSV exports, SSRF protection for outbound checks, security headers (HSTS, frame-ancestors, nosniff, referrer policy).
Reviews?	Security review with each release; findings and fixes are documented. External penetration testing is planned before large-scale onboarding.

8. Incident response

Question	Answer
Breach notification?	Clients are notified without undue delay as set out in the Security Incident Policy and the Data Processing Agreement.
Security contact	security@iteronix.co