BridgeOut: Security Checklist

Below is BridgeOut’s official security checklist. Every step must be completed before userdata is stored in the production instance. The engineer conducting the check must provide their signature at the end of the document.

Django configuration:

- □ Only allow HTTPS.
- □ Set DEBUG flag to false.
- □ Update all modules to latest version.
- □ Check modules for CVE vulnerabilities.
- □ Obfuscate /admin/ url path to something hard to guess.

Cloud configuration (Cloud Dashboard):

- □ Add alerts for CPU spiking.
- □ Redirect HTTP to HTTPS.
- □ Store database credentials, secret keys in environment variables.
- □ Isolate databases from the public web using Virtual Private Clouds

Testing with tools:

- □ Port scan the website to assure only HTTPS is open.
- □ Test for SQL injections with sqlmap.
- □ Brute force password on login (Should trigger CPU alert).

I hereby acknowledge that I have thoroughly reviewed and completed the cybersecurity checklist provided by BridgeOut. I affirm that all the necessary measures and protocols outlined in the checklist have been diligently implemented in accordance with industry best practices and BridgeOut’s cybersecurity policies.

Signature: ____

Date: ____________________