Southern Mutual Bank

51 824 753 556

Network Interconnections Inventory — Payments Switch

Register · synthetic assessor-grade test document

Generated 09 November 2026 · CyberSentien test harness · personalised to Southern Mutual Bank

Register ID	SOU-REG-0233
Version	3.3
Owner	David Okafor (Head of Compliance)
Classification	Internal Use Only
Status	Maintained — current
Last reviewed	20 Oct 2026
Review cycle	Quarterly

1. Purpose

This register records the network interconnections inventory — payments switch maintained by Southern Mutual Bank. It is reviewed on a defined cycle; overdue or expired entries are escalated to the accountable owner and the Executive Risk Committee. It is the inventory of network interconnections and boundary protection devices: every external network and partner connection, the firewall or gateway protecting it, the physical security of the managed interfaces, and the rule that no classified national security system connects directly to an external network.

2. Register entries

Interconnection	External network / party	Boundary protection device	Physical connection controls	Classification	Review
Internet ingress	Cloud service provider	Firewall + IPsec VPN gateway	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	Classified segment — isolated; no direct external connection	Inventory reviewed and network diagram updated 29 Oct 2026

Interconnection	External network / party	Boundary protection device	Physical connection controls	Classification	Review
SWIFT network	Cloud service provider	Next-generation firewall pair, default deny	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 13 Jul 2026
Payments scheme (Mastercard)	Cloud service provider	Private endpoint, firewall, network traffic inspection	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 22 Jun 2026
Cloud provider (AWS) private link	Cloud service provider	Next-generation firewall pair, default deny	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 27 Oct 2026
Regulator secure gateway	Partner network	Private endpoint, firewall, network traffic inspection	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	Classified segment — isolated; no direct external connection	Inventory reviewed and network diagram updated 23 Aug 2026

Interconnection	External network / party	Boundary protection device	Physical connection controls	Classification	Review
Partner API (open banking)	Partner network	Firewall + IPsec VPN gateway	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 24 Jun 2026
Corporate WAN to branches	Regulator	Firewall + IPsec VPN gateway	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 16 Jul 2026
Third-party SOC telemetry feed	Untrusted network	Private endpoint, firewall, network traffic inspection	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 24 Jul 2026
Data centre cross-connect	Regulator	Next-generation firewall pair, default deny	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	Classified segment — isolated; no direct external connection	Inventory reviewed and network diagram updated 22 Oct 2026

Interconnection	External network / party	Boundary protection device	Physical connection controls	Classification	Review
BGP peering (internet routers) — RPKI route origin validation: routes for RPKI-registered IP addresses that are advertised from invalid autonomous systems, or that are longer than allowed, are rejected or deprioritised by the routers that exchange routes via BGP	Partner network	Private endpoint, firewall, network traffic inspection	Managed interfaces protected against unauthorised physical connections: 802.1X port-based network access control, unused switch ports shut, patch panels in locked racks (physical security, physical access logged)	OFFICIAL — no classified national security system is directly connected to an external network without a boundary protection device	Inventory reviewed and network diagram updated 08 Oct 2026

3. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification