IDENTITY CHECK LOG · TEMPLATE · AS OF NOVEMBER 2026

Contract Engineer Identity Verification Checklist

By Kris Drouet, Engineering Executive, in partnership with KORE1. Twenty-two checks in five groups to run before a remote contract engineer gets a laptop or a login.

Contract engineer	Role and systems they will touch	Hiring manager
Security contact	**Interview date**	**Planned start date**

HOW TO READ A LINE — **Tick it** when the check is done and logged · **FBI, Okta, KnowBe4** where the check comes from · **Our practice** a check we add

1 Live video controls

Is the face on the call a real face, and the same one every time?

CHECK	WHAT TO DO	LOG THIS	RUN BY
V1 **Camera on, background in view, no filters** FBI and Okta	Make video a condition of the interview. Ask them to drop any virtual background or filter and keep the camera on for the whole call.	Video on for the full call, background visible	**Hiring side**
V2 **A hand waved across the face** FBI	Ask them to wave a hand slowly in front of their face. The FBI says it may make AI-generated video malfunction, so watch the edges of the face and the hand.	Face stayed intact when the hand crossed it	**Hiring side**
V3 **The camera pointed out a window** FBI	Ask them to point the camera out a window, then ask about what you can see, the weather or the time of day. It should fit the place they say they are.	The view matches the place they claim	**Hiring side**
V4 **The same person at every round** FBI and Okta	With their consent, save a still from the first call and compare it with each later call. Okta tells hiring teams to look for a candidate swapped out between rounds.	Still from round one compared with later calls	**Hiring side**
V5 **A question about where they live or studied** FBI	Ask for a detail a local or a graduate knows without searching, such as a street, a campus habit or a good lunch spot near the school.	Answer fits the place they claim	**Hiring side**

2 Document checks

Does one real person own every name on the paper?

CHECK	WHAT TO DO	LOG THIS	RUN BY
D1 **A government ID held next to the face** Our practice	Ask them to hold a current photo ID beside their face on camera. Compare the photo, the name and the date of birth with the person you see.	ID type and the date you saw it, no number kept	**Hiring side**
D2 **The ID authenticated by an accredited service** Okta	Run the document through an accredited third-party identity service. A good fake passes a human glance.	Service result and date saved	**Hiring side**

D3 **Name, photo and contact details agree everywhere** FBI	Line up the ID, the resume, the professional profile, the portfolio and the payment account. Look for typos and the name spelled two ways.	Sources compared, any difference explained	**Hiring side**
D4 **Past employers and schools confirmed directly** FBI	Contact the company and the school yourself. Do not rely on a letter or a link the candidate sends.	Who you reached, how, and when	**Hiring side**
D5 **A clear background check tied to the face you saw** KnowBe4	A check clears a name and a number. Confirm that the name on the report is the name on the document shown on camera.	Report name matches the document shown	**Hiring side**

3 Device and geolocation consistency

Is the laptop where the person says they are?

CHECK	WHAT TO DO	LOG THIS	RUN BY
G1 **The laptop ships only to the address on the ID** FBI	Send equipment to the address on the identification documents. If they ask for a different one, require more documentation first.	Ship-to address matches the ID, or extra documents on file	**Security side**
G2 **The stated location checked against IP and time zone** Okta	Cross-check where they say they are with the login location, including VPN detection, and with the hours they actually work.	Login location and work hours fit the claim	**Security side**
G3 **Remote access tools blocked before the laptop ships** FBI	Limit remote desktop software and local admin rights. The FBI also suggests watching for tools that run several audio and video calls at once.	Endpoint shows no remote access software	**Security side**
G4 **No access until the background check clears** FBI and Okta	Open nothing until the check is complete, then give the least access the work needs. Contract workers start with the smallest set.	Access request shows scope and the date checks finished	**Security side**

4 Reference callbacks

Did someone you found yourself really work with this person?

CHECK	WHAT TO DO	LOG THIS	RUN BY
R1 **A reference reached through the main switchboard** Okta	Find the company's main number yourself and ask for the reference by name. Do not use the number on the resume.	Number you found, who answered, when	**Hiring side**
R2 **A corporate email address, not free webmail** Okta	Ask for a reference with a company address and confirm it matches the company's own domain. A free webmail address is a flag.	Address and domain checked	**Hiring side**
R3 **A question only a colleague could answer** Our practice	Ask what the person worked on, who they reported to and what the team looked like. A real colleague answers without effort.	Answers match the resume	**Hiring side**
R4 **No reused phone numbers, emails or resume text** FBI	Search your applicant records for the same phone number, email address or resume wording. Treat a voice-over-IP number as a reason to look harder.	Search run, no matches or matches explained	**Hiring side**

5 First-week anomalies

Does anything in week one look like someone else is doing the work?

CHECK	WHAT TO DO	LOG THIS	RUN BY
W1 **Several IP addresses on one account** FBI and Okta	Watch for many logins to one account in a short time from different IP addresses, and for off-hours logins from places that do not fit.	Login report reviewed on days 1 to 5	**Security side**
W2 **A late change of address or payment details** FBI	Flag a new shipping address, a new bank account or a new payment platform during onboarding. The FBI also warns about pay in virtual currency.	Any change flagged and verified again	**Hiring side**
W3 **Remote connections or code leaving for personal accounts** FBI	Watch network logs and browser sessions for remote connections, remote desktop software and code copied to personal cloud or repository accounts.	Alerts reviewed, none open	**Security side**
W4 **Day one matches the interview** FBI	Ask for a camera-on check-in on the first morning. Compare it with the still you saved at the interview.	Day one still compared with the interview still	**Hiring side**

READY FOR ACCESS

Hiring side

I ran the checks on this side and logged what I saw. Signature and date.

Security side

I checked the device, the location and the access and logged what I saw. Signature and date.

Access opened by

Both signatures are above, so access can open. Signature and date.

Read this too. A checklist template, not legal advice or a security audit. Run the same checks on every candidate, keep as little personal data as you can, and ask counsel about state rules on biometric data and ID copies before you store anything. The reasoning behind each group is at kore1.com/contractor-identity-verification-checklist/.