NIMBioS
Security and Acceptable Use Policy

Version 1.1

Presented and Reviewed by NIMBioS Advisory Board, November 2008

Responsible Officer: NIMBioS Information Technology Manager

Effective Date: December 1, 2008

Date of Next Full Review: September 1, 2010

Errors or changes to: security@nimbios.org

Contents

1 Purpose

Primary goals of NIMBioS are to foster the maturation of cross-disciplinary approaches in mathematical biology and foster the development of a cadre of researchers who are capable of conceiving and engaging in creative and collaborative connections across disciplines to address fundamental and applied biological questions. NIMBioS will 1) address key biological questions by facilitating the assembly and productive collaboration of interdisciplinary teams; and 2) foster development of the critical and essential human capacity to deal with the complexities of the multi-scale systems that characterize modern biology.

All NIMBioS data, software tools, and other resources will be made freely and publicly available under creative commons or applicable open source terms, subject to the intellectual property rights of the owners of such resources. NIMBioS will strive to insure that NIMBioS-developed data and software are:

- Suitable for appropriate use based on the types of users.
- Accompanied by adequate documentation and metadata to enable their use.
- Checked and validated for quality control and include provenance where possible.
- Cataloged according to community-developed metadata standards.
- Discoverable and accessible using web services and open standards protocols.
- Registered with appropriate authoritative repositories or information clearing houses.
- Accessible to the community under policies that maximize opportunities for their use and redistribution.

The purpose of this document is to describe and establish the set of policies relating to confidentiality, integrity, and availability of NIMBioS services and resources while maintaining the goals outlined above.

NIMBioS will primarily utilize the networking and computing infrastructure of the University of Tennessee. NIMBioS assets and personnel will adhere to University of Tennessee system policies regarding the use of information technology resources in NIMBioS-sponsored activities. These policies are described in the following UT policy documents.

University of Tennessee Information Technology Policy #IT0110, Acceptable Use of Information Technology Resources. This policy governs the use of information technology resources in an atmosphere that encourages free exchange of ideas and a commitment to academic freedom, based on principles of honesty, academic integrity, and respect for others. The policy seeks (1) to protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under

federal and state law, including the Tennessee Public Records Act; (2) to ensure that the use of electronic communications complies with the provisions of university policy and state and federal law; and (3) allow for the free exchange of ideas and support of academic freedom.

University of Tennessee Information Technology Policy #IT0115, Information and Computer System Classification. This policy describes protection requirements for the confidentiality, integrity, and availability of electronic information, and provides a guide for identification of information assets and determination of the level of risk associated with information disclosure, alteration, and/or destruction.

University of Tennessee Information Technology Policy #IT0120, Secure Network Infrastructure. This policy provides the definitions for creation and maintenance of a secure systems infrastructure, including technical, administrative, maintenance, computer systems refresh, and operations solutions for information technology network infrastructure security.

The standards and policies set forth within this document will complement the University of Tennessee system policies. If any overlapping or conflicting policy is set forth within this document, NIMBioS will defer to the policy with the more stringent security requirements. In addition, state and federal laws may have jurisdiction, in which case NIMBioS will be required to abide by all state and federal laws relating to its applications, systems, and networks. The intent of this document is to specify and highlight policies that are particularly important to NIMBioS and not to detail every known situation, circumstance, and process relating to IT security.

2 Access Control

The IT Management team is ultimately responsible for determining the appropriate level of access to ensure the confidentiality, integrity, and availability of NIMBioS systems and resources to the NIMBioS participants and the general academic community. This section presents a broad view about the organizations access control policy. However, due to the diverse nature of participation in NIMBioS, access will be determined based upon the type of NIMBioS activity involved.

Individual Responsibility

Every NIMBioS staff, researcher, participant, and user is responsible for protecting the access to any information and systems that has been granted to him or her. If there is any suspicion of a breach of access, the IT Management team should be contacted immediately so that an appropriate investigation can be performed.

Every NIMBioS workstation and laptop should be password protected.

Access Notification

A distinct and clear message will be displayed to users if an application, system, or network is restricted from the general public, including the applicable Acceptable Usage Policy.

Authentication and Authorization

Single sign-on based authentication and authorization mechanisms will be employed according to the needs of the application, system, and network. The NIMBioS internal systems that are deemed critical infrastructure will employ a higher level of security in order to maintain highly restrictive access.

NIMBioS Working Groups and Investigative Workshop teams may employ temporary authentication and authorization schemes for the benefit of rapid development and prototyping. As applications and systems migrate under the professional services of the IT Management team, these schemes will be standardized or removed, as appropriate, to ensure consistency for the NIMBioS community and general public.

Intellectual Property and Copyright

NIMBioS will make every effort to comply with the intellectual property rights and copyrights of software, source code, data, documents, and other relevant materials. Participating researchers and NIMBioS visitors must declare and disclose any intellectual property rights and associated copyrights to NIMBioS in writing before any contributed material to be used in NIMBioS activities can be utilized by NIMBioS. For further details refer to the document titled *NIMBioS: Intellectual Property Policy* (under development).

3 Awareness and Training

NIMBioS will provide security documentation for all end-users. All security-related documentation, including this security policy, will be posted on the NIMBioS website. If necessary, more detailed security documentation and training will be provided, depending on the nature of the applications, systems, and networking utilized. Operations and Infrastructure documentation and training will be provided to staff and researchers who will be directly accessing core infrastructure services.

4 Audit and Accountability

The IT Management team is ultimately responsible for managing the security audits of NIMBioS activities. This will encompass source code, libraries, shared data contributions from NIMBioS participants and collaborators where applicable.

Responsible Officers

The IT Manager is the designated information security officer (ISO) and the liaison for NIMBioS and participating organizations.

