CHG0030100 — [TITAN] Critical — network on sqlsrv-pyx-banking-prd

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	Assigned
Resource	sqlsrv-pyx-banking-prd	Group	network_operations
Resource type	Microsoft.Sql/servers	Change type	Emergency
Opened	2026-04-22 20:19:22	Closed	2026-04-22 20:19:22
CAB required	Yes	Close code	—

Security Finding

```
SQL Server firewall permits 0.0.0.0-255.255.255.255 on port 1433 — direct database exposure across internet. Violates PCI DSS 1.2.1 and SOX ITGC access controls.
```

Justification

```
Critical: SQL Server firewall permits 0.0.0.0-255.255.255.255 on port 1433 — direct database exposure across internet. Violates PCI DSS 1.2.1 and SOX ITGC access controls.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az sql server firewall-rule delete --resource-group rg-banking-prod-data --server
sqlsrv-pyx-banking-prd --name AllowAllWindowsAzureIps
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT — finding must no longer appear.
5. Close ticket with Successful close_code.
```

Risk & Impact Analysis

```
Risk level: HIGH business risk — active exposure; fix required immediately.
Business impact if unremediated: Potential data exfil, privilege escalation, or compliance breach.
Scope: single resource (sqlsrv-pyx-banking-prd).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: SQL Server firewall permits 0.0.0.0-255.255.255.255 on port 1433 — direct database
exposure across internet. Violates PCI DSS 1.2.1 and SOX ITGC access controls.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of sqlsrv-pyx-banking-prd before change (baseline:
titan-banking-demo-20260422T201922Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
a. TITAN FORGE fires rollback automatically using stored snapshot.
b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.
```

Test Plan

```
1. TITAN SCOUT rescans sqlsrv-pyx-banking-prd immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
```

```
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.
```

Recommended Fix Command

```
az sql server firewall-rule delete --resource-group rg-banking-prod-data --server
sqlsrv-pyx-banking-prd --name AllowAllWindowsAzureIps
```

Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, CIS Azure 6.2
```

AI Close Notes

```
TITAN CONDUIT opened this critical network change request and assigned it to the
banking_compliance group for review. STATE: ASSIGNED — awaiting human action. Per TITAN AI policy
(and Kazmi rule, 2026-04-22), configuration changes are NEVER auto-applied and change tickets are
NEVER auto-closed by TITAN. The assigned group reviews the recommended fix, schedules a
CAB-approved change window, applies the fix manually, validates via SCOUT rescan, and closes this
ticket themselves. TITAN documents and routes — the human owns the change from here.
```