THE IEEE INTERCLOUD TESTBED ACCEPTABLE USE POLICY
March 2013

BACKGROUND

THE IEEE INTERCLOUD TESTBED ("the Intercloud Testbed") is an overlay testbed designed to allow researchers to experiment with cloud computing platforms and services that benefit from distribution across a wide geographic area. All uses of the Testbed should be consistent with this high-level goal.

This Acceptable Use Policy ("AUP") was directly derived from (1) THE NSFNET BACKBONE SERVICES ACCEPTABLE USE POLICY, June 1992, and (2) PlanetLab Acceptable Use Policy, PlanetLab Consortium, February 2004.

GENERAL PRINCIPLES:

1. The Intercloud Testbed services are provided to support open research and education in and among Global research and instructional institutions, research arms of for-profit firms, and others when engaged in open scholarly communication and research. Use for other purposes is not acceptable.

2. Use for for-profit, or for private or personal business is not acceptable.

3. Illegal use, as defined by the host country, is not acceptable.

GUIDELINES:

4. A good test when considering whether an experiment is appropriate for the Intercloud Testbed is to ask what the network administrator at your organization would say about the experiment running on your local site. If the experiment disrupts local activity (e.g., uses more than its share of your site's Internet bandwidth) or triggers complaints from remote network administrators (e.g., performs systematic port

scans), then it is not appropriate for the Intercloud Testbed. It is your responsibility to ensure that your use of the Intercloud Testbed falls within these constraints. This means you should debug your code in a controlled environment so you have confidence that its behavior will be within acceptable limits.

5. The Intercloud Testbed is designed to eventually allow experimental services to run continuously, thereby supporting an end-user community. However, there is no guaranteed Service Level Agreement for users. As a consequence, the Intercloud Testbed could indirectly support users that have not officially registered with the Testbed and may even be unknown to you (the service provider). It is your responsibility to ensure that your users understand this AUP and do not cause your service to violate the terms of this AUP. In particular, service providers should ensure that their users are not able to hijack the service and use it to attack or spam other nodes or network users.

6. The Intercloud Testbed is designed to support network measurement experiments that purposely probe Clouds and the Internet. However, we expect all users to adhere to widely-accepted standards of network etiquette in an effort to avoid complaints from network administrators. Activities that have been interpreted as worm and denial-of-service attacks in the past (and should be avoided) include sending SYN packets to port 80 on random machines, probing random IP addresses, repeatedly pinging routers, overloading bottleneck links with measurement traffic, and probing a single target machine from many Intercloud Testbed nodes.

7. It is likely that individual sites that host Intercloud Testbed nodes will have their own AUPs. Users should not knowingly violate such local AUPs. Conflicts between site AUPs and IEEE's stated goal of supporting research into wide-area networks should be brought to the attention of the Intercloud Testbed administrators. The expectations placed on sites that host Intercloud Testbed nodes are described in a companion document: **Hosting an IEEE Intercloud Testbed Node**.

8. While the central Intercloud Testbed authority is often the first point-of-contact for complaints about misbehaving services, it is our policy

to put the complainant in direct contact with the researcher that is responsible for the service.

9. The Intercloud Testbed provides absolutely no privacy guarantees with regard to packets sent to/from any points. In fact, users should assume that packets will be monitored and logged, for example, to allow other users to investigate abuse (see previous paragraph).

10. The Intercloud Testbed also does not provide any guarantees with respect to the reliability of individual nodes, which may be rebooted or reinstalled any time. Reinstalling a node implies that the stored information is wiped, meaning that users should not treat the local disk as a persistent.

11. Use existing security mechanisms. For example, all access to Intercloud Testbed nodes must be via SSH.

12. Do not circumvent accounting and auditing mechanisms (once these are implemented). This means you must associate your identity with the Intercloud Testbed account in which your service runs, and you must not do anything to obfuscate the audit trail.

13. No hacking attempts of the Intercloud Testbed nodes is allowed. This includes "red team" (hacker test) experiments. All access is non-root except as needed to Host an IEEE Intercloud Testbed Node.

14. Avoid spin-wait for extended periods of time. If possible, do not spin-wait at all.

15. Do not use your Intercloud Testbed account to gain access to any hosting site resources that you did not already have.

16. Do not use one or more Intercloud Testbed nodes to flood a site with so much traffic as to interfere with its normal operation. Use congestion controlled flows for large transfers.

17. Do not do systematic or random port or address block scans. Do not spoof or sniff traffic.