SOP D — Lost/Stolen Device: 5-Step Rapid Response

ToroTek LLC — Standard Operating Procedure

Move fast to contain risk, confirm encryption, and protect client confidences when a device goes missing.

Before You Start

- Maintain a current device inventory with owner, last seen, and encryption status.
- Enable remote lock/wipe capability on all laptops/phones where possible.

Step-by-Step

1. **Step 1.** Notify the managing attorney and IT immediately; record the time and last known location.
2. **Step 2.** Attempt remote lock and, if necessary, remote wipe; document results.
3. **Step 3.** Change the user's account passwords and revoke active sessions/tokens.
4. **Step 4.** Verify BitLocker/Device Encryption status for the missing device.
5. **Step 5.** Assess client data exposure; follow client-notification requirements and consider a police report.

Done-Right Checklist

- Remote lock/wipe attempted and logged.
- All account credentials rotated; MFA re-enrolled if needed.
- Encryption status confirmed in inventory records.
- Incident record created with who/what/when and next steps.

When to Call ToroTek

- The device was not encrypted or contains highly sensitive case materials.
- Evidence of account compromise or data access after loss/theft.
- Regulatory/ethical notification thresholds may be met.

Pro Tips

- If a personal device is used for work, require encryption and the right to wipe the work profile.
- Keep recovery keys secured and accessible to owners only.

Need help? ToroTek is here.
Call/Text: 619-376-6995
Support: help@toro-tek.com
Web: torotekllc.com

Updated: 2025-08-13