

Rules of Engagement

<CLIENT NAME>

<Insert Date>

Executive Summary

<<Insert your EXSUM here>>

The Rules of Engagement (ROE) document the approvals, authorizations, and critical implementation issues necessary to execute the engagement. Signing of the ROE constitutes acknowledgement and approval of the customer, system owner, and Red Team of the Red Team’s authorities in execution of the engagement.

The objectives include: <<short list with reference to Appendix D>>

* Objective 1
* Objective 2
* Objective 3
* Objective 4

Explicit Restrictions: <<short list with reference to Appendix A>>

* Restriction 1
* Restriction 2

Authorized Target Space: <<short list with reference to Appendix A>>

* IP Range (or set)
* Domains
* URLs
* Network Segments

Activities: <<short list with reference to Appendix C>>

* Reconnaissance
* Access Types
* Positioning
* Impacts

TABLE OF CONTENTS

Section Page

1 Rules of Engagement Introduction 1

1.1 Purpose 1

1.2 References: 1

1.3 Scope 1

1.4 Definitions 1

2 Rules of Engagement and Support Agreement: 1

2.1 ROE Provisions 4

2.2 Requirements, Restrictions, and Authority 5

2.3 Ground Rules 5

2.4 Resolution of Issues/Points of Contact (POC) 6

3 Authorization 6

4 Approval 6

APPENDIX A – Target Environment 7

APPENDIX B - Points of Contact 9

APPENDIX C – Red Team Methodology 10

APPENDIX D – Engagement objectives 11

APPENDIX E – Threat profile 12

# Rules of Engagement Introduction

## Purpose

To establish the responsibilities, relationships, and guidelines between the I♥REDTEAMS, INC Red Team hereafter referred to as “Red Team”, <<the customer>>, <<system owner (if different)>>, and <<any stakeholders required for engagement execution>> for conducting a Red Team engagement on <<organization, network, or system>> hereafter referred to as “target of engagement”. The engagement will be conducted from Red Team locations at <<address>> on target systems located at <<IP/Domain, Address>>.

## References:

* 1. <<Applicable References Here>>
	2. PIA …
	3. HIPAA …
	4. ISO …

## Scope

This agreement is applicable to <<business, customer, system, network>> for the receipt of Red Team activities. This document will establish the guidelines, limitations, and restrictions for conducting a Red Team engagement.

