ITERONIX HELPDESK

Data Processing Agreement

Version 1.1

Audience: Client organisation · Version 2026-11-18

This Data Processing Agreement ("DPA") forms part of the Master Services Agreement between **Iteronix LLC** ("Processor" or "Iteronix") and the Client ("Controller"). It applies where Iteronix processes personal data on behalf of Client in providing the Services.

1. Roles and scope

1.1 Client is the controller (or "business") and Iteronix the processor (or "service provider") of Client personal data processed for the Services. 1.2 **Subject matter and duration:** provision of the Services for the term of the Agreement. 1.3 **Nature and purpose:** IT support, device management, monitoring, patching, security, remote access, documentation, billing and related services. 1.4 **Data subjects:** Client's employees, contractors and other users; Client's contacts. 1.5 **Categories of data:** names, business contact details, job titles, account identifiers, sign-in and audit logs, IP addresses, device and software inventory, support communications and attachments, and any personal data Client or its users choose to submit or store on managed systems. Client will not ask Iteronix to process special-category or regulated data (e.g. health, biometric, payment card data) unless agreed in writing with appropriate additional terms.

2. Processor obligations

Iteronix will: (a) process personal data only on Client's documented instructions (this Agreement and use of the Service are Client's instructions), unless required by law; (b) not sell or share personal data, or use it for any purpose other than providing the Services (including as required by the California Consumer Privacy Act as a service provider); (c) ensure personnel with access are bound by confidentiality; (d) implement appropriate technical and organisational measures (Annex 1); (e) assist Client, at Client's cost where more than minimal, with data-subject requests, security, breach notifications and impact assessments; (f) notify Client **without undue delay (and in any case within 72 hours)** after becoming aware of a personal-data breach affecting Client data, with the information reasonably available; (g) at the end of the Services, delete or return Client personal data within 90 days, unless retention is required by law, and delete backups in the ordinary backup cycle; (h) make available information reasonably necessary to demonstrate compliance, via written responses and documentation; on-site audits only once per year, on 30 days' notice, at Client's cost and subject to confidentiality.

3. Sub-processors

3.1 Client authorises Iteronix to use the sub-processors listed in the **Sub-processor List** published in the portal. 3.2 Iteronix will give notice of new sub-processors by updating the list; Client may object on reasonable data-protection grounds within 15 days, in which case the parties will discuss in good faith and Client may terminate the affected Service as its sole remedy. 3.3 Iteronix imposes data-protection terms on sub-processors substantially no less protective than this DPA.

4. International transfers

Personal data may be processed in the United States, the United Kingdom, the European Economic Area and other countries where Iteronix or its sub-processors operate. Where required, the parties agree to the applicable standard contractual clauses (including the UK International Data Transfer Addendum) which are incorporated by reference.

5. Client obligations

Client warrants that it has a lawful basis and has given all notices (including notices to employees of device monitoring) required for Iteronix to process personal data under this DPA.

6. Liability

Liability under this DPA is subject to the limitations in the Master Services Agreement.

Annex 1 — Security measures

- Encryption in transit (TLS) for the portal, agents and integrations; stored credentials and secrets encrypted (AES-256-GCM).
- Role-based access with per-client scoping; multi-factor authentication for Iteronix staff.
- Audit logging of administrative actions, credential access and remote actions.
- Individually revocable device-agent keys; commands only from authorised staff.
- Regular patching of Iteronix systems; vulnerability monitoring.
- Backups of the Iteronix database with restricted access.
- Document Backup files encrypted on the device (AES-256-GCM) before upload; per-client keys stored encrypted on the Iteronix server.
- Deleted records and removed devices kept for 90 days to allow recovery, then permanently deleted.
- Security incident response procedure (see Security Incident Policy).