Ombudsman Connect for Business: Security statement

Prepared by the
Financial Ombudsman Service

June 2025

Ombudsman Connect for Business: security statement

This document provides key security information about Ombudsman Connect for Business, the Financial Ombudsman Service's self-serve portal for financial services providers (businesses).

Strategic approach

The Financial Ombudsman Service manages the 'confidentiality, integrity and availability triad (CIA) of data and assets in line with our cyber security strategy, which is shaped around the NIST CSF 2.0 framework and aligns with the National Cyber Security Strategy.

The governance of the Strategy incorporates Cyber, InfoSec, DP and Tech teams to maintain the Security posture.

As a service, Ombudsman Connect for Business is subject to, and benefits from, this strategic approach.

Penetration tests and vulnerability management

Ombudsman Connect for Business has controls in place to ensure the security, confidentiality, availability and integrity of data. This is on top of leveraging our platform's (Microsoft Azure's) security features and compliance certifications.

Pen tests are a standard part of our security activities. We have contracted a CHECK-accredited third party for this, but it is managed and assured by our in-house Cyber Security team.

We have conducted two fully scoped pen tests to identify risks, and a managed remediation programme to address security vulnerabilities and risks to the integrity of Ombudsman Connect for Business. The most recent of these was in May 2025.

Based on the findings from these tests – and the further work we have carried out since (in line with the Pen Test recommendations) – we are satisfied that the current security controls, and the configuration we have in place, are appropriate for Ombudsman Connect for Business.

Pen testing and a continuous vulnerability management programme underpin our commitment to a robust and secure portal.

Security monitoring

In addition to pen testing and vulnerability management, Ombudsman Connect for Business is continuously monitored by a dedicated team of security operatives.

We employ an outsourced security operations centre. This is managed and assured by an internal Security Operations (SecOps) team – using an industry approved security information and event management (SIEM) solution – to alert us to anomalous events and behaviour.

Data security

We ensure robust security for both data in transit and at rest by implementing a defence-in-depth strategy, utilising TLS 1.2 for data transmission and encryption for stored data.

We manage access through security models based on roles and permissions. A dedicated antivirus/malware solution is implemented to protect against malicious software and other threats.

Our customer data is protected by encryption, using industry standard approved crypto algorithms, block ciphers and key lengths, and retained in line with regulatory recommendations and legal requirements.

Threat intelligence

We leverage third parties and internal threat intelligence and horizon scanning capabilities to inform our risk-management approach and evolve our identify, protect and detect capabilities.

Further information

See our website for more information about Ombudsman Connect for Business.