



Data Security Policy

1. Hosting & Infrastructure

- Bema1's data is hosted on AWS servers located in Malaysia.

2. Secure Communication

- All communication between users and our servers is secured using HTTPS (TLS v1.2).
- A lock icon in the browser URL bar confirms that all web interactions occur over a secure channel.
- APIs require authentication tokens, ensuring that only authorized requests from Bema1 can access the system.

3. Network & Access Controls

- The server exposes only one secure gateway to external access.
- All backend services and databases operate within a private network, inaccessible from outside the system.
- External access to these services is only possible via a VPN-protected gateway, adding an extra layer of security.

4. Data Encryption & Storage

- All data, including database records, files, and images, is encrypted using a security key.
- Even AWS (Amazon Web Services) itself cannot access or view the encrypted data.
- User passwords are not stored in plaintext; sensitive authentication details are securely handled.

5. Protection Against Cyber Threats

- A Content Delivery Network (CDN) layer helps filter and mitigate attacks, including DDoS (Distributed Denial of Service) attacks.

6. User Authentication & Privacy

- Users log in using email and password authentication, with confirmation steps to ensure security.

- Bema1 does not store passwords or sensitive authentication details.
- Only minimal user metadata is stored to support item discovery and user interaction within the platform.

For further inquiries regarding our security measures, please contact our team at hello@bema1.com