

RULES OF ENGAGEMENT

This Rules of Engagement (this "**ROE**") governs the conduct of the security assessment, penetration testing, vulnerability scanning, and Continuous Threat Exposure Management (collectively, the "**Testing**") to be performed by:

Zugzwang (Private) Limited ("**Zugzwang**" or the "**Tester**"), a company duly incorporated under the laws of the Republic of Zimbabwe, having its registered office and principal place of business at _____, represented in this matter by **Busani Ndlovu, Founder & Chief Executive Officer**;

ON BEHALF OF

_____ ("**Client**"), a _____ (company / other entity) duly established under the laws of _____, having its principal place of business at _____.

Zugzwang and the Client are each referred to individually as a "**Party**" and collectively as the "**Parties**".

1. PURPOSE AND SCOPE

1.1 The Client engages Zugzwang to perform Testing of the systems, networks, applications, and data specified in **Appendix A** (the "**In-Scope Assets**"), on the terms of this ROE, the Letter of Authorization executed between the Parties, and any Master Services Agreement or Statement of Work in effect between the Parties.

1.2 The objectives of the Testing are: to identify vulnerabilities and control gaps; to assess compliance with the Cyber and Data Protection Act [Chapter 12:07] and related obligations; and to provide a prioritised remediation roadmap. The Testing is defensive in nature and is performed solely for the Client's benefit.

2. AUTHORISATION

2.1 The Client represents and warrants that it owns, or has full lawful authority to authorise Testing of, each In-Scope Asset, and that it has obtained all necessary consents (including from any third-party host, upstream provider, or data subject where required).

2.2 Testing shall be performed strictly within the scope, targets, methods, and timeframes described in this ROE and the Letter of Authorization. Any Testing outside that scope is expressly prohibited.

2.3 Zugzwang will not perform any Testing until: (a) this ROE is signed; (b) the Letter of Authorization is signed by an authorised signatory of the Client; and (c) the Mutual Non-Disclosure Agreement between the Parties is in effect.

3. TESTING METHODOLOGY

3.1 Testing will follow an industry-recognised methodology (such as the OWASP Testing Guide, OWASP Web Security Testing Guide, PTES, and NIST SP 800-115) and, where applicable, the five-stage Continuous Threat Exposure Management cycle of scoping, discovery, prioritisation, validation, and mobilisation.

3.2 The approach may be one or more of: **black box** (no prior knowledge or credentials), **grey box** (limited knowledge or credentials), or **white box** (full knowledge and credentials), as specified in Appendix A.

3.3 Zugzwang may use automated scanners, manual testing, and controlled exploitation to confirm the real-world impact of identified findings. All tools and techniques are used with the care of a reasonable professional and are limited to the In-Scope Assets.

4. PROHIBITED ACTIONS

4.1 Zugzwang shall not:

- **(a)** perform denial-of-service, stress, or destructive testing of any kind, unless expressly agreed in writing;
- **(b)** deploy malware, ransomware, or any persistent or self-propagating software;
- **(c)** access, copy, modify, or exfiltrate personal data or production data, except to the minimum extent necessary to demonstrate a vulnerability, and never for any purpose other than the Testing;
- **(d)** target any asset, system, or third party outside the In-Scope Assets;
- **(e)** attempt to cause actual damage, downtime, or data loss; or
- **(f)** use or retain any vulnerability, credential, or data obtained during the Testing after the Testing has concluded, except as required to prepare the report.

4.2 Zugzwang shall take reasonable steps to avoid unintended impact on systems that share infrastructure with the In-Scope Assets.

5. TESTING WINDOWS

5.1 Testing shall be conducted within the agreed testing window(s) set out in Appendix A (the "**Testing Windows**"). Zugzwang shall notify the Client's nominated contact before commencing Testing and shall suspend Testing immediately upon written instruction from the Client.

5.2 Testing outside the Testing Windows is prohibited unless the Client provides prior written consent.

6. DATA HANDLING AND CONFIDENTIALITY

6.1 All information obtained or generated during the Testing, including findings, credentials, screenshots, and the final report (the "**Deliverables**"), is the Client's Confidential Information and shall be handled in accordance with the Mutual Non-Disclosure Agreement between the Parties.

6.2 Zugzwang shall store Deliverables and testing data in encrypted form, shall restrict access to

personnel with a genuine need to know, and shall return or securely destroy all such data within _____ days of the Client's written request or the conclusion of the engagement, whichever is earlier.

6.3 Zugzwang shall not disclose the existence, scope, findings, or results of the Testing to any third party without the Client's prior written consent, except as required by law.

7. COMMUNICATION AND POINTS OF CONTACT

7.1 The Client's nominated point of contact for the engagement is:

Name: _____ Role: _____

Email: _____ Telephone: _____

7.2 Zugzwang's nominated point of contact for the engagement is:

Name: _____ Role: _____

Email: _____ Telephone: _____

7.3 Zugzwang shall provide a status update at least once every _____ during active Testing, and shall notify the Client's point of contact promptly of any critical or high-severity finding.

8. EMERGENCY AND INCIDENT PROCEDURE

8.1 In the event of an unintended outage, service degradation, or suspected security incident during the Testing, Zugzwang shall immediately cease Testing, notify the Client's point of contact, and assist the Client in stabilising the affected systems.

8.2 If Zugzwang, during the Testing, identifies evidence of an ongoing or prior security incident affecting the In-Scope Assets, it shall notify the Client promptly and provide reasonable assistance in accordance with the Client's breach-notification obligations under the Cyber and Data Protection Act.

9. REPORTING AND DELIVERABLES

9.1 Upon completion of the Testing, Zugzwang shall deliver a written report that includes: an executive summary; a description of scope and methodology; an inventory of findings ranked by severity; supporting evidence; and a prioritised remediation roadmap.

9.2 Zugzwang shall provide reasonable remediation support following delivery, including clarification of findings and, where agreed, a retest to confirm remediation.

10. LIMITATION OF LIABILITY

10.1 Zugzwang shall perform the Testing with reasonable skill and care. Zugzwang's total aggregate liability arising out of or in connection with the Testing shall be limited to the fees paid

for the Testing, and neither Party shall be liable for indirect, incidental, or consequential loss, except to the extent such liability cannot be excluded by law.

11. GOVERNING LAW

11.1 This ROE shall be governed by and construed in accordance with the laws of the Republic of Zimbabwe, and the Parties submit to the exclusive jurisdiction of the courts of the Republic of Zimbabwe.

12. AMENDMENT AND TERM

12.1 This ROE may be amended only by written instrument signed by both Parties. It shall remain in effect for the duration of the Testing and until the Deliverables are provided and any agreed retest is complete.

APPENDIX A — SCOPE OF TESTING

In-Scope Assets (systems, domains, IP ranges, applications, networks, buildings):

Out-of-scope (must not be touched):

Testing type: black box / grey box / white box (select)

Testing Windows:

From: _____ To: _____

Approved methods / constraints:

SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Rules of Engagement as of the date first written above.

ZUGZWANG (PRIVATE) LIMITED

By: _____

Name: **Busani Ndlovu**

Title: **Founder & Chief Executive Officer**

Date: _____

CLIENT

By: _____

Name: _____

Title: _____

Date: _____