ZIRILIO
ASSESS • PROTECT • MANAGE

CLIENT DETAILS	
Organisation Name:	
ABN:	
Address:	
Contact Person:	
Cyber Policy Number:	

IT CONTACT PERSON	
Name:	
Email Address:	
Mobile Number:	
Phone Number:	

CLIENT TECHNICAL DETAILS	
Public IP Address / Range:	
Restrictions / Exclusions (if any):	

ZIRILIO TECHNICAL DETAILS	
Zirilio Source IP Address:	103.28.217.254 and 61.68.21.138

Definitions

1. The term 'Services' refers to an external vulnerability scan of Customer internet accessible infrastructure. All testing will be conducted without prior knowledge of the systems simulating access of a typical internet user.

Key Assumptions

1. Permission to Perform Testing is granted upon signing of this form.
2. Customer is the registered owner of the devices and IP addresses which will be included in the testing. Where the Customer is not the owner, permission has been sought from the respective owner authorising the abovementioned testing.
3. IP addresses are required to perform the testing. These must be provided prior to the commencement of the engagement.
4. Scanning will include up to 10 IP addresses.
5. Scanning against the devices listed above may run 24 hours per day, for the duration of that particular engagement. These tests will be non-destructive.
6. Zirilio does not guarantee that its recommendations will make the system 'hack proof'. New vulnerabilities at any future date may make the advice superfluous.
7. There may be some "tidy up" work for system administrators, such as the cleaning of errors, alerts and generated emails. There may be thousands of automated tests directed at the system.

These automated tests allow Zirilio to focus on where the problems lie within the system. All of these tests will be coming from the Source IP addresses provided for the purpose of the Security testing.

8. Emergency contact and backup contact numbers for Zirilio during the engagement are 1300 652 646 (toll free within Australia), +61 2 9921 1370 or +61 404 881 911 (outside Australia).

Permission to Perform Testing

1. Customer authorises Zirilio to perform the Services and acknowledges that the Services constitute authorisation to perform external internet testing of your computer systems.
2. Customer understands and agrees to the following:
   a. Excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;
   b. The performance and throughput of Customer system(s), as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded;
   c. Some operating system data may be changed temporarily as a result of probing certain vulnerabilities;
   d. Customer system(s) may hang or crash, resulting in temporary system unavailability;

Completion of Testing

1. Zirilio shall have fulfilled its obligations under this engagement when the following occurs:
   a. Zirilio has performed Security testing and has supplied a report detailing all findings and recommendations.

Authorisation

Customer Name:	
Authorised by:	
Title:	
Print Name:	
Date:	
Signature:	

About ZIRILIO

Growing compliance requirements demand a better approach to IT security. ZIRILIO assists clients to identify and manage business and security risk. ZIRILIO provides security assessments, protection solutions and management services as part of an end-to-end security platform solution.

ZIRILIO's unique approach provides customers with a clear, business-aligned security framework, a strategic allocation of budget, and a security road map for the future.