# Security Overview

Version 1 (Current)

**Effective October 28, 2026**

This Security Overview summarizes how Vybose approaches the security of its services, including Vnique Social Connect. It is provided for information and does not create additional obligations beyond those in our agreements.

## Our approach

Our connection services are designed to handle as little data as possible. We do not retain message content after it is delivered to the Customer's system, except for a temporary hold of up to 24 hours when redelivery is needed. What we do hold, such as access tokens, account identifiers, and connection activity records, is described in our Privacy Policy.

## Safeguards

We maintain reasonable administrative, technical, and physical safeguards designed to protect the information we process, appropriate to its nature and to the size of our business. Depending on the system, these may include encryption of data in transit, protection of stored credentials and tokens, access limited to personnel who need it, verification of notifications we receive from platforms, separation of Customer data, monitoring for misuse, and procedures for responding to incidents. Our infrastructure providers maintain their own physical and network security.

No system is completely secure, and we cannot guarantee the security of any information.

## Shared responsibility

Customers are responsible for the security of their own systems, accounts, credentials, and users, for the records they keep, and for how they configure and use the services.

## Reporting a vulnerability

If you believe you have found a security vulnerability in our services, email security@vybose.com with the details. Please allow us reasonable time to investigate and address it before disclosing it publicly, and do not access, modify, or delete data that is not yours or disrupt our services.