SOUTHGATE TERMINAL

## Port Operations Security Documentation

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

---

Access Control Incident Scenarios and Detailed Procedures

Purpose

This section provides specific scenarios and detailed procedures for access control incidents that may occur during cybersecurity events, ensuring appropriate response to various access-related security concerns.

Common Access Control Incident Scenarios

Scenario 1: Service Account Authentication Failures Situation: Critical service accounts (svc_gantry, svc_crane) failing authentication

Immediate Actions (0-5 minutes): - [ ] Impact Assessment: Identify all systems using the failing service account - [ ] Operations Notification: Alert operations team to potential automated system failures - [ ] Account Status Check: Verify account lock status, password expiration, permissions - [ ] Workaround Implementation: Switch affected systems to manual operation if safe

Investigation Steps: 1. Authentication Log Analysis: - Check authentication server logs for failure patterns - Review account activity prior to failure - Identify any unusual access attempts or patterns

2. System Dependency Mapping:
    - Document all systems dependent on failing service account
    - Assess operational impact of each system failure
    - Prioritize restoration based on operational criticality

3. Security Assessment:
    - Determine if failure is technical or security-related
    - Check for evidence of credential compromise
    - Review concurrent security events

Resolution Process: - [ ] Account Recovery: Reset/unlock account following security procedures - [ ] Credential Update: Update credentials in all dependent systems - [ ] System Testing: Verify restored functionality of all dependent systems - [ ] Enhanced Monitoring: Monitor account for 24 hours for stability

Scenario 2: Unauthorized Access Attempts Situation: Multiple failed login attempts from external sources detected

Immediate Actions (0-10 minutes): - [ ] Source Analysis: Identify IP addresses and geographic locations of attempts - [ ] Attack Pattern Recognition: Determine if brute force, credential stuffing, or targeted attack - [ ] Account Protection: Lock targeted accounts if necessary - [ ] Network Protection: Implement IP blocking for malicious sources

Investigation Procedures: 1. Attack Analysis: - Document attack vectors and methods used - Identify accounts being targeted - Assess whether any attempts were successful

2. Intelligence Gathering:
    - Cross-reference attacking IPs with threat intelligence
    - Check for known attack campaigns or threat actors
    - Assess potential for escalation or persistence
3. Impact Assessment:
    - Determine if any accounts were compromised
    - Assess potential access to sensitive systems or data
    - Evaluate need for broader security measures

Response Actions: - [ ] Defensive Measures: Enhance monitoring, implement rate limiting - [ ] User Notification: Alert affected users to potential targeting - [ ] Evidence Preservation: Collect logs and evidence for potential investigation - [ ] Incident Escalation: Escalate to appropriate authorities if required

Scenario 3: Privilege Escalation Detection Situation: Evidence of unauthorized privilege escalation or administrative access

Immediate Actions (0-5 minutes): - [ ] Account Identification: Identify accounts with suspicious privilege changes - [ ] Access Revocation: Immediately revoke elevated privileges - [ ] Session Termination: Terminate all active sessions for affected accounts - [ ] Change Documentation: Review all recent privilege changes and authorizations

Investigation Process: 1. Privilege Audit: - Review all accounts with administrative privileges - Verify authorization for all privilege grants - Identify any unauthorized or unexplained changes

2. Activity Analysis:
    - Review activities performed with elevated privileges
    - Check for unauthorized system changes or data access
    - Assess potential damage or compromise
3. Authorization Verification:
    - Verify legitimacy of all recent privilege changes
    - Review authorization documentation and approvals
    - Identify any gaps in authorization processes

Containment Actions: - [ ] Privilege Reset: Reset all accounts to minimum required privileges - [ ] System Verification: Verify integrity of critical systems and data - [ ] Enhanced Monitoring: Implement additional monitoring for privilege usage - [ ] Process Review: Review privilege management processes for gaps

Scenario 4: Insider Threat Indicators Situation: Access patterns suggesting potential insider threat activity

Immediate Actions (0-15 minutes): - [ ] Activity Documentation: Document suspicious access patterns - [ ] Risk Assessment: Assess potential for data exfiltration or sabotage - [ ] Legal Consultation: Consult with legal team on investigation approach - [ ] Discrete Monitoring: Implement enhanced monitoring without alerting subject

