NDA - GET OUT OF JAIL

A NDA is a Non-Disclosure Agreement. This is a vital part of any security testing you may undertake, be it internally but especially if you end up doing any external auditing of any type. You see when you do any audit looking for holes in a companies security posture, you are basically doing exactly what a normal attacker would do, and in case you have'nt realised it yet, there are laws against what attackers do. If you get caught undertaking any of these attacks you can expect to be treated as a hostile attacker engaged in cybercrime activities ... except that you have permission from the "victims" - the NDA. This is your "Get Out of Jail Free" -quite literally these days- which is your only proof of your good intentions.

The idea of this agreement is to protect the auditor and the company being audited, so that neither one of them gets the short end of the stick. I generally go as far as to suggest that the agreement should be signed by the auditor who will be doing the actual audit and -at least- a board member of the company being audited. Trust me, this saves hassles in the long run and ensures everyone knows what is expected of them.

The rest of this article is a template I have used for a NDA, and you can feel free to use it or change it as well if you think it will help you. Just be aware that I am no lawyer, so make sure you run this past someone who is so that you make sure you are'nt breaking any laws where you might find yourself doing the audit.

Non-Disclosure Agreement

This AGREEMENT made on the _____ day of _____ , _____ .
(day) (month) (year)

1.1 The parties
This Non-Disclosure Agreement exists between (hereafter referred to as "<company_name>")
_____ (Individual or company representative)

and (hereafter referred to as "Auditor") _____ (Individual or company representative)

1.2 Commencement date of the Non-Disclosure Agreement
This Non-Disclosure Agreement commences on the date indicated at the top of this page.

1.3 The purpose of the Non-Disclosure Agreement
This Non-Disclosure Agreement serves to protect confidential information and intellectual property developed for and owned by <company_name> as more fully set out in 2 below.

1.4 Tests
1.4.1 This confirms that <company_name> authorizes Auditor to perform tests on <company_name>'s networks from an external location. All tests will be performed only at specific dates that have been preauthorized by an elected <company_name> representative (Elected representative: _____).
1.4.2 It is understood and agreed that Auditor will execute all tests according to the best practice in the industry and that all measures will be taken to avoid damaging our networks and systems, as well as the data that it might contain within such networks and systems. If prejudice has been caused to the network or on the data stored on <company_name> systems due to negligence while performing the tests, Auditor will be held responsible and will compensate <company_name> for all damages of whatever nature and howsoever arising.
1.4.3 If, damages caused by Auditor were unforeseeable, Auditor will not be held responsible for the damages or any of its consequences.
1.4.4 If Auditor discovers any security breach in <company_name>'s networks, Auditor is obliged to document it, and advise <company_name>, or the <company_name>'s elected representative immediately upon such discovery.

1.4.5 The elected <company_name>'s representative will provide a list of IP addresses to be tested from time to time. Such IP's must be used only for the specific purposes of this project. Auditor will take appropriate measures to protect all confidential information regarding this project.
1.4.6 Auditor will provide <company_name> with a written report of the results of the tests within 7 working days after completion of all of the tests.

Meaning of Confidential information

For the purpose of this Agreement, "Confidential Information" means any and all information which has been or which will in future be disclosed by <company_name> to Auditor or ascertained by Auditor from <company_name>, including without limitation any secret knowledge, financial, technical or commercial information, specifications, procedures, contracts and any associated relationships with principals or other parties, manuals and other written information, trademark information of any nature, information about customers and methods of conducting, information concerning materials, marketing and business information generally, and other materials or knowledge of whatever description in which <company_name> has an interest in being kept confidential, know how, intellectual property, trade secrets, financial process, structure, but excluding any information that;

* Auditor is required to disclose in terms of a Court Order; and
* Is or becomes lawfully in the public domain otherwise than pursuant to a breach by Auditor of its obligations in terms of this Agreement.

Title to the Confidential Information

Auditor acknowledges that all right, title and interest in and to the Confidential Information disclosed to it by <company_name> or ascertained by it in any manner, vests in <company_name> and that the Auditor has no claim of any nature in and to that Confidential Information.

Undertakings

2.1 Auditor undertakes:

2.1.1 To use all Confidential Information disclosed to it or ascertained by it exclusively only for the purpose of carrying out its obligations in terms of the agreement to conduct the tests required by <company_name>, and only to disclose the information to its officers, employees and professional advisors if strictly necessary.
2.1.2 Not to publish, disclose or use for its own benefit or the benefit of any third party any of the Confidential Information that it may acquire.
2.1.3 To protect the confidential information ascertained using the same standard of care that Auditor applies to its own proprietary, secret or confidential information and to store and handle the Confidential Information in such a way as to prevent any unauthorized disclosure thereof.

2.2 In addition, Auditor undertakes to:

2.2.1 Maintain the confidentiality of any Confidential Information to which Auditor has gained access whether before or after the Effective Date of this Agreement. Auditor will not divulge or permit to be divulged to any person any aspect of such Confidential Information otherwise than may be allowed in terms of this Agreement;
2.2.2 Auditor shall take all such steps as may be reasonably necessary to prevent the Confidential Information falling into the hands of any unauthorized third party;
2.2.3 All documentation furnished to Auditor by <company_name> or acquired by Auditor will remain the property of <company_name>. Auditor will not make copies of any such documentation without the prior written consent <company_name> and upon termination of the work carried out by Auditor in terms of its obligations to <company_name>, any such documentation still in its possession will be destroyed;
2.2.4 Any material of a confidential nature which comes into the possession of Auditor or any of its agents or employees, or which is generated by Auditor, or one of its agents or employees, after the Commencement Date as a consequence of the work being carried out by Auditor:

2.2.4.1 shall be deemed to form part of the Confidential Information of <company_name>;
2.2.4.2 shall be deemed to be the property of <company_name>;
2.2.4.3 shall not be copied, reproduced, published or circulated by Auditor; and
2.2.4.4 shall be surrendered to <company_name> on demand, unless <company_name> provides its

prior written consent to the contrary.

3 Period of Confidentiality

The provisions of this undertaking and agreement shall remain in force indefinitely, unless a set period of time has been agreed upon beforehand. (Time Period:_____) .

SIGNED for and on behalf of <company_name> by its duly appointed officer

_____

(Individual or company representative - signature)

SIGNED BY

_____

(Individual or company representative's name - in print)