RULES OF ENGAGEMENT

Internal Network & Active Directory Penetration Testing Engagement

Between

TadiSec (Provider)

and

Navigating Security Corp. (Client)

Document No.	TDSC-ROE-2026-001
Associated SOW	TDSC-SOW-2026-001
Version	1.0
Date Issued	March 12, 2026
Classification	Confidential

CONTROLLED DOCUMENT

This Rules of Engagement document is classified as Confidential. It contains sensitive information about authorized testing activities, network infrastructure, and security controls. Distribution is restricted to authorized personnel identified in Section 2.

1. Purpose & Authority

1.1 Purpose

This Rules of Engagement ("ROE") defines the operational boundaries, authorized activities, prohibited actions, communication protocols, and escalation procedures governing the Internal Network and Active Directory Penetration Test conducted by TadiSec on behalf of Navigating Security Corp.

All TadiSec personnel assigned to this engagement must read, understand, and acknowledge this document before testing begins. Any activity not explicitly authorized herein or in the associated SOW is prohibited.

1.2 Relationship to Statement of Work

This ROE is a companion document to SOW TDSC-SOW-2026-001. The SOW defines scope, deliverables, pricing, and contractual terms. This ROE defines how testing is conducted. In conflict, the SOW governs scope/deliverables; the ROE governs testing conduct.

1.3 Authorization

Field	Detail
Authorizing Individual	Oliver Whitaker
Title	Chief Information Security Officer
Organization	Navigating Security Corp.
Authorization Date	March 12, 2026
Authorization Scope	DC01 (10.1.1.10) and the navigatingsecurity.corp Active Directory domain

Legal Notice

This document constitutes written authorization for TadiSec to perform the testing activities described herein. TadiSec will retain a signed copy for the duration of the engagement and the 90-day data retention period. This document serves as evidence of authorized activity in the event of any security alert or investigation.

1.4 Engagement Period

Parameter	Detail
Engagement Start Date	March 23, 2026 (Kickoff)
Engagement End Date	April 23, 2026 (Readout)
Active Testing Window	March 24 through April 3, 2026

Blackout Period	March 30–31, 2026 (month-end)
Report Delivery	April 21, 2026
Readout	April 23, 2026

No testing may occur before March 24 or after April 3, 2026 without written re-authorization from Oliver Whitaker.

2. Authorized Personnel & Contacts

2.1 TadiSec Testing Team

Name	Role	Certifications	Contact
Rumbidzai Moyo	Engagement Lead	OSCP, CRTO, CPTS	r.moyo@tadisec.co.zw / +263 77 234 8901
Tonderai Chigubhu	Lead Tester	OSCP, OSEP	t.chigubhu@tadisec.co.zw / +263 71 445 6782

2.2 Navigating Security Corp. Contacts

Role	Name	Phone	Email	Availability
Primary POC	Oliver Whitaker	+1 (212) 555-0147	o.whitaker@navseccorp.com	Business hours
Technical POC	Aarav Patel	+1 (212) 555-0162	a.patel@navseccorp.com	Business hours
Emergency POC	Cathy Williams	+1 (212) 555-0199	c.williams@navseccorp.com	24/7 during testing

3. Scope Boundaries

3.1 In-Scope: DC01 Only

This engagement is scoped exclusively to DC01 and the Active Directory domain it hosts. TadiSec may perform host discovery scanning across 10.1.1.0/24 to map the network, but only DC01 is authorized for enumeration, exploitation, and interaction.

Target	Detail
Domain	navigatingsecurity.corp
Domain Controller	DC01 (10.1.1.10) — Windows Server 2019
Forest Functional Level	Windows Server 2016

Trust Relationships	None — single-forest, single-domain
ADCS	Installed on DC01 — single-tier enterprise CA
LAPS	Deployed domain-wide (verify during testing)

3.2 Out-of-Scope Systems

PROHIBITED — Do Not Test

All systems other than DC01 are out of scope, including any hosts discovered during network scanning. Accidental interaction with an out-of-scope system must be reported to Rumbidzai Moyo and Aarav Patel within 30 minutes.

System / Network	Reason
All hosts on 10.1.1.0/24 other than DC01	Not authorized — DC01-only engagement
10.1.1.1 (Network Gateway)	Network infrastructure — disruption risk
Any IP outside 10.1.1.0/24	Not authorized
Azure AD / Microsoft 365 / Cloud	Not in scope

3.3 Boundary Handling

1. Halt exploitation at the boundary of any out-of-scope system.
2. Document the attack path as a finding.
3. Notify Aarav Patel (Technical POC).
4. Written authorization from Oliver Whitaker required to extend scope. Email is acceptable.

