

# iLab Solutions Security Management Document

Information security policy and description of operational safeguards

June 9, 2011

## Contents

<b>ABOUT ILAB SOLUTIONS .....</b>	<b>3</b>
<b>ILAB SECURITY MANAGEMENT .....</b>	<b>3</b>
1 SCOPE .....	3
2 PURPOSE .....	3
3 APPROACH .....	3
<b>3.1 Overview .....</b>	<b>3</b>
3.1.1 Hardware Protection .....	4
3.1.1.1 Hosting provider security .....	4
3.1.1.1.1 Prevention against unauthorized access: .....	4
3.1.1.1.2 24/7 Information availability .....	5
3.1.2 Application Protection.....	5
3.1.2.1 Authentication .....	5
3.1.2.1.1 Authenticated system access.....	5
3.1.2.1.2 Strong passwords.....	5
3.1.2.1.3 Inactive session termination .....	5
3.1.2.1.4 Password expiry .....	6
3.1.2.1.5 Server access.....	6
3.1.2.2 Authorization .....	6
3.1.2.2.1 Data partitioning.....	6
3.1.2.2.2 Data validation checks .....	6
3.1.2.2.3 iLab access to information .....	6
3.1.2.3 Auditing .....	6
3.1.2.3.1 Auditing User Activity .....	6
3.1.2.4 Product development process .....	7
3.1.2.5 Enterprise grade data protection and encryption .....	7
3.1.3 Network and Monitoring.....	7
3.1.3.1 Network protection.....	7
3.1.3.2 Monitoring .....	8

## About iLab Solutions

iLab Solutions develops, deploys, and markets software designed to help labs at research institutions streamline their day-to-day activities. The iLab system has two parts, a Materials Management module and a Core Facility Management module, both of which are offered as a web-based subscription with ongoing and real-time support over the life of the subscription.

## iLab Security Management

### ***1 Scope***

The purpose of this document is to outline the strategies and control mechanisms that form the Security Management practices of the iLab Solutions (“iLab”) service (the “Service”). Additionally it provides a description of the information security safeguards provided by third-party tools and vendors used by iLab.

### ***2 Purpose***

The purpose of the Security Management practices is to ensure that information stored and accessed through the iLab Service is managed such that:

- All information is available and usable when required.
- All information is observed by/disclosed to only those individuals who have a right to know it.
- All information is complete, accurate and protected against unauthorized modification.
- All information exchanges can be trusted.
- Where appropriate, information access and modifications are tracked for audit purposes.

### ***3 Approach***

iLab works continuously with researchers, lab-managers and administrators to identify information-security needs, and with experts in the hardware security, application security and network security to update the Service to meet those needs.

#### **3.1 Overview**

iLab’s approach to security employs multiple fail-safe strategies against multiple types of security threats including:

- Damage or unauthorized access to hardware
- Low level vulnerabilities such as Buffer overflow attacks
- Application or OS vulnerability and misconfiguration
- Data malformation attacks, including SQL injection, and XSS

- Session fixation attacks
- Sniffing/eavesdropping
- Network attacks

iLab takes measures across the three layers of the application framework in order to maximize security precautions:

- Hardware protection
- Application protection
- Network protection and monitoring

### **3.1.1 Hardware Protection**

iLab locates all hardware in SAS 70, Type II certified facilities, which meet the most stringent civilian hardware uptime and security standards. Facilities ensure 24/7 information availability, prevent against unauthorized access to hardware, and provide protection against hardware damage from accidents and natural disasters.

#### **3.1.1.1 *Hosting provider security***

iLab confirms that hosting providers employ the following mechanisms and security checks.

##### **3.1.1.1.1 Prevention against unauthorized access:**

- All employees undergo criminal background, credit and social security checks, as well as employment verification.
- Access to the network infrastructure is limited to 3rd party facility managers and network engineers.
- Support staff use individually generated public/private key authentication, which is more secure than traditional passwords.
- Multi-layered access control points.
- Biometric identification and badge scanners.
- Secure cages and locked racks.
- No unauthorized package deliveries.
- Physical access controls.
- Application and Database operating system users are required to authenticate with a valid private key before being granted access.
- Systems that store or process customer data are properly configured and adequately hardened
- Vendor-supplied defaults for system passwords and other security parameters are never used. Vendor-supplied defaults are changed before installing a system on the network.
- All remote administrative access protocols are encrypted.
- SSH is used for remote administration of Linux/Unix systems and SSL/TLS for web-based management consoles.
- DenyHosts is used to expire logins after repeated login failures to prevent brute force attacks.

- Root logins over ssh have been disabled on all public facing systems.
- All allowed traffic is based on a whitelist of allowed ports and protocols.

#### **3.1.1.1.2 24/7 Information availability**

- The hosting provider maintains an internal Network Management Suite (NMS) that alerts issues associated with customer equipment. This system is designed to automatically route and escalate issues to the proper staff who can resolve the issue.
- All machines are scanned at a minimum of every 5 minutes with any outage triggering instant action.
- Industry standard configuration and hardening standards are used for all systems such as those from SANS Institute, Center for Internet Security (CIS) or National Institute of Standards (NIST).
- Facilities use FM-200/ECARO-25 gas based fire suppression that is zone based and allows the suppression of fires in the facility without the damaging use of water based sprinklers. Dry chemical extinguishers are located throughout the facility for human intervention pre-action on the gas suppression systems.
- Hosting provider SLA ensures 100% uptime for network connectivity, power and primary DNS.
- All failed hardware replaced within a 2 hour window.

