Monitoring, Incident & Remediation Plan

Keeps employment AI governance active after launch through metrics, triggers, incident response, pause authority, corrective action, and annual reassessment.

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. Monitoring dashboard

KPI / KRI	Cadence	Trigger	Required action
Selection-rate / impact-ratio by approved audit group	Monthly pilot; quarterly steady state	Any group <0.80 preliminary screen or material trend deterioration	Validate data; Legal/Validation review; pause if severe
Intersectional selection-rate outliers	Monthly pilot	Large practical gap or repeated low-rate subgroup	Deep dive; feature/workflow analysis
Score distribution drift	Monthly	PSI / distribution shift above approved threshold	Investigate data/model change
Parser failure / correction rate	Monthly	>2% overall or material group/path difference	Pause affected formats; vendor remediation
Recruiter override rate	Monthly	>20% or 2x baseline; directionally concentrated	Review tool usefulness / automation bias
Screen-out second-review reversal rate	Monthly	>10%	Threshold/model/rubric investigation
Accommodation requests affected by tool	Monthly	Any unresolved request; increasing pattern	Accessibility review
Candidate AI questions / complaints	Monthly	Spike >2x trailing baseline or discrimination allegation	Incident triage
Reconsideration reversal rate	Monthly	>10% or repeated same reason	Root-cause analysis
Response time to recourse	Monthly	>10 business days target	Capacity / process remediation
Unapproved model/version events	Continuous	Any	Immediate stop-use
Vendor material-change notices	Per event	Change affects features/data/model role	Reassessment gate
Data retention/deletion exceptions	Quarterly	Any overdue deletion without legal basis	Privacy remediation
Job profile changes	Per requisition / quarterly	Material qualification change	Revalidate mapping
Annual reassessment completion	Annual	Overdue high-risk assessment	Suspend approval until completed

Authority notes: R5.

2. Incident severity and authority

Severity	Example	Authority / response
SEV-1 Critical	Confirmed automated rejection without required review; credible systemic discrimination; protected/sensitive data used as prohibited input; major privacy/security incident	Immediately pause system/feature. Legal + Executive Sponsor + AI Governance lead incident. Preserve records; notify parties/regulators as counsel determines.
SEV-2 High	Material adverse-impact shift; accommodation process failure; unapproved model change; repeated wrongful screen-outs	Pause affected workflow or decision step within hours; complete investigation and corrective plan before restart.

Severity	Example	Authority / response
SEV-3 Moderate	Rising complaints, override spike, parser error cluster, missed SLA	Open corrective action; enhanced monitoring; escalate if threshold persists.
SEV-4 Low	Documentation defect, isolated user error without candidate harm	Correct, coach, document in issue log.

3. Incident response procedure

1. Detect and log: capture tool/version, job, candidate population, timeline, decision pathway, reporter, and suspected harm.

2. Contain: suspend automated actions or affected feature if continued use could create additional harm.

3. Preserve: retain relevant decision logs, model/version records, notices, audit datasets, vendor communications, reviewer notes, and access logs.

4. Assess: Legal, HR, Privacy, Security, Validation, and EEO/DEI determine affected people, legal obligations, root cause, and severity.

5. Remediate: correct candidate decisions where possible; provide reconsideration/alternative process; change model/features/workflow; retrain reviewers; update notices or contracts.

6. Verify: re-test before restart and document go/no-go decision.

7. Learn: update risk register, controls, monitoring thresholds, and vendor requirements.

4. Consolidated risk register

Risk	Scenario	Likelihood	Impact	Rating	Treatment	Owner	Status
R-01	ResumeRank disparity signal	High	High	Critical	Feature removal + re-test; no production baseline	Validation Lead	Open
R-02	Insufficient job-validation evidence	High	High	Critical	Job analysis + criterion validation plan	HR + I/O / Validation	Open
R-03	Disability screen-out / inaccessible parser	Med	High	High	Accessibility QA + alternative process + accommodation handoff	HR + Accessibility	Open
R-04	Vendor material update without review	Med	High	High	Contract notice + version lock + release gate	Procurement + Security	Open
R-05	Automation bias / weak human review	Med	High	High	Structured rubric, override authority, screen-out review, metrics	Talent Acquisition	Open
R-06	NYC notice / bias-audit failure	Low-Med	High	High	Jurisdiction gate; audit/notice checklist; evidence retention	Legal + Recruiting Ops	Open
R-07	Candidate recourse delays	Med	Med	Moderate	2-day acknowledgment / 10-day target; second-review queue	Candidate Experience	Open
R-08	Secondary vendor data use	Low-Med	High	High	No-training clause; retention/deletion controls	Privacy + Procurement	Open
R-09	Prohibited video emotion POC data remains	Low	High	Moderate	Verify deletion and feature disablement	Privacy + Innovation	Open

Risk	Scenario	Likelihood	Impact	Rating	Treatment	Owner	Status
R-10	Monitoring degrades to annual-only review	Med	High	High	Monthly dashboard; committee review; trigger reassessment	AI Governance	Open

5. 90-day remediation roadmap

Timing	Priority action	Evidence of completion
Days 0-30	Freeze baseline EMP-AI-01 launch; disable risky features; close prohibited EMP-AI-08 POC; finalize Charter and inventory ownership.	Change tickets, deletion confirmation, approved Charter, owner attestations
Days 0-30	Implement human-review, accommodation, alternative-process, reconsideration, and audit-log workflow.	Workflow configuration, training, SLA dashboard
Days 31-60	Complete job analysis, dataset/feature assessment, parser accessibility QA, mitigated fairness re-test, and validation plan.	Signed assessments, test report, job-analysis evidence
Days 31-60	Complete vendor contract addendum for model changes, audit access, data use, retention/deletion, incident notice, and exit.	Executed addendum
Days 61-75	Complete jurisdiction/notice controls, including NYC audit/public-summary/notice workflow where applicable.	Compliance checklist, notice templates, audit record
Days 76-90	Governance Committee go/no-go for monitored pilot. If go: launch 90-day limited pilot with monthly dashboard and pre-defined pause triggers.	Decision record, pilot charter, dashboard, rollback plan

6. Annual reassessment questions

- Is the original business need still valid, and can a simpler method achieve it?
- Has the model, feature set, data source, threshold, or vendor changed?
- Do subgroup outcomes, complaints, overrides, or recourse reversals indicate new harm?
- Is job-validation evidence still current for the roles and populations in use?
- Are accommodation and alternative-process routes actually functioning?
- Are notices, retention terms, and applicable bias-audit/public-summary obligations current?
- Should the system be narrowed, paused, replaced, or retired?