4. Authorized Testing Activities

4.1 Reconnaissance & Enumeration

- Host discovery scanning across 10.1.1.0/24 (mapping only — no exploitation of non-DC01 hosts)
- Active port and service scanning of DC01
- LDAP/AD enumeration: users, groups, GPOs, ACLs, SPNs, OUs, trusts, delegation settings
- DNS enumeration (forward, reverse, zone transfer attempts) against DC01
- ADCS certificate template and enrollment policy enumeration
- SYSVOL and NETLOGON share enumeration
- LLMNR/NBT-NS/mDNS traffic analysis on 10.1.1.0/24

4.2 Credential Attacks

- Password spraying (respecting lockout thresholds — Section 6.1)
- Kerberoasting and AS-REP roasting
- LLMNR/NBT-NS poisoning and hash capture via Responder
- NTLM relay attacks against DC01
- Offline hash cracking (NTLM, Kerberos TGS, NetNTLMv2)
- Credential extraction from LSASS, SAM, registry, and GPP on DC01

4.3 Exploitation & Privilege Escalation

- Exploitation of known vulnerabilities on DC01
- Kerberos delegation abuse (constrained, unconstrained, RBCD)
- DACL/ACE abuse (GenericAll, WriteDACL, WriteOwner, ForceChangePassword, etc.)
- DCSync (replicating domain credentials via DRS protocol)
- Silver Ticket and Golden Ticket generation
- ADCS certificate template abuse (ESC1–ESC8)
- GPO abuse for code execution or privilege escalation
- AdminSDHolder abuse, DCShadow (documented and controlled)

4.4 Post-Exploitation

- Assessing domain persistence mechanisms
- Sensitive data access via AD attributes, SYSVOL, GPP
- Testing CrowdStrike Falcon detection against common AD tooling
- Exfiltration path validation (without actual exfiltration of real data)

5. Prohibited Activities

ABSOLUTE PROHIBITIONS
Violation requires immediate cessation and notification to Rumbidzai Moyo and Oliver Whitaker.

5.1 Denial of Service

- No intentional DoS/DDoS testing. No resource exhaustion.
- DoS-capable vulnerabilities documented without exploitation.

5.2 Data Destruction & Modification

- No deletion, modification, or encryption of production data.
- No modification of AD schema, domain functional levels, or replication topology.
- No GPO modifications without written pre-approval.

5.3 Data Exfiltration

- No actual exfiltration of PII or sensitive data from the environment.
- Access validation permitted using redacted screenshots.

5.4 Social Engineering

- No phishing, vishing, smishing, pretexting, or physical security testing.

5.5 Persistence & Implants

- No persistent backdoors surviving reboot or the testing window.
- In-memory agents permitted during testing hours only; terminated end-of-day.
- All Kerberos tickets documented; not used after April 3, 2026.

5.6 Out-of-Scope Interaction

- No exploitation, enumeration, or interaction with any host other than DC01.
- No pivoting to cloud environments.
- Host discovery scanning of the /24 subnet is permitted for mapping purposes only.

5.7 Interference with Business Operations

- No intentional disruption of production workloads.
- No mass account lockouts (Section 6.1).
- No restarting services on DC01 without real-time approval from Aarav Patel.
- No testing during blackout period (March 30–31, 2026).

6. Operational Safety Thresholds

6.1 Account Lockout Policy

Parameter	Value
Lockout Threshold	5 failed attempts
Lockout Duration	30 minutes (auto-unlock)
Observation Window	30 minutes
Password Complexity	Enabled
Minimum Password Length	8 characters

TadiSec will attempt no more than **3 passwords per account per 30-minute window** (2 below the lockout threshold).

6.2 Scanning Rate Limits

Activity	Constraint
Port scanning	Max 500 packets/sec (nmap -T3)

LDAP enumeration	Standard query rate; no bulk modifications
Responder/Relay	Passive listening during business hours; active poisoning off-hours only (Sat 2–6 AM EST)

6.3 High-Risk Technique Approval

The following require Rumbidzai Moyo to notify Aarav Patel in real-time before execution:

Technique	Risk	Notification
DCSync against DC01	Replication load on sole DC	Yes — before execution
NTLM relay against DC01	Auth disruption on sole DC	Yes — before execution
Golden / Silver Ticket generation	Persistence artifacts	Yes — before execution
DACL/ACE modification on AD objects	Permission changes	Yes — notify and document
LSASS dump on DC01	CrowdStrike alerting, DC instability	Yes — before execution
Responder active poisoning	Auth disruption for users	Yes — off-hours only, notify before
ADCS certificate abuse (ESC1–ESC8)	Certificate issuance, persistence	Yes — before execution

Single Domain Controller Warning

DC01 is the only domain controller. If it becomes unstable, all domain authentication, DNS, and DHCP stops. Exercise extreme caution with memory-intensive operations (LSASS dumps, large LDAP queries) and replication-based attacks (DCSync).

Pre-Approved Techniques

Standard enumeration, port scanning, Kerberoasting, AS-REP roasting, pass-the-hash, and local privilege escalation do not require real-time notification.

7. Testing Schedule & Windows

Window	Hours	Activities Permitted
Primary	Mon–Fri, 9:00 AM – 6:00 PM EST	All authorized techniques
Extended	Mon–Fri, 6:00 PM – 10:00 PM EST	Standard techniques; no high-risk without approval
Off-Hours	Saturday 2:00 AM – 6:00 AM EST	High-risk techniques (Responder, mass scanning)
Blackout	March 30–31, 2026	No testing permitted

7.1 End-of-Day Procedure

1. Terminate all C2 sessions and in-memory agents.
2. Document all actions (timestamped log).
3. Post status update in Teams channel.
4. Secure evidence in encrypted storage.
5. Verify no lingering processes on DC01.

