Credicorp
Suite 53C Unimix House
Abbey Road
London NW10 7TR
www.credicorp.co.uk
support@credicorp.co.uk

30 May 2026

Security disclosure (responsible-disclosure policy)

Reference: POL/SEC/2026.1

Version 1.0 - last revised 25 May 2026

Welcoming security research

We welcome reports from security researchers, customers and members of the public about potential vulnerabilities in credicorp.co.uk, the customer portal and our REST APIs. This page sets out our responsible-disclosure approach and our commitments to anyone reporting a vulnerability in good faith.

How to report

• Email security@credicorp.co.uk. Encrypt with our PGP key if you are sending exploit details; the key fingerprint is published at /.well-known/security.txt alongside this page.

• Include enough detail to reproduce: affected URL or endpoint, the technique, the impact you observed, and any screenshots that help.

• Tell us how you would like to be credited (or anonymously, if you prefer).

What we ask of you

• Give us a reasonable amount of time to triage and fix the issue before publishing it - typically 90 days for high-impact, 30 days for lower-impact.

• Do not access, modify, or destroy customer data you find. If your test produces an incidental disclosure of customer data, stop and tell us - we do not consider that a violation of this policy.

• Do not perform denial-of-service tests against production. Rate-limit your probing.

• Do not use social-engineering against our staff or customers.

What we promise back

- We will acknowledge receipt within 5 working days.
- We will provide an initial triage decision within 10 working days.
- We will keep you updated on the fix and credit you (or, if you prefer, leave you anonymous) in the patch notes when the fix lands.
- We will not pursue legal action against good-faith security research that follows this policy.

Scope

In scope: anything served from credicorp.co.uk, the customer portal, the REST APIs at /wp-json/ccfs/v1/, the PWA shell at /app/, and the staff portal endpoints. Out of scope: third-party services we link to (Stripe, GoCardless, ICO, Companies House), the operator's personal accounts, and physical-security tests.

Bug bounty

We do not currently run a formal cash bounty. We do publicly credit researchers (with their permission) in patch notes and hold a "thanks list" in /credits/. As we grow, we expect to formalise a bounty programme.
ICO Registration No. ZC157682