
Who Owns Your Interview Task? Understanding Your Rights as a Candidate

One of the questions I keep coming back to is simple: who actually owns the work I submit during an interview process? The answer is not always as clear as it should be.

When a candidate is asked to produce an audit, a strategy document, a deck, or a written plan, that work can have real value. Naturally, that raises the question of ownership.

From what I have seen, many candidates assume that because the work was created for an interview, the company automatically owns it. That is not necessarily true.

The legal grey area

In most cases:

- You retain ownership of your work
- Unless you sign an agreement transferring rights

The difficulty is that enforcement in practice is much harder than the theory. Even if you are legally in the right, that does not make misuse easy to prove or challenge.

Why this matters

Organisations treat intellectual property as a serious business asset. That makes sense, because ideas, analysis, frameworks, and strategic recommendations all carry economic value.

That is exactly why this matters to candidates as well. We are often expected to share valuable work without the same level of protection or control that companies would normally apply to their own internal documents.

The practical reality

Even if I legally own my work:

- Proving misuse is hard
- Taking action is costly

- Evidence is often limited

That is the part people do not talk about enough. Ownership on paper is important, but if the file has already been downloaded, forwarded, or reused, the practical options can be limited.

A prevention-first approach

That is why I think it makes more sense to focus on prevention rather than relying on legal protection later. In practice, that means:

- Control how your work is accessed
- Limit distribution
- Maintain visibility

Using TaskLock to protect ownership

TaskLock helps shift that balance by letting candidates:

- Restrict access to named viewers
- Log activity
- Revoke access

For me, that is the more useful model. It moves the focus away from reactive enforcement and towards proactive control.

Conclusion

Ownership matters, but control matters more. The best protection is reducing the chances of misuse in the first place rather than trying to fix the problem afterwards.

Start using TaskLock