

## TRANSPORT AUTHORITY 1 – EXECUTIVE COMMITTEE BRIEFING

**SUBJECT:** Legal Contract for Signaling System Support

**BETWEEN:** Transport Authority 1 and NordStadt Signals AG

**CONTRACT VALUE:** €145,000,000 (2024–2029)

**CLASSIFICATION:** TRANSPORT AUTHORITY 1 COMMERCIAL – IN CONFIDENCE

### 1. Overview

This briefing summarises key contractual provisions governing the long-term support, maintenance, and security obligations associated with the Authority's primary signalling systems.

### 2. Key Clauses of Interest

#### 2.1 Section 12.4 – Security Breach Liability

- Liability for security breaches **originating from NordStadt-controlled system backdoors** is capped at **€5,000,000**.
- The Authority is contractually responsible for **60% of all post-breach system-hardening expenditures**, irrespective of source attribution or contributory fault.
- Implication: Exposure for remediation costs may substantially exceed vendor liability in a high-impact incident.

#### 2.2 Section 8.7 – Source Code Escrow

- NordStadt's **full signalling-system source code** is maintained in escrow with **National Bank (Vault A-77)**.
- **Release Conditions:**
  - Formal declaration of NordStadt bankruptcy, or
  - Failure by NordStadt to issue critical-security patches within **30 days** of confirmed notification.
- **Escrow Access Code: NS-ESCROW-8821-ZULU**
  - Note: Access credentials are maintained under Secure Custody Protocols. Executive Committee members may request the validated credential through the Chief Legal Officer under controlled-access procedures.

### 3. Commercial and Operational Implications

- The current liability cap introduces a **potential fiscal imbalance** in a severe breach scenario, particularly if system-wide remediation is required.
- Escrow arrangements provide continuity safeguards but require **strict internal stewardship** of access credentials and activation protocols.

### 4. Recommended Executive Actions

1. Request a legal review of Section 12.4 to evaluate renegotiation pathways for more balanced liability sharing.
2. Confirm that internal custody of escrow credentials adheres to updated secure-storage standards.
3. Direct the CIO and CISO to assess operational risk arising from the liability cap and prepare an impact model for next-quarter reporting.