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

30 May 2026

Information Security

Information Security Policy

Reference: UK GDPR · DPA 2018 · ISO 27001 (aligned)

Version 1.0 - last revised 25 May 2026

Credicorp Limited treats the security of customer data as a foundational obligation. This policy is the public-facing summary of our information-security controls. The detail behind it is held in internal documentation (the Information Security Management System, ISMS), reviewed at least annually.

1. Encryption

• In transit: TLS 1.2 or higher on every connection to credicorp.co.uk and the customer portal. We do not accept older protocols.

• At rest: the application database, file uploads (ID documents, bank statements) and backups are encrypted at rest by the underlying storage layer.

• Application-level: sensitive option values (third-party API keys, webhook secrets) are encrypted with a per-installation key separate from the database.

2. Access control

• Every staff account is unique to a named colleague - no shared credentials.

• Multi-factor authentication is mandatory on every staff login (TOTP authenticator or WebAuthn).

• Access to customer data is role-based: a Collections agent does not see the Settings tab; an Auditor (Read-only) cannot mutate any record.

• Sensitive operations (override settings, deep-data exports, customer impersonation) require step-up "sudo" re-authentication that expires after a short window.

• All staff access to customer data is audit-logged with actor, timestamp and the specific records viewed.

3. Network & infrastructure

- Hosted on UK-based infrastructure (data residency: United Kingdom).
- Web application firewall on the front edge; rate-limiting at both the front edge and the application layer.
- HTTP security headers: HSTS, Content-Security-Policy, X-Content-Type-Options, X-Frame-Options, Referrer-Policy, Permissions-Policy.
- Outbound HTTPS connections from the application are guarded against SSRF (no loopback, no private/reserved address ranges).

4. Vulnerability management

- Code dependencies are scanned on every change; high and critical vulnerabilities are patched within 14 days, others within 30.
- Regular external security review of the production surface.
- Responsible-disclosure programme - see section 7.

5. Personal-data handling

We minimise the personal data we collect to what is necessary for identity verification, anti-money-laundering compliance and the operation of the loan. We do not sell personal data. Our Privacy Notice sets out the full detail. Retention follows the statutory minimum (typically 6 years from settlement) and erasure procedures are described in the Privacy Notice.

6. Breach response

A confirmed personal-data breach is assessed under UK GDPR Article 33 within 72 hours of becoming aware. If the breach is likely to result in a risk to affected individuals, we notify the Information Commissioner's Office (ICO). If the breach is likely to result in a HIGH risk, we notify the affected individuals directly using the contact details on their record. We maintain a breach register with root cause and remedial action for every confirmed breach (notifiable or not).

7. Responsible disclosure

If you have found a security weakness in credicorp.co.uk, the customer portal or any system we operate, please tell us so we can fix it. Email security@credicorp.co.uk with the details. We commit to:

- Acknowledge receipt within 1 business day.
- Provide an initial triage within 5 business days.
- Not take legal action against good-faith research that does not exploit customer data and that complies with the Computer Misuse Act 1990.
- Credit the reporter (with their permission) once the issue is fixed, on a private "thanks" page.

This policy was last reviewed in May 2026.
ICO Registration No. ZC157682