## Definitions

<<Short definition of terms>>

# Rules of Engagement and Support Agreement:

1. I♥REDTEAMS, INC has been agreed upon to conduct a Red Team engagement and supporting Red Team activities. This document provides the ground rules for planning, executing and reporting the engagement.
2. <<Short description of the services requested and information about the requesting entity>>. The following systems, networks and/or assets will be included:
* <<List of business/organization systems and networks included>>
* All software and hardware included as a target during the engagement.
1. The Red Team will <<list of activities>>
* The engagement is designed to <<objectives>>. This means the system must <<whatever the objectives are designed to test/assess/evaluate/stress>>.
* For the Red Team, an open network will be utilized. An open network is defined as a network with access to the internet.
* Engagement activities will be conducted using scenarios detailed in the Threat Profile <<Appendix x>>.
* The customer is responsible for <<responsibilities>>.
* There will be complete and open coordination with all stakeholders required for engagement execution. Stakeholders are the parties represented by the signatories of this document.
* Red Team activities are limited to the target of engagement.
* Red Team tools and activities may be intrusive, but will not intentionally disrupt services outside the authorizations of these Rules of Engagement.
* The Red Team will provide <<X>> updates (<<list each>>) as follows:
	+ Update 1: <<Conditions>>
	+ Update 2: <<Conditions>>
1. <<Customer>> will: <<Include list of responsibilities>>
* Provide the Red Team administrative facilities and support for all team personnel as necessary to conduct the engagement (if onsite).
* Provide support with network and resources for conducting the engagement, including adequate workspace (quiet facility), network drops and power connections for the Red Team’s systems.
* Provide IP address ranges and administrative support for target of engagement.
* Coordinate support of Red Team activities, with the appropriate stakeholders.
* Provide contact information (i.e., names, job titles, phone & email address) to the signatories of this document.
* Provide to the Red Team the results of the Vulnerability Assessment scans performed prior to the engagement to create the effects of intelligence gathering background efforts expected of a malicious entity.
1. Red Team efforts will be coordinated with <<insert POC position/title>> for the duration of the engagement. The Red Team will target only those hosts and internet protocol (IP) addresses within the confines and control of the target of engagement network.
2. Red Team methods may be intrusive, but should not be destructive, and will be terminated if information is gathered pertaining to an actual intrusion. Red Team is responsible for informing <<insert POC position/title>> if an actual intrusion is discovered. <<insert POC position/title>> will report the actual intrusion to the appropriate representative, along with any substantiating information regarding the detected intrusion.
3. Red Team operations require the use of exploitation and attack tools and techniques. All tools employed by the Red Team have been extensively tested by the team to ensure they are non-destructive and are under positive control when employed.
4. Red Team systems contain exploit tools, code, and technical references, which are not to be viewed, distributed or evaluated by external organizations.
5. The Red Team will attempt to gain access to the target of engagement.
6. Off limits IP lists is provided as Appendix <<X>>. This list should only include those IP ranges within the network that are not part of the engagement.
7. The Red Team may only conduct activities against client networks that provide sufficient notice to system users that their use of those systems constitutes consent to monitoring. It is the responsibility of the target of engagement legal counsel to review these notice procedures and certify they provide sufficient notice.
8. Sensitive information reporting:
* Vulnerabilities discovered during the engagement that present an immediate risk to life, limb, or eyesight will be reported promptly to <<insert POC position/title>> to enable immediate response or action. Representatives of the signatories of this ROE will receive follow-on notification as appropriate.
* Incidental discovery of information that relates to serious crimes such as sabotage, threats, or plans to commit offenses that threaten a life or could cause significant damage to or loss of customer property, and which does not present an immediate risk, will be reported to the applicable local authorities for action.
* The Red Team reporting is otherwise conducted in a way that does not attribute information or particular activity to an individual.
* Red Team activities may not be conducted in support of law enforcement or criminal investigation purposes.
1. Cease operations process:
* The Red Team will suspend activity upon detection of computer anomalies that could potentially be unauthorized intrusions into target of environment networks.
* The Red Team will suspend activity when unintentional information as described above is encountered, and until the appropriate reporting has taken place.
* All engagement activities operate under the direction of the Engagement Director, who may alter or cease activities as necessary.
1. Information usage:
* The Red Team will not intentionally compromise Privacy of Information Act (PIA), medical, justice, worship or religious pursuit, or any other protected or privileged information. If a compromise does occur, it will be handled through normal procedures. The proper security personnel will be notified immediately.
* The Red Team is authorized to exploit files, email, and/or message traffic stored on the network, as well as communications transiting the network for analysis specifically related to the accomplishment of their objectives. (e.g., identifying user ID’s, passwords and/or network IP addresses in order to gain further access).
* The Red Team will not intentionally modify or delete any operational user data, or conduct any Denial of Service attacks. The Red Team will not otherwise intentionally degrade or disrupt normal operations of the targeted systems.
* The Red Team reporting is conducted in a way that does not attribute information or particular activity, to a specific individual.
1. Deconfliction process:
* All detected information assurance incidents, whether real-world or alleged Red Team activity, should immediately be reported using normal incident reporting processes.
* The <<the customer>>, <<system owner (if different)>> POC may contact the Red Team’s POC to determine if discovered activities are the result of the Red Team.
1. Deliverables:
* The Red team will provide an engagement summary presentation for the target of engagement representatives at the completion of the engagement.
* The Red Team will provide a written summary of the engagement results to the <<insert POC position/title>> representative within 30 days following completion of the test.

