**Technical / Ops Procedures – Access Control Summary**

**Purpose:**  
To maintain a clear and current record of all system-level access during the incident response period. This includes admin credentials, service accounts, login logs, and any known access changes made during containment or investigation.

**When to Use**

• During an active incident where access controls are adjusted or monitored  
• Post-incident to review unauthorised access attempts or changes  
• As part of closure or audit reporting

**Active Admin Credentials**

| **Username** | **System / VM** | **Role/Scope** | **Notes** |
| --- | --- | --- | --- |
| admin | All VMs | Root shell access | Primary access via SSH |
| ops\_user | Physical Ops VM | Docker/service ops | Limited sudo rights |
| vendor\_ro | Vendor Gateway | Read-only | Contractual limits apply |
| tech\_monitor | AIS & GPS Containers | Log access only | No write permissions |

Access keys and passwords stored in secure /creds/ directory on Coordination VM (read-only).

**Temporary or Elevated Access Granted**

| **Timestamp** | **Account** | **Change Type** | **Authorised By** | **Notes** |
| --- | --- | --- | --- | --- |
| 2025-06-04 10:35 | ops\_user | Temporary sudo | Tech Lead | Needed for node isolation |
| 2025-06-04 11:20 | admin (GPS VM) | Password changed | Coordinator | Suspected key reuse |

**Recent Access Logs to Review**

• SSH login records:  
cat /var/log/auth.log | grep sshd

• Last login overview:  
last -a | head -n 10

• Failed attempts:  
grep -i fail /var/log/auth.log

• Sudo usage:  
grep sudo /var/log/auth.log

• Container access:  
docker logs [container\_id]

**Access Cleanup Post-Incident**

• Revert temporary permissions and sudo grants  
• Rotate shared credentials  
• Remove unnecessary SSH keys:  
rm ~/.ssh/unknown\_key.pub  
• Confirm permissions on /creds/ directory  
• Log changes and hash credential files if retained for audit

**Owner:** Ops Lead  
**Reference:** TECH-06  
**Version:** 1.0  
**Approved by:** Cyber-Ops Coordination Cell