

Social Media Security: IT & Security Checklist

Social media is a critical business channel — driving visibility, engagement, and revenue. But because these platforms often sit outside enterprise identity systems, they often bypass security controls. The result? IT loses visibility, marketing juggles complex access tasks, and attackers exploit accounts for fraud or brand damage. Use this checklist to close gaps, streamline workflows, and safeguard your brand.



- 1. Centralize account ownership and visibility** ☐
Create a single source of truth for all corporate social accounts.
Track owners, purpose, users, and platforms to eliminate rogue or unapproved profiles.
- 2. Use corporate accounts, not individual accounts, for access and recovery** ☐
Register every account with managed corporate credentials and align recovery options with enterprise identity tools so access never depends on personal emails or phone numbers.
- 3. Strengthen authentication** ☐
Vault credentials, enforce phishing-resistant MFA, rotate passwords automatically, and delegate access so users never handle passwords or one-time codes.
- 4. Automate provisioning and deprovisioning** ☐
Tie social accounts to identity workflows. Grant access at onboarding and revoke instantly at offboarding.
- 5. Govern permissions with least privilege** ☐
Apply role-based access, grant only what's required, and review entitlements regularly.
- 6. Secure third-party integrations** ☐
Audit apps connected to social platforms, remove unused integrations, and restrict active connections to approved scopes.
- 7. Monitor activity and detect anomalies** ☐
Track logins and configuration changes across platforms, and alert on suspicious behavior to quickly identify misuse or compromise.
- 8. Protect against shared credential risks** ☐
Stop using spreadsheets, email, and chat to store or share passwords.
Use secure, delegated access so every user gets an individual, auditable path without ever exposing credentials.
- 9. Enable marketing with secure access** ☐
Automate access, enforce MFA, and remove manual credential handling so Marketing can launch campaigns fast without sacrificing security.
- 10. Establish incident response and recovery procedures** ☐
Develop and test a plan for account takeovers, lockouts, or fraudulent spend.
Define clear roles, escalation paths, and recovery steps to keep the business running.

About Cerby

Cerby provides Marketing and IT teams with the only solution for securely and centrally managing access across all social media platforms. We automate and simplify key identity processes, including password rotations, MFA enforcement, managing user access, onboarding & offboarding agencies and freelancers, and monitoring shared accounts. By streamlining these tasks, Cerby enhances team productivity, enables seamless collaboration with external parties, and safeguards your brand's online presence, allowing your teams to focus on growth without worrying about social media security.

Visit us at [Cerby.com](https://cerby.com) and follow us on social at [@CerbyHQ](https://twitter.com/CerbyHQ).