

A Regional ISP in
Latin America Secures
Technical Staff
Access and Meets
Data Protection
Compliance
Requirements with
eMudhra SecurePass



Client Overview

The organisation is a regional internet service provider in South America offering broadband and business connectivity services to around 180,000 residential and SME subscribers. The company employs approximately 420 staff across network operations, technical support, customer care, and administration. Operating under the country's data protection framework, the company has been reviewing its internal controls to ensure that access to subscriber data and network management systems meets regulatory requirements.

The Challenge

The company's technical support and network operations staff accessed subscriber management systems, network provisioning tools, and billing platforms using password-only authentication. Under the national data protection law, the company was required to demonstrate that access to systems holding subscriber personal data was appropriately controlled — including the use of strong authentication for staff accessing those systems. An internal compliance review found that the provisioning process for new staff was informal and varied by team, and that access was rarely reviewed or updated when staff moved between roles. Two over-privileged accounts were found during the review — one for a staff member who had been promoted and retained access to their previous role's systems, and one for a contractor whose engagement had ended but whose account remained active. The company's legal team flagged the situation as a potential compliance exposure under the data protection framework.

“Our legal team pointed out that password-only access to subscriber data systems, combined with accounts we couldn't account for, was a potential compliance issue under the data protection law. We needed to fix it before it became a problem.”

Head of IT and Compliance

The Solution

eMudhra deployed SecurePass to address the access management gaps identified in the compliance review. A centralised identity directory was set up, integrating with the company's HR system to automate provisioning and deactivation. The two over-privileged and stale accounts identified in the review were corrected immediately. MFA was enforced using TOTP for all access to subscriber management and billing systems — directly addressing the data protection compliance requirement. SSO was configured for subscriber management, network provisioning, billing, and the HR system, reducing the credential overhead for staff. Role-based access profiles were defined for technical support, network operations, customer care, and administration, with subscriber data access explicitly restricted to roles that required it. A quarterly access review was set up to maintain ongoing compliance with the data protection framework.

Results

MFA was deployed on all subscriber data systems within five weeks. The stale and over-privileged accounts were addressed in the first week. The company's legal team reviewed the deployment and confirmed that the access controls met the data protection framework requirements for systems holding subscriber personal data.

| Metric | Before | After |
|---|--|---|
| MFA on subscriber data systems | Password only; compliance gap | TOTP MFA enforced within 5 weeks |
| Stale and over-privileged accounts | 2 identified; compliance exposure | Addressed in first week; controls in place |
| Provisioning process | Informal; inconsistent across teams | Automated HR-integrated lifecycle management |
| Subscriber data access control | No role restriction enforcement | RBAC restricting data access to authorised roles only |
| Data protection compliance | Potential exposure flagged by legal team | Legal team confirmed controls meet framework requirements |

About eMudhra

eMudhra is a globally trusted provider of digital trust services, offering eSignatures, PKI, Certificate Lifecycle Management, Multi-Factor Authentication, and Identity & Access Management solutions. Licensed by the Controller of Certifying Authorities (CCA), India, eMudhra serves 1000+ enterprises across 40+ countries, helping organisations build secure, compliant, and paperless digital ecosystems.