** DRAFT Internet2 Computer and Network Security Expectations DRAFT **

All Internet2 members should strive to meet community computer and network security expectations.

Specifically, Internet2 member institutions should --

* Have an **information security officer** and an adequately staffed information security team with executive management support, real operational authority, and sufficient budget.

* Have a comprehensive institutional **information security plan** (including information classification and PII stewardship policies), and an acceptable use policy (AUP).

* Firewall important administrative assets at the subnet level (as may be required by PCI-DSS and similar policies, and by audit practice), but **minimize or eliminate firewall obstacles** in front of non-administrative research and education users to preserve network transparency and protect network performance (encourage hardening at the host level).

* Have a site-wide **intrusion detection capability** (Snort, Bro, etc.), and be prepared to address any compromised systems.

* Be prepared to **cope with malware**: promote alternative operating systems; site license an antivirus product; facilitate patching of all software; offer help for infected users, including potentially deploying quarantine networks for online self-remediation of infected hosts, etc.

* **Manage password authentication**: deploy scalable institutional identity management/federated authentication; secure any apps still using unencrypted passwords; offer two-factor authentication for high security scenarios; secure the password reset processes.

* **Harden DNS** at your site. At a minimum, you should control any open recursive resolvers and work to develop a plan for deploying DNSSEC.

* **Control emission of spoofed network traffic** (do BCP38 filtering at the subnet level and at your network border).

* Work to **overcome potential security objections** that might inhibit deployment of critical advanced networking services (such as IPv6).

* Be active in the information security community, including participating in the **REN-ISAC.**

Questions/Comments/Feedback? Please feel free to contact Joe St Sauver, Internet2 Nationwide Security Program Manager (joe@internet2.edu or joe@oregon.uoregon.edu)

Draft v0.1, November 1st, 2010