Vendor Due-Diligence & Contract Controls

Requires evidence and enforceable contractual controls before purchase, renewal, or material model change for employment AI vendors.

SIMULATED OPERATING DOCUMENT

Prepared for a fictional employer using synthetic systems and synthetic applicant data. This document is a governance demonstration, not legal advice.

1. Go / no-go due diligence

Domain	Due-diligence question	Go / no-go evidence
Model purpose and limits	What exactly does the system predict, rank, classify, infer, summarize, or automate? What uses are unsupported or prohibited?	Documentation complete and consistent with client use
Feature/data disclosure	Which raw and derived features affect output? Which data are collected, inferred, purchased, or obtained from third parties?	No undisclosed sensitive/proxy inputs
Validation evidence	What evidence supports job relevance for the intended job family and use?	Evidence is specific enough to assess intended use
Adverse-impact testing	What group outcome tests were run, on which population, with which method and limitations?	Underlying tables/methodology available under NDA if needed
Disability/accessibility	How was interface and assessment behavior tested for people with disabilities and alternative formats?	Accessible flow + accommodation handoff supported
Human oversight	Can employer configure no-auto-reject, override, explanation tags, review queues, and audit logs?	Meaningful review technically possible
Model changes	How are model/version/feature updates communicated and controlled?	Advance notice + version lock / approval gate
Data use	Does vendor train or improve models using client/candidate data?	No secondary use without explicit written approval
Security/privacy	Encryption, access controls, incident response, subprocessors, deletion, data location?	Meets enterprise standards
Auditability	Can employer or independent auditor access evidence needed for legal/governance review?	Contractual audit/cooperation rights
Incident history	Known discrimination, accessibility, security, privacy, or material model incidents?	Transparent disclosure and remediation evidence
Exit	Can data, models/config, logs, and records be exported/deleted at termination?	Documented exit and deletion process

2. Contract control matrix

Control	Requirement	Evidence / contract artifact
Scope limitation	Vendor may process candidate data only for documented, approved employment use.	Contract clause + SOW
No secondary model training	No use of client/candidate data to train general models without written opt-in.	DPA / AI addendum
Feature disclosure	Vendor discloses material input and derived feature categories.	Technical schedule
Prohibited features	Emotion/personality/protected-trait inference disabled and contractually barred for this deployment.	Config evidence + clause

Control	Requirement	Evidence / contract artifact
Validation cooperation	Vendor provides methodology, limitations, and documentation needed for job/impact review.	Evidence package
Bias audit cooperation	Vendor supports employer/independent auditor with necessary data and calculation inputs.	Audit clause
Accessibility	Vendor maintains accessible interface and supports alternative formats / accommodation workflows.	Accessibility representation + test evidence
Human review controls	No forced auto-reject; employer can override, pause, and export audit trail.	Product configuration + clause
Change notification	Advance notice before material model, feature, data-source, threshold, or subprocessor change.	30-day notice clause or negotiated equivalent
Version control	Employer can identify version used for each decision and block unapproved version.	Version log
Incident notice	Prompt notice of discrimination, privacy, security, accessibility, or material model issue.	Incident SLA
Audit rights	Employer or qualified independent assessor may review relevant controls/evidence.	Audit clause
Data retention	Retention schedule aligned to employer policy/legal requirements.	DPA schedule
Deletion	Verified deletion after retention / termination, subject to legal hold.	Deletion certificate
Subprocessors	Advance list and change notice; flow-down obligations.	Subprocessor schedule
Security	Encryption, RBAC, logging, vulnerability/incident controls.	Security exhibit
Confidentiality of audit data	Protected-class audit data not exposed to operational users or reused.	DPA + technical control
Records export	Decision logs, score/version, explanations, override records exportable.	Exit plan
Regulatory cooperation	Vendor supports lawful investigations, notices, audits, and documentation requests.	Cooperation clause
Indemnity / allocation	Commercial allocation reviewed by Legal; does not replace employer controls.	Negotiated contract
Termination / suspension	Employer can suspend affected feature or terminate for material governance breach.	Termination clause

3. Renewal and model-update gate

- No auto-renewal of a high-risk tool without current AIA and monitoring review.
- No material model update enters production until version-specific impact/validation review is complete.
- Vendor marketing terms such as “bias-free,” “objective,” or “validated” are treated as claims requiring evidence, not as control evidence themselves.
- If vendor cannot provide necessary documentation because of proprietary constraints, Governance determines whether the residual risk is acceptable; lack of transparency can itself block deployment.