

# Documentation and Legalities

---



**Alexander Tushinsky**

Cybersecurity & Software Development Consultant

@ltmodcs alextushinsky.com



# Overview



- Documents
  - Non-disclosure Agreement (NDA)
  - Master Service Agreement (MSA)
  - Statement of Work (SoW)
  - Rules of Engagement (RoE)
  - Communications Plan
- Hacking the cloud considerations



# Document Overview

---





## Legal Requirements

- Protects pen tester and client
- Allows client to share privileged details

## Project Requirements

- Determines what's in scope
- Establishes work standards



## Pre-engagement

- Non-disclosure
- Master Service Agreement





## Engagement

- Statement of Work
- Rules of Engagement



# Non-disclosure Agreement

---





## Non-disclosure Agreement

- Legal document
- Confidentiality
- Provides legal protection





## Types of NDA Agreements

- Unilateral
- Mutual



## Details of an NDA

- Defines what information is covered
- Obligations for both parties
- Scope of information
- Length of time
- Exclusions
- Remedies

# Master Service Agreement

---





## Master Service Agreement

- Legal document
- Contract between parties
- Outlines responsibilities and terms





## MSA Details

- Confidentiality
- Outline of services
- Work standards
- Payment terms
- Warranties and indemnification
- Dispute resolution



# Demo



## Rapid7 MSA



# Statement of Work

---





## Statement of Work

- Defines the pen testing activities
- Can include time and pricing information







## SoW Details

- Project description
- Scope of work
- Outline of work to be performed
- Deliverables
- Acceptance criteria
- Financials and timeframe
- Disclaimers



# Rules of Engagement

---





## Rules of Engagement

- Protection for the ethical hacker
- Required before you begin
- Signed and accepted by the client



## RoE Details

- In-scope attack surface
- Out-of-scope items
- Disclaimer
- May incorporate a communications plan
- Client acceptance of terms





## Hacking the Cloud

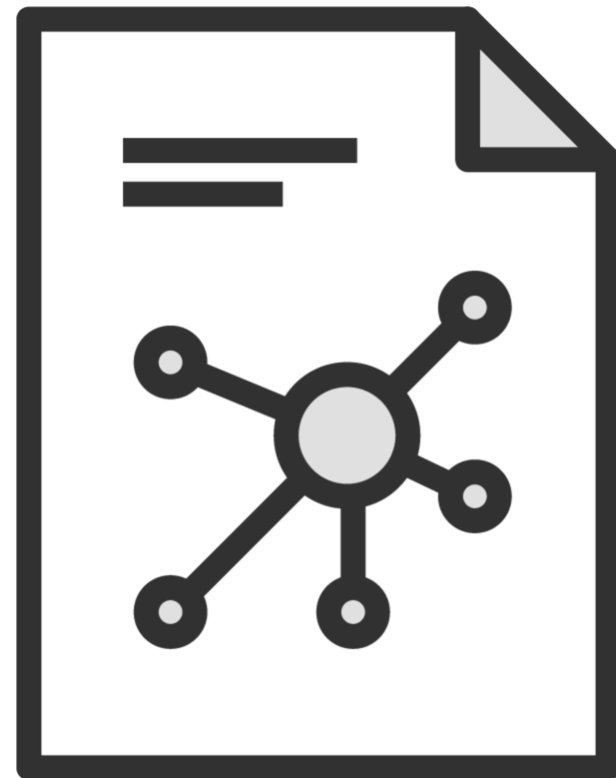
- Provider should be notified
- Provider may have their rules of engagement



# Communications Plan

---

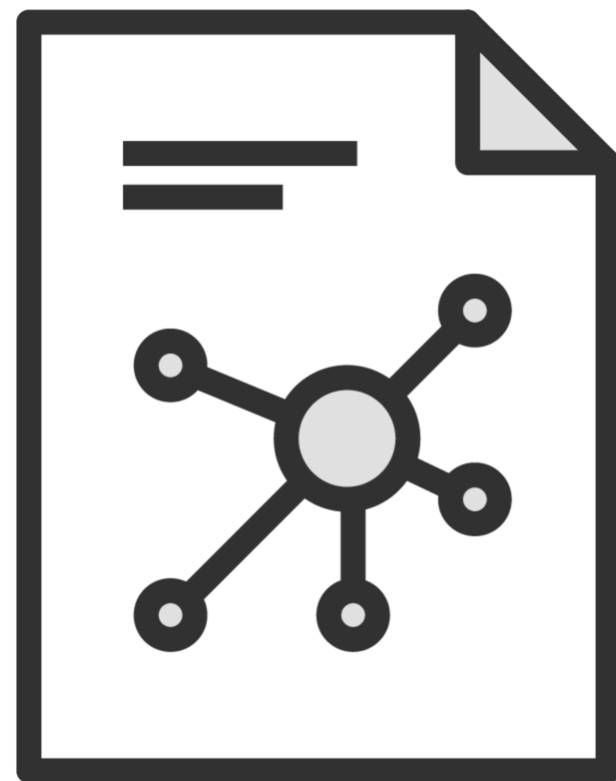




## Communications Plan

- Defines a clear path for communication
- Includes different levels of communication
- Should be agreed upon with the client





## Points of Contact

- General support and assistance
- Critical issues
- Reporting illegal activity
- Who gets the report
- Cloud Provider





## Hacking the Cloud

- May require approval by the provider
- Notification and scope should be given
- Identify support channels for help