## ROE Provisions

The following additional provisions apply to this memorandum:

1. All operations will be conducted within guidelines established by applicable policy, regulations and laws.
2. All contact with computer networks/subnets will be from within the Red Team or target of engagement environment.
3. During the engagement, any deviations from these ROE must be mutually agreed to and approved in writing by the senior representatives for the Red Team, <<the customer>>, <<system owner (if different)>>, and <<any stakeholders required for engagement execution>>.

## Requirements, Restrictions, and Authority

1. The Red Team will:
* Provide the appropriate support and input for the planning of the engagement.
* Coordinate engagement approval and support via this Rules of Engagement (ROE).
* Inform target of engagement POCs of all team requirements (logistics, administrative, etc.).
* Coordinate team personnel and administrative issues/concerns with <<insert POC position/title>>.
* Provide contact information (i.e. names, job titles, phone & email address) to the <<customer>> representatives.
* Escalate problems and issues to the appropriate representatives.
* Upload, where appropriate, indicators on systems to demonstrate a compromised state.
* When necessary, add/modify/disable accounts (not delete them) on compromised systems.
* Conduct exploitation with the intent of emulating threat techniques, tactics and procedures.
* May view/read or modify personal data files, PII, or emails.
* NOT use unapproved tools.
* NOT damage systems or networks.
* NOT conduct denial of service (DOS), except as explicitly approved.

## Ground Rules

This section identifies specific rules associated with the execution of this event.

1. Network Operations

* All systems outside the IP ranges provided under separate cover are off limits
* All <<insert here>> applications that are discovered during network operations will be off limits. This includes the following (list provided)
* <<insert here>> are off limits. IP addresses will be provided Appendix <<X>>.
1. Physical Engagement
* All <<insert here>> areas are off limits to Red Team personnel including transient movement due to potential loss of life, limb, or eyesight
* Buildings <<0>> through <<1>> are off limits
* <<X>> binders in any office will not be inspected, touched or removed.

## Resolution of Issues/Points of Contact (POC)

Any issues that may develop, which are not covered by this ROE, will be resolved mutually with all stakeholders.

* CIO Representative: Mr. Joe Snuffy, (555) 555-0001, joe.snuffy@customer.com
* CIO: Mrs. Jane Doe, (555) 555-0005, jane.doe@customer.com
* Red Team Lead: Mr. James Tubberville, (256) 262-7776, james@minis.io
* Red Team Tech Lead: Mr. Joe Vest, (205) 913-8868, joe@minis.io
* <<Trusted Agent>>: Mr. Blah Phisher, (555) 555-9876, blah.phisher@cnd.com
* <<System Owner>>: (REPRESENTAIVE) (PHONE) (EMAIL)
* <<Engagement Director>>: (REPRESENTAIVE) (PHONE) (EMAIL)
* <<White Cell Lead>>: (REPRESENTAIVE) (PHONE) (EMAIL)
* <<CEO>>: (REPRESENTAIVE) (PHONE) (EMAIL)

# Authorization

This agreement becomes effective upon the date of the last approving official's signature.

Termination of this agreement can be directed by any of the stakeholders listed in this document at any time by giving notice in writing to the non-terminating parties. This agreement can only be modified by mutual written consent of the signatories. Changes must be coordinated by means of an exchange of memoranda between the signatories. This agreement will undergo a review in its entirety with each modification request or by the request of either party after giving notice in writing at least 7 days prior to the review.

# Approval

The signatures below denote that all parties have read and agree to this Memorandum of Agreement.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(NAME) (NAME)

Red Team Lead Chief Information Officer

I♥REDTEAMS, INC LLC Customer ORG

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Date) (Date)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(NAME ) (NAME)

Engagement Directory Chief Executive Officer

Organization Customer ORG

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Date) (Date)

# APPENDIX A – Target Environment

List of assets, systems and data

Restricted IP Addresses:

* 10.10.10.0/24
* 10.10.11.0/24
* 10.11.0.0/16

Authorized IP Space:

* 10.10.12.0/24
* 10.10.13.0/24
* 10.12.0.0/16

Restricted Hosts:

* customer\_workstation\_1-1000
* customer\_server\_1-20

Authorized Hosts:

