ITERONIX HELPDESK

Security Incident Policy

Version 1.0

Audience: Information · Version 2026-11-18

How **Iteronix LLC** ("Iteronix") handles security incidents affecting Iteronix systems or Client data processed by Iteronix.

1. Report

Report suspected incidents to **security@iteronix.co** or by opening a Critical ticket. Client users should also report phishing, lost devices and suspicious activity immediately.

2. Response steps

1. **Triage** — confirm the incident, classify severity, open an incident record.
2. **Contain** — isolate affected devices or accounts, revoke keys and credentials, block malicious activity.
3. **Investigate** — preserve logs and evidence; determine scope and data affected.
4. **Eradicate and recover** — remove the cause, restore from clean sources, monitor for recurrence.
5. **Notify** — inform affected Clients without undue delay and within 72 hours of confirming a personal-data breach affecting their data, with the facts known and updates as they develop. Clients remain responsible for notifying regulators and individuals where they are the controller, and Iteronix will assist.
6. **Review** — document lessons learned and improvements.

3. Records

Iteronix keeps a record of incidents, actions taken and notifications made.