Document Version: 1.0
Jim Venuto

1) Policy statements (for the PoC form)

- **Data: Synthetic/anonymized only.** No production data, no PHI/PII at any time in Phase 0.
- **Identity:** SSO/IDP federation targeted; MFA enforced on all admin identities.
- **Scope:** Minimal attack surface; SFTP-only for transfer; no Aspera/VPN/scheduler in Phase 0.
- **Security tools:** Posture checks and workload protection to be evaluated; deeper controls land in the LRI-owned account as the program transitions to paid scope.
- **Duration:** PoC window sized at ~90 days with defined budgets and stop/cleanup hygiene.

2) Required controls by layer

A. Account & Identity

1. **MFA** required for Admin/Editor roles.
2. **SSO/IDP federation** (SAML/OIDC) with CC IT; IBMid fallback allowed only for PoC admins.
3. **Access groups & least privilege:**
    - LRI-Phase0-Admins (Jim + designated CC/IBM)
    - LRI-Phase0-Researchers (non-admin)
4. **Scoped API keys** per persona; rotate on handoff; no key sharing.
5. **Resource groups & tags** for chargeback/segregation: org=LRI, phase=0, lab=<name>, data=synthetic. (Child-account vs tagging model is under discussion; tags are required either way.)

B. Network (VPC)

1. **VPC with two subnets** (separate AZs).

2. **Security groups**: deny-by-default; inbound SSH/SFTP (22) from approved CC/LRI CIDRs only; no 0.0.0.0/0.
3. **Public gateway** minimal path for Phase 0; bastion is optional for private-only access.
4. **Name/port discipline**: close all unused ports; ephemeral outbound allowed; document any exceptions.
5. **(Optional)** VPC flow logs enabled to COS for forensics.

C. Compute (GPU VSI)

1. **OS hardening**: key-only SSH; disable root SSH; update packages; minimal packages; time sync.
2. **SFTP** via OpenSSH (internal-sftp/chroot recommended for lab user), log to syslog.
3. **Secrets hygiene**: no creds on disk; no tokens in shell history.
4. **Driver/toolchain** pinned to profile; verify accelerator (e.g., nvidia-smi) before data ingress.
5. **(Optional)** Agent-based **Workload Protection** for malware/vuln/runtime checks (trial in PoC account or enable in LRI account).

D. Data Protection

1. **At rest**: default encryption on Block volumes and COS.
2. **In transit**: SFTP over SSH only; prohibit plaintext protocols.
3. **Key management**: PoC can use provider-managed keys; Key Protect/HPCS evaluated for Phase 1+.
4. **COS access**: private bucket; no public reads; per-lab prefixes or buckets; lifecycle (optional 30-day expire) for non-prod.
5. **Anonymized data** used for any "production-like" tests; verify anonymization with LRI governance.

E. Logging, Monitoring, & Cost Guardrails

1. **Audit logs** at account level (create/modify/delete events) retained for the PoC window.

2. **Budget alerts**: threshold emails to Jim + CC IT; tags filter by lab. (Budget oversight was a key huddle theme.)
3. **Runbook evidence** capture: provisioning, SFTP checksums, accelerator check, COS put/get, alert screenshots.
4. **Idle control**: no GPU VSI left running idle > 8 hours; cleanup after each exercise.

3) Step-by-step hardening runbook (Phase 0)

Account/IAM

1. Create RG LRI-Phase0; enforce MFA; set SSO (when available).
2. Create access groups; attach least-privilege policies; add users.
3. Create per-persona API keys; store securely; rotate on handoff.

Network

4) Create VPC + two subnets + public gateways.
5) Create SGs: sg-ssh-inbound (TCP/22 from approved CIDRs), sg-default-egress.
6) Upload SSH key; no passwords; optional bastion if private-only path is required.

Compute

7) Provision **GPU VSI** per lab (and one Dev/MVP), attach boot + data volume.
8) Harden SSH (PermitRootLogin no, PasswordAuthentication no, MaxAuthTries 3).
9) Enable **SFTP** and log; create per-lab user if not using admin key; verify accelerator.

Storage

10) Create COS instance; bucket per lab **or** shared bucket with per-lab prefixes; block all public access.
11) (Optional) Lifecycle rule for non-prod retention (e.g., 30 days); set tags.

Observability/Cost

12) Enable audit and (optional) flow logs; budget alert policy based on tags; test the alert.
13) Establish cleanup checklist (detach/delete volumes, delete VSIs/IPs, confirm zero orphans).

Evidence package

14) Drop screenshots/logs into Box (IAM policies, SGs, SSH config, SFTP checksum, COS object list, budget alert, pre/post inventories).

4) RACI (short form)

Area	LRI/Researcher	CC IT (Santino)	IBM (Jim/Roderick)
Data (synthetic only)	Provide/test	Approve policy	Verify in runbook
IAM (roles/MFA/SSO)	Use	Configure SSO	Define groups/policies
VPC/SGs	Use	Approve CIDRs	Build/runbooks
GPU VSI hardening	Follow SOP	Review	Implement baseline
COS & retention	Use	Approve	Configure baseline
Audit/Budget	Review	Receive alerts	Configure/test
Evidence	Capture	Co-sign	Collate & deliver

5) Hand-off & paid-scope trigger

- At PoC close, re-deploy in the LRI-owned account via Schematics, copy datasets/results to LRI COS, and apply LRI security/compliance policies (e.g., CBR/Private endpoints, BYOK/HPCS, formal vulnerability mgmt, bastion-only, org-wide guardrails). That transition marks the conversion to paid support/services.

6) What to attach to the PoC application (evidence checklist)

- **Screenshots:** MFA on; Access Groups; SG rules; VPC/subnets; SSH config; SFTP checksum; COS bucket ACLs; budget alert email; pre/post cleanup inventories.
- **Runbooks:** UI, CLI, and Schematics; start/stop/terminate; data hygiene & checksum steps.
- **Attestations:** “Synthetic-only” confirmation for each lab.