* PII\_workstation\_1-1000
* PII\_server\_1-20
* All hosts not expressly restricted

Restricted Buildings:

* Bldg. 1 Office 310
* Bldg. 2 Office 600

Authorized Buildings:

* Buildings 1, 2, 3, 4
* All spaces not expressly restricted

# APPENDIX B - Points of Contact

<<Role, Name, Title, Phone, Email, Office>>

Engagement Director:

* Name
* Phone
* Email
* Office Location

Trusted Agent:

* Name
* Title: Chief Information Officer
* Phone
* Email
* Office Location

White Cell Lead:

* Name
* Title: Chief Executive Officer
* Phone
* Email
* Office Location

Emergency Contact:

* Name
* Title: Executive Assistant
* Phone
* Email
* Office Location

Red Team Lead:

* Name
* Phone
* Email
* Office Location

# APPENDIX C – Red Team Methodology

<<Example or representative activities only – Detail not required>>

Get-In:

* Reconnaissance
	+ Perform Open Source Intelligence (OSINT) against the target
	+ Search using open unauthenticated sources
	+ Target web sites
	+ Social Media
	+ Search engines
	+ Public Code repositories
* Enumeration
	+ Identify external assets
	+ Perform reverse DNS scan to identify registered hosts
	+ Identify URLs and other external touch points from scan and OSINT
	+ Web presence evaluation
	+ Browse as a normal user through a web proxy to capture intelligence and understanding
	+ Identify known vulnerabilities and vulnerable conditions
* Exploitation
	+ Attempt to exploit targets based on current knowledge
	+ Perform situational awareness on target
	+ Attempt Local Privilege Elevation
	+ Attempt Domain or other system level Privilege Elevation

Stay-In:

* Post Exploitation
	+ Identify domain user/groups/memberships
	+ Identify IP space
	+ Identify file shares
	+ Establish persistence
	+ Use persistence plan to place agents on target systems
	+ Move Laterally
* Continued Lateral Movement
* Continued Enumeration

Act:

* Impact
	+ Modification of Transaction Records
* Impact
	+ Modification of customer order database

# APPENDIX D – Engagement objectives

As part of the Red Team engagement, I♥REDTEAMS, INC will be replicating the TTPs associated with the group known as <<insert group>>. Details have been provided in the threat profile listed in Appendix E. This threat has been known to exploit and attack the systems and networks servicing the transactional records, customer order database, and XYZ of organizations similar to <<customer>>.

Objective 1:

* Integrity of critical customer transactional data
	+ Determine ability of customer to <<insert>>
	+ Determine the system’s ability to <insert>>
	+ <<next>>

Objective 2:

* Integrity of customer’s order database
	+ Determine ability of customer to <<insert>>
	+ Determine the system’s ability to <insert>>
	+ <<next>>

Objective 3:

* Evaluation of Incident Response Procedures
	+ Determine ability of customer to <<insert>>
	+ Determine the system’s ability to <insert>>
	+ Identify potential entry vectors into <insert>>

# APPENDIX E – Threat profile

As part of the Red Team engagement, I♥REDTEAMS, INC will be replicating the TTPs associated with the group known as <<insert group>>. This threat has been known to exploit and attack the systems and networks servicing the transactional records, customer order database, and XYZ of organizations similar to <<customer>>.

<<Note this is a simplified example. A full threat profile will likely be several pages in length>>

Intent:

* Access and control to Financial Transaction Systems

Characterization

* Associated with the Russian Federation
* Active over multiple years
* Active primarily during Moscow business hours
* Targeted organization based in the financial sector
* Goal of gathering intelligence on financial based organizations

Attack and Delivery TTPs

* Phishing
* Watering-Hole
* Compromised web servers

Exploitation TTPs

* PDF Exploits
* JAVA and IE exploits
* Custom Binaries

Post Exploitation TTPs

* Local system enumeration for OS, username, processes, internet history, etc.
* Scan for known transaction related ports
* DLL injection to migrate into explorer.exe

Persistence TTPs

* Run key registry modifications
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\”TmProvider”
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\InternetRegistry