**TASK 1: Password Policy Review**

**Step 1: Review Current Password Policy**

This step is about understanding the baseline. You’re asking:

• Does the company have a written policy?

• Are users following it?

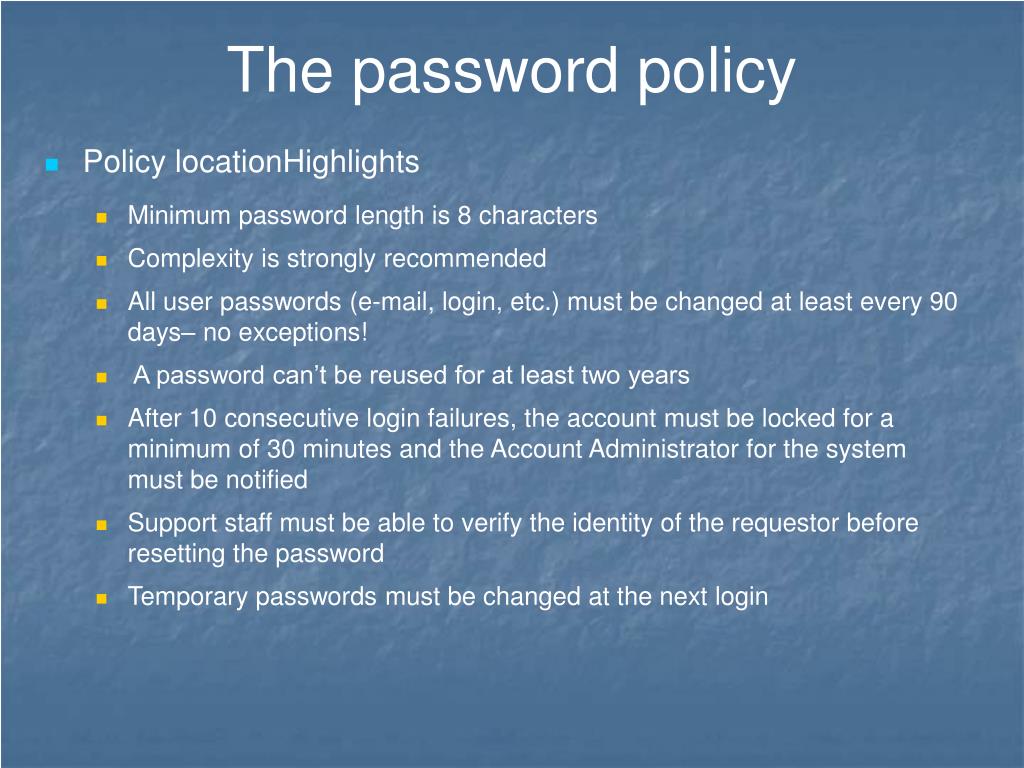
• Is it aligned with modern security standards?

Why it matters:

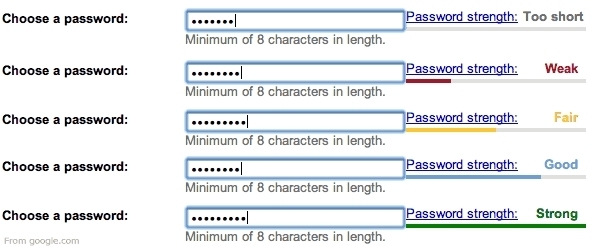
• Many small companies either don’t have a policy or use outdated rules.