Responsible Organizations

All NIMBioS assets (e.g. servers, data stores, desktops etc.) subscribe and adhere to the University of Tennessee security policies, in conjunction with those set forth by the NIMBioS security requirements. Ultimately the NIMBioS IT Management Team will be responsible for security of its assets and will work cooperatively with local security organizations to share relevant information.

Acceptable Use

All NIMBioS assets and personnel will adhere to the Acceptable Usage Policy (AUP) for computer and network use set forth by the University of Tennessee, noted above.

For services and resources available through NIMBioS, an AUP will be established based on the specific resource and service being provided, and users will be required to comply with policies to gain access.

Servers

All NIMBioS servers will record login and connection information including the remote host, timestamps, protocols, and user login information. If applicable, application and server logs will be consolidated in a central logging system. Server logs will be maintained for a minimum of one year.

Applications

All third-party applications (ones not developed by NIMBioS) will have logging enabled as appropriate. Applications that require authentication or authorization should capture connection information, including remote host, timestamps, and user login information and, if applicable, display the relevant Acceptable Usage Policy.

Applications that result from the research and education activities at NIMBioS will eventually be made available for general public access, subject to arrangements that protect the Intellectual Property rights of the owners. During the migration process, the IT Management Team will evaluate the security of these applications and perform penetration testing. If applicable, the data and any data collection process will also be evaluated to ensure that there are no issues related to privacy, confidentiality, copyright, or patents.

Audit

Ongoing traffic pattern analysis and intrusion detection systems (IDS) will be employed to perform host-based intrusion detections (HIDS) and network-based intrusion detection (NIDS).

Cursory audits of the server logs will occur on a periodic basis. If a situation warrants immediate attention, such as a potential security breach, then the IT Management team will perform a more detailed audit.

5 Incident Response

The IT Management team will investigate any reports of security breaches. If the investigation results in a credible claim, the IT Management team will take necessary action to remove or isolate the threat in conjunction with University of Tennessee security personnel as appropriate. The IT Management team will make a best effort to minimize any downtime. In the event that a downtime must occur for a significant duration, then appropriate notifications will be sent and posted to the website.

All security-related incidents should be reported to security@nimbios.org. For active threats requiring urgent and secure communication, call: 1-865-974-9363.

6 Incident Reporting

As part of an incident response, the IT Management team will notify all responsible authorities on the occurrence of the incident and actions being taken to mitigate the situation. This will include the University of Tennessee and participating authorities, funding agencies and law enforcement agencies. e.g. UT's system for reporting security incidents: http://security.tennessee.edu/incident.shtml

Cognizant officer and authorities at the National Science Foundation (NSF) will be informed of any incident that involves misappropriation of copyrighted material and incidents escalated to involve law enforcement agencies. NSF will be informed utilizing the email address of the assigned NSF Program Manager. For incidents requiring immediate attention from NSF, the responsible program manager at NSF will be contacted via telephone by the NIMBioS director.

Occurrence of all incidents will be logged by the IT Management team for evaluation and audit.

7 Maintenance

Maintenance of applications and operating systems is expected to happen periodically. The IT Management team will be responsible for managing the maintenance process for NIMBioS and for executing the maintenance for the core infrastructure systems. If any server requires a hardware or system update and results in a system reboot, loss of connectivity, or otherwise impacts users, then the IT Management team will plan for scheduled downtime for the servers in question. The IT Management team will make a best effort to minimize the impact and notify the affected users of the scheduled downtime.

Server operating systems maintenance and patching will be performed using a centralized system management console. Desktops and laptops will be managed using similar systems (e.g. LANDesk, Apple remote desktop). End-users of laptops and desktops that are not managed and maintained under centralized systems (e.g. due to offsite locations or firewall restrictions) are expected to periodically check for updates on their operating systems and supporting applications (i.e. Windows Updates, Mac OS updates, and anti-virus signatures). If the end-user is not familiar with updating the operating system and applications, the IT Management team will provide training on these tasks.

8 Physical Protection

NIMBioS servers will be located in a secure, limited access, and monitored data center. Workstations and laptops should be physically secured to an immovable or difficult-to-move object whenever possible. To secure a physical system, a special cable with a locking mechanism should be used, such as a Kensington lock.

Loss or theft of physical NIMBioS assets will require contacting law enforcement (using NIMBioS incident reporting procedures).

9 Planning

NIMBioS will formally re-evaluate and document all security, business continuity, and backup and recovery plans at least every six months, including this security policy document. The re-evaluation process may occur more frequently and policies may be modified in response to changes in internal requirements, the external environment, or risk assessments.

10 Risk Assessment

A formal risk assessment process for the servers, workstations, laptops, and network equipment will be conducted every six months. This process will include participation in risk assessment procedures and security scans conducted by the University of Tennessee's Security Office.

11 System and Information Integrity

To ensure business continuity and information integrity, NIMBioS will adhere to all relevant University of Tennessee disaster preparedness and recovery policies. Credentials and passwords for NIMBioS equipment will be held in an encrypted document that will be in possession of the IT Manager.

12 References

Security policies documents from the following organizations were referred to while developing this document:

University of Tennessee Information Technology Policy #IT0110, Acceptable Use of Information Technology Resources.
https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=IT0110

University of Tennessee Information Technology Policy #IT0115, Information and Computer System Classification.
https://my.tennessee.edu/pls/portal/policy.portlet_policy_view.policy_print?p_refid=255

University of Tennessee Information Technology Policy #IT0120, Secure Network Infrastructure.
https://my.tennessee.edu/pls/portal/policy.portlet_policy_view.policy_print?p_refid=252

Iplant Collaborative Security Policy
http://wiki.iplantcollaborative.org/public/images/8/87/IPlant-Collaborative-Security-Policy-V1-final.pdf