**Frontend Developer Interview Scorecard**

Candidate Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role Interviewed For: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Interviewer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **Dimension** | **Guidance** | **Score (1–5)** |
| System Architecture | 1-2: Shows limited understanding of system components; proposes fragile or unscalable designs.
3: Designs reliable services with clear component boundaries and reasonable scalability plans.
4: Architects for failure, capacity, and cost; defines interfaces and scaling strategies.
5: Leads architecture decisions across teams and drives long-term system evolution and trade-offs. |  |
| CI/CD & Automation | 1-2: Relies on manual deployments and ad-hoc scripts with no repeatable pipelines.
3: Implements pipelines that build, test, and deploy reliably for a service.
4: Creates reusable, secure pipelines across services with fast feedback and rollbacks.
5: Defines organization-wide CI/CD standards and automates release orchestration and canaries. |  |
| Infrastructure as Code | 1-2: Performs manual provisioning or uses undocumented scripts without versioning.
3: Uses IaC to provision and update environments with basic modules and state handling.
4: Builds modular, testable IaC with drift detection and environment parity.
5: Designs and enforces IaC patterns and promotes reusable module libraries across teams. |  |
| Observability & Monitoring | 1-2: Lacks metrics, structured logs, or alerts and is purely reactive.
3: Implements metrics, structured logs, and basic alerts for services.
4: Designs dashboards, SLOs, and alerting with noise reduction and routing.
5: Introduces system-wide SLO strategy and drives proactive observability improvements. |  |
| Security & Compliance | 1-2: Ignores security hardening and exposes credentials or overly permissive access.
3: Applies standard controls: least-privilege IAM, secret management, and patching.
4: Integrates security scans into pipelines and performs threat modeling and remediation.
5: Defines organization-level security practices and drives compliance audits and fixes. |  |
| Incident Response & Troubleshooting | 1-2: Slow to diagnose, escalates without clear steps, and avoids postmortems.
3: Diagnoses incidents, follows runbooks, and resolves within agreed SLA.
4: Leads incident response, isolates root cause, and documents remediation.
5: Improves playbooks, reduces MTTD/MTTR, and drives closure of systemic fixes. |  |
| Collaboration & Communication | 1-2: Poor communication; misses handoffs and creates friction with stakeholders.
3: Communicates clearly with engineers and documents changes and runbooks.
4: Proactively aligns stakeholders, negotiates trade-offs, and mentors peers.
5: Drives cross-team initiatives, influences roadmap, and coaches other teams in practices. |  |

 **Overall Evaluation**

**Strengths Observed:**

**Concerns / Weaknesses:**

**Recommendation (Yes / No / With Reservations):**

**Final Score (Avg / Weighted):**