### **3.1.2 Application Protection**

The iLab Service is built on an application stack which integrates best-of-breed operating systems, database-servers and application-servers. iLab continuously updates all components of the stack with the latest security patches and releases to prevent unauthorized attempts to gain access or control of the Service.

#### **3.1.2.1 Authentication**

Measures aimed at ensuring that only authorized individuals can access the iLab Service.

##### **3.1.2.1.1 Authenticated system access**

Accessing the iLab Service requires authentication with a login identifier and password. All login identifiers are unique and all passwords are always encrypted. iLab logs all successful and failed system login attempts to identify suspicious activity trends.

##### **3.1.2.1.2 Strong passwords**

The iLab Service requires that all passwords be at least 6 characters and include a combination of alphabetic and numeric characters. iLab salts and encrypts all stored passwords.

##### **3.1.2.1.3 Inactive session termination**

In order to mitigate the risk of unauthorized access from a user forgetting to log out of the iLab Service, iLab automatically terminates all sessions after 120 minutes of "inactivity".

#### **3.1.2.1.4 Password expiry**

iLab offers customers the option to define the frequency with which users must change their passwords in order to protect against password guessing, cracking or threat.

#### **3.1.2.1.5 Server access**

Only registered iLab administrators have access to the iLab database servers, application servers and operating systems with a secure password. In addition, iLab audits all server access attempts.

### **3.1.2.2 Authorization**

Measures aimed at ensuring that only authorized users can access specific pieces of information in the iLab Service.

#### **3.1.2.2.1 Data partitioning**

Users can control access to data at a granular level, including providing access to individual “information assets” such as files, with the ability to specify which others users are allowed to read, modify, and share each information asset. In addition, administrators can control which users have access to project, lab or department information.

#### **3.1.2.2.2 Data validation checks**

iLab tests all user-generated input for malformed input, which prevents unintended code execution and inappropriate access to information in files or databases. We prevent SQL injection and Cross-Site Scripting (XSS) attacks by using parameterized queries, applying stringent data validations and sanitizing all user input before use.

#### **3.1.2.2.3 iLab access to information**

All iLab access to user-generated content is controlled by the following policies and conditions:

- iLab staff may only access user generated content for the purpose of user support.
- Only iLab’s Chief Operating Officer (“COO”) and Chief Software Architect (“CSA”) have default access to information in the Service; all other iLab staff must work through one of these two people in order to gain data access.

### **3.1.2.3 Auditing**

Measures aimed at tracking access and modification of information in the system.

#### **3.1.2.3.1 Auditing User Activity**

iLab maintains detailed logs of access to and modification of all information in the Service. Audit entries capture:

- Username
- Date and time of modification
- A description of the action taken

- Identity or name of affected data, system or resource.
- Old value/new value information for changed data, where appropriate
- Audit trails are protected from unauthorized modifications.

#### **3.1.2.4 Product development process**

- All software applications are developed based on industry best practices and incorporate information security throughout the development lifecycle.
- All system and software changes are tested before deployment.
- Separate development, staging, and production environments are maintained.
- Production data is never used for testing or development.
- All test data and accounts are removed before production systems become active.
- All temporary accounts, usernames, and passwords are removed before an application is released to customers.
- Source code is reviewed and applications are tested periodically for security vulnerabilities, especially those related to:
  - Invalid login and authentication
  - Cross-site scripting (XSS) attacks
  - Injection vulnerabilities (for example, SQL injection)
  - Cross-site request forgeries (CSRF)
  - Improper error handling
  - Logical data separation to ensure that one customer's data is not visible to others even in the case of programmer error.
  - Customer data is protected from corruption even in case of programmer error.

#### **3.1.2.5 Enterprise grade data protection and encryption**

- Data backups are bulk encrypted using the AFS algorithm immediately upon creation.
- Fully documented key management processes and procedures are used for encryption keys.
- Keys are generated using a cryptographically strong pseudorandom number generator.
- Encryption keys are never transmitted via unsecure protocols.
- Encryption keys are changed periodically, at least annually.

### **3.1.3 Network and Monitoring**

#### **3.1.3.1 Network protection**

Multilevel security products from leading security vendors and proven security practices ensure network security.

- To prevent malicious attacks through unmonitored ports, external firewalls allow only ssh, http, and https traffic on specific ports.
- All data is encrypted in transfer to prevent sniffing/eavesdropping attacks.
- Web based applications that collect or display customers data do not allow access via un-secured HTTP and redirect all HTTP connections to HTTPS (SSL/TLS).
- Remote administration protocols other than SSH and SSI./TIS are tunneled through a Virtual Private Network (VPN). Telnet. FTP. VNC, or SNMPv1 are never used for remote administration.

- Router Access Control Lists (ACLs) are configured to refuse any type of network connection that is not explicitly allowed by the ACL rules.
- The ability to make changes to the router