29 West 35th Street, 7th Floor
New York, NY 10001 USA
sprinklr.com

# Sprinklr 10-Point Security Checklist

Security should always be a foundational part of your social media and messaging strategy, but it's easy to get caught up in your day to day and overlook it. As a brand manager, what should you do? How can you sleep better at night knowing that you are doing everything in your power to mitigate risk?

We have gathered the ten best practices for social access security: your "**10-Point Security Checklist**". While this is not 100% foolproof, it will go a long way to protecting your brand. If you need help with any of these items, we are here to help:

1. **Make sure you know who manages your social media accounts and that you're maintaining proper access hygiene**
   Check that the email address and phone number associated with your company's social media accounts are the correct ones. And for Facebook, check Business Manager to see which Facebook Profiles have access to your business' Pages and Ad Accounts. If you don't know them or why they have access, make sure you find out. Put a recurring hold on your calendar to check this monthly.
2. **Set-up Two-Factor Authentication (TFA) on all your social media accounts**
   Ensure that everyone who has native channel access to your Facebook Page has TFA set-up for their Facebook Profiles - and do the same on any social media or messaging channel that allows TFA. We recommend monthly checking that the email address and phone number associated with your social media accounts are the correct ones.
3. **Go into each social channel and see which third-party apps are connected**
   If you haven't used them in a while, disconnect them (If you don't use it, lose it!).
4. **Use a system to secure and govern native access to your accounts such as Sprinklr Secure Access**
   Systems like Sprinklr Secure Access (SSA) can set access based on time frames which can be useful when engaging with contractors or agencies.
5. **Set up Single-Sign-On (SSO) connected to your company's active directory**
   This means when people no longer have access to your company's network, they don't have access to your social channels either.
6. **Have a mandate that your business only permits publishing through a secure social media management solution and set up a rule to notify you when posts get published natively**
   Posts publishing directly on social media, outside of a system, could be a red flag.
7. **Set up a listening query to establish the source application of your posts**
   Understanding which third party apps are posting on your behalf will help to alert you to take action and where the source of the problem is.
8. **Whitelist IP Addresses**
   Provide a list of IP addresses to your social media management platform provider to whitelist and ensure they're the only ones allowed by users to access your social media management platform.
9. **Set up rules to auto-delete or at least alert you to posts containing keywords typically associated with account breaches**
   These are similar to rules you would set up for good social media practices around profanity for example.
10. **Use an enterprise-grade, security-obsessed social media management platform**
    Whoever you choose, make sure they've got the clientele to back up their security credentials - e.g. banks who have exhaustive security requirements (and rightfully so). And ensure that your technology partner is not just relying on infrastructure to protect you, but monitoring accounts in their platform for questionable behavior.