8. Communication Protocols

Purpose	Channel	Detail
Daily status	Microsoft Teams	Channel: "TadiSec × NavSec — Pentest"
Real-time coordination	Microsoft Teams	DM Aarav Patel for urgent items
Emergency / Critical	Phone + Email	Call Cathy Williams, then encrypted email
Report delivery	Encrypted email (PGP)	To Oliver Whitaker and Aarav Patel

8.1 Critical Finding Notification

1. **Verbal:** Rumbidzai Moyo calls Cathy Williams within **1 hour** of confirmed discovery.
2. **Written:** Critical Finding Advisory via encrypted email within **4 hours**.
3. **Joint decision:** Continue, pause, or adjust scope.

9. De-Confliction

9.1 TadiSec Source Indicators

Indicator	Value

Tester Workstation	TDSC-TEST-01
Source IP	10.1.1.200 (or VPN endpoint confirmed at kickoff)
Domain Account	t.chigubhu
User-Agent	TadiSec-PenTest/2026

9.2 SOC Posture

Agreed posture: Alert but No Response. The SOC will monitor and log TadiSec activity but will not block, isolate, or interfere with testing.

9.3 De-Confliction Hotline

Contact	Phone	Availability
Rumbidzai Moyo	+263 77 234 8901	During testing hours
TadiSec Emergency Line	+263 86 770 0100	Business hours

TadiSec will respond within 15 minutes. If unreachable, the SOC should treat activity as potentially hostile.

10. Escalation Procedures

10.1 Unintended Disruption

6. **HALT:** All testing stops.
7. **NOTIFY:** Rumbidzai Moyo calls Cathy Williams within 15 minutes.
8. **DOCUMENT:** Written summary within 2 hours.
9. **RESUME:** Only after written authorization from Oliver Whitaker.

10.2 Active Compromise Discovered

1. Cease activity to preserve forensic evidence.
2. Call Cathy Williams immediately.
3. Provide all IOCs.
4. Jointly decide next steps.

10.3 Escalation Matrix

Event	First Contact	Escalation	Timeline
Service disruption	Cathy Williams	Oliver Whitaker	Within 15 min
Active compromise	Cathy Williams	Oliver Whitaker + SOC	Immediately
Critical finding	Cathy Williams	Oliver Whitaker	Within 1 hour

Out-of-scope contact	Aarav Patel	Oliver Whitaker	Within 30 min
High-risk technique	Aarav Patel	—	Before execution
Scope dispute	Aarav Patel	Oliver Whitaker	Within 4 hours
Access issues	Aarav Patel	—	Same business day
De-confliction	Rumbidzai Moyo	TadiSec Emergency Line	Within 15 min

11. Tester Conduct & OPSEC

- Professional conduct at all times.
- No access to sensitive data beyond what is necessary to demonstrate impact.
- All evidence on encrypted TadiSec systems (AES-256). Credentials in KeePassXC.
- No discussion of engagement details outside authorized personnel.
- Tool log maintained: all tools with version numbers and timestamps.
- Only Rumbidzai Moyo-approved tools. No personal or unapproved tools.

12. Evidence Handling

- Timestamped screenshots, command output logs, PCAPs where relevant.
- Sensitive data redacted in screenshots. Full credentials in encrypted appendix to Aarav Patel only.
- PII findings flagged as relevant to applicable state privacy regulations.
- Activity logs available upon request; included in evidence package (SOW Deliverable #7).

13. Cleanup & Post-Engagement

Action	Responsible	Verified By
Terminate all C2 sessions	TadiSec	Aarav Patel
Remove tools/scripts/binaries from DC01	TadiSec	Aarav Patel
Revert DACL/ACE modifications	TadiSec	Aarav Patel
Document un-removable artifacts	TadiSec	Aarav Patel
Confirm no Kerberos persistence artifacts remain	TadiSec	Aarav Patel

Data retained 90 days post-Final Report (until July 20, 2026), then destroyed per NIST SP 800-88.

14. Amendments

Amendments require written consent from Rumbidzai Moyo and Oliver Whitaker (email acceptable).

Amendment #	Date	Description	Authorized By

15. Acknowledgment & Authorization

15.1 Provider Acknowledgment

By signing below, TadiSec confirms that all assigned testers have read, understood, and will comply with this document.

TadiSec — Engagement Lead

Name: Rumbidzai Moyo

Title: Principal Consultant

Signature: _____

Date: _____

15.2 Tester Acknowledgment

Name	Signature	Date
Rumbidzai Moyo		
Tonderai Chigubhu		

15.3 Client Authorization

By signing below, Navigating Security Corp. authorizes the testing activities described in this document.

Navigating Security Corp. — Authorizing Individual

Name: Oliver Whitaker

Title: Chief Information Security Officer

Signature: _____

Date: _____

— End of Rules of Engagement —