Sentrike

TEMPLATE

Takedown authorization charter

Signed once at onboarding, so the provider can act on phishing and impersonation without asking each time. **Not legal advice:** adapt it with both parties' counsel before signing.

CLIENT	PROVIDER	EFFECTIVE DATE

1. SCOPE

COVERED	DETAILS
Brands and trademarks	
Domains owned by the client (never reported)	
Official social accounts (never reported)	
Executives covered (with consent)	

2. PRE-APPROVED ACTIONS

- [ ] Reporting phishing and impersonating sites to Google Safe Browsing, SmartScreen and similar services
- [ ] Abuse reports to hosts, registrars, registries and CDNs, with follow-up until removed
- [ ] Reporting accounts that impersonate the client or its executives
- [ ] Notices about content copied from the client's websites, as authorized agent

3. NEEDS WRITTEN APPROVAL, PER CASE

- [ ] Filing a UDRP, URS or other domain dispute
- [ ] Legal letters or cease-and-desist notices
- [ ] Contacting law enforcement or the press
- [ ] Buying or registering domains
- [ ] Any public statement

4. EVIDENCE AND CONTACTS

ITEM	DETAILS
Evidence kept for	
Approvals and escalations	
Signs letters of authorization	

SIGNED FOR CLIENT · NAME, TITLE, DATE	RIGHTS HOLDER, IF DIFFERENT	SIGNED FOR PROVIDER · NAME, TITLE, DATE