ITERONIX HELPDESK

Acceptable Use Policy

Version 1.0

Audience: All users · Version 2026-11-18

This policy applies to everyone who uses **Iteronix HelpDesk** or is covered by services from **Iteronix LLC**. It is part of the Terms of Use and the Client Agreement.

You must not

1. Access, or try to access, data, devices or accounts you are not authorised to use — including other Clients' data.
2. Probe, scan, test or bypass the security of the Service or of Iteronix systems without written permission.
3. Upload or send malware, or use the Service to attack, spam or defraud anyone.
4. Share your credentials, or use another person's account.
5. Interfere with, overload or disrupt the Service, device agents, remote-access or monitoring tools.
6. Remove, disable or tamper with Iteronix device agents, security software or monitoring on managed devices without authorisation from your organisation and Iteronix.
7. Use the Service to store or transmit unlawful, infringing, harassing or defamatory content.
8. Put passwords, payment card numbers or sensitive personal data into tickets or chat unless we ask through a secure channel.
9. Copy, resell, reverse-engineer or build a competing product from the Service.

You should

- Report suspicious emails, lost devices and suspected security incidents to Iteronix **immediately**.
- Keep your device updated and restart it when asked.
- Use strong, unique passwords and multi-factor authentication.

Enforcement

Iteronix may investigate suspected breaches, preserve evidence, suspend access, isolate devices from the network to contain a threat, and report unlawful activity to authorities. Breaches by a Client's users are the Client's responsibility under the Client Agreement.