Investigation Coordination: 1. Legal Framework: - Ensure investigation complies with employment law - Coordinate with HR on personnel matters - Consider privacy implications of monitoring

2. Technical Investigation:
    - Review detailed access logs and patterns
    - Analyze data access and system usage
    - Look for evidence of policy violations
3. Risk Mitigation:
    - Assess need for immediate access restrictions
    - Consider data protection measures
    - Evaluate operational security implications

Response Framework: - [ ] Evidence Collection: Preserve digital evidence following legal requirements - [ ] Access Management: Modify access as appropriate while maintaining operational needs - [ ] Stakeholder Coordination: Coordinate with HR, Legal, and Executive teams - [ ] Incident Documentation: Maintain detailed records for potential disciplinary or legal action

Access Control Recovery Procedures

Emergency Access Provision When Normal Access Control Systems Fail:

Immediate Emergency Access (0-15 minutes): 1. Emergency Account Activation: - Activate pre-configured emergency administrative accounts - Use secure emergency credential distribution process - Document all emergency access granted

2. Manual Verification Process:
   - Implement manual identity verification procedures
   - Use alternative authentication methods (phone verification, in-person)
   - Require dual authorization for sensitive access
3. Temporary Access Management:
   - Grant minimum necessary access for critical functions
   - Set automatic expiration for all temporary access
   - Implement enhanced monitoring of emergency access usage

Access Control System Restoration Recovery Process for Access Control Infrastructure:

System Assessment Phase: - [ ] Damage Assessment: Evaluate extent of access control system damage - [ ] Backup Verification: Verify integrity of access control backups - [ ] Dependencies Check: Identify all systems dependent on access control - [ ] Recovery Timeline: Estimate time required for full restoration

Restoration Process: 1. Core Infrastructure: Restore authentication servers and databases 2. Account Verification: Verify integrity of all user accounts and permissions 3. System Integration: Restore integration with dependent systems 4. Testing and Validation: Comprehensive testing before full restoration

Post-Restoration Actions: - [ ] Access Audit: Complete audit of all access permissions - [ ] Security Review: Review for any compromise during outage - [ ] Lessons Learned: Document improvements for future incidents - [ ] Enhanced Monitoring: Implement additional monitoring post-restoration

Advanced Access Control Scenarios

Cross-System Access Control Failures Multiple Authentication Systems Affected:

Coordinated Response: - [ ] System Inventory: Identify all affected authentication systems - [ ] Impact Assessment: Assess operational impact across all systems - [ ] Priority Matrix: Prioritize restoration based on operational criticality - [ ] Resource Allocation: Coordinate technical resources across multiple recovery efforts

Third-Party Access Management Vendor or Contractor Access Issues During Incidents:

Vendor Access Review: - [ ] Access Audit: Review all third-party access permissions - [ ] Risk Assessment: Assess security risk of maintaining third-party access - [ ] Communication: Coordinate with vendors on access requirements - [ ] Temporary Restrictions: Implement temporary access restrictions if needed

Documentation and Reporting Requirements

Access Control Incident Documentation Required Documentation for All Access Control Incidents: - Timeline of incident discovery and response - Technical details of access control failures or compromises - Impact assessment on operations and security - Response actions taken and their effectiveness - Evidence collected and preservation methods

Regulatory Reporting Considerations Access Control Incidents Requiring External Reporting: - Unauthorized access to regulated data - Compromise of critical infrastructure access controls - Potential insider threat activities - Cross-border access control incidents

Continuous Improvement

Access Control Incident Analysis Post-Incident Review Process: - Effectiveness of detection capabilities - Response time and coordination efficiency - Technical recovery procedures performance - Process gaps and improvement opportunities

Security Enhancement Recommendations Common Improvements Following Access Control Incidents: - Enhanced monitoring and alerting capabilities - Improved authentication and authorization processes - Better coordination between technical and operational teams - Enhanced training and awareness programs

Success Criteria

- Rapid detection and response to access control incidents
- Effective coordination between technical, operational, and legal teams
- Minimal operational impact from access control failures
- Comprehensive documentation and evidence preservation
- Continuous improvement of access control security posture

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