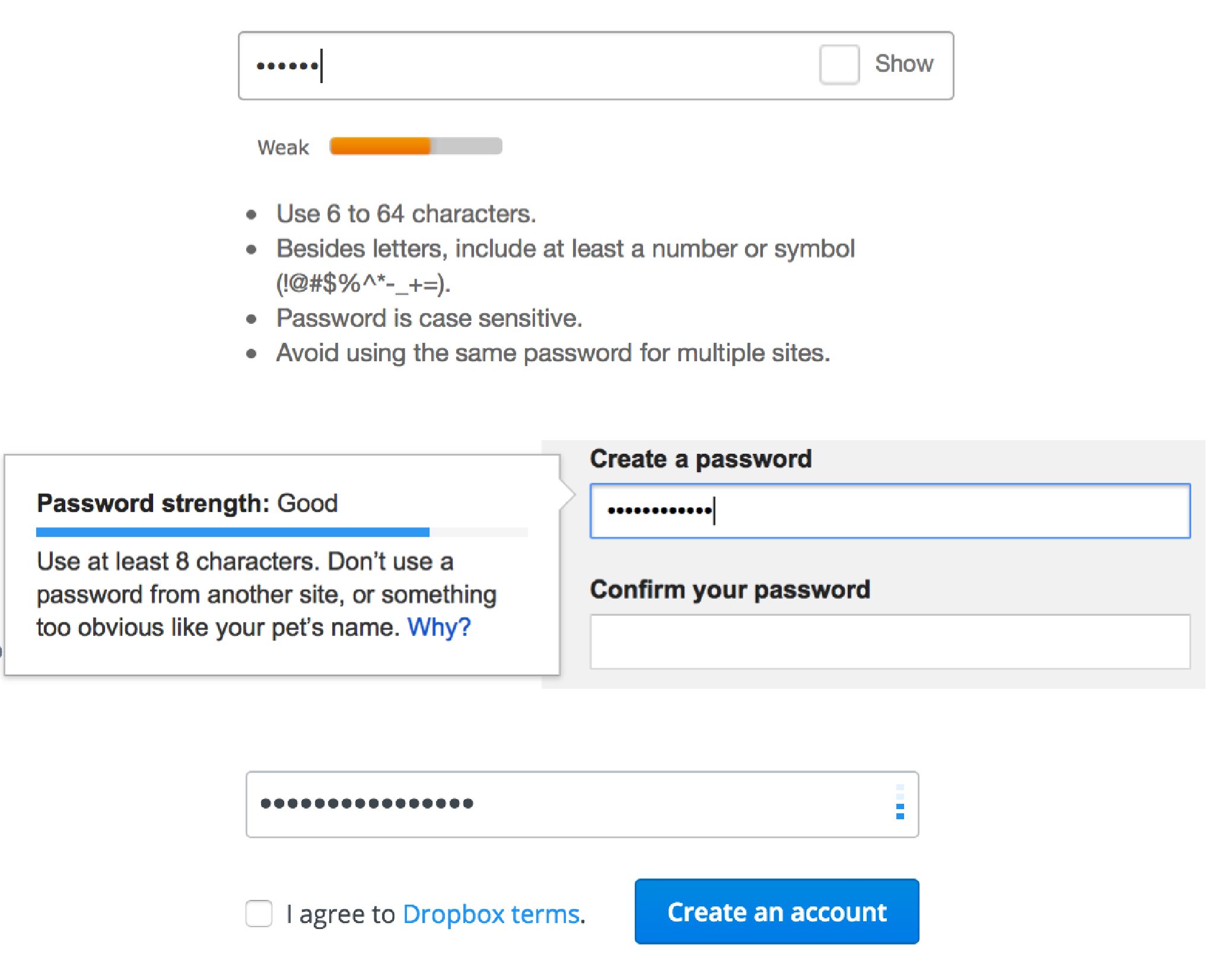
• Reviewing helps identify gaps like short passwords, no expiration, or lack of complexity.

Example: If the policy says “passwords must be 6 characters,” that’s too weak. Modern standards recommend 12+ characters with mixed types.



**Step 2: Password Strength Assessment**





Here, you’re testing how strong the actual passwords are — not just what the policy says.

How to do it:

• Use sample passwords (not real ones from users — keep it ethical).

• Tools like Security.org Password Checker estimate how long it would take to crack a password.

Why it matters:

• Even with a good policy, users may choose weak passwords like sagar123 or Sagar123456 .

• This step shows the real-world risk.

Example: A password like S@g@r may look complex but is still predictable and commonly used — attackers know this.

**Step 3: Recommendations**

This is where you apply your cybersecurity knowledge to improve the situation.

What to include:

• Length: Minimum 12–16 characters

• Complexity: Must include uppercase, lowercase, number, symbol

• Expiration: Change every 90–180 days

• Reuse restriction: Don’t allow reuse of last 5 passwords

• MFA: Add multi-factor authentication for sensitive systems

• Education: Teach users why password hygiene matters

Why it matters:

• A policy is only effective if users understand and follow it.

• MFA adds a second layer of protection even if the password is compromised.

Example: You might recommend using password managers like Bit warden or LastPass to store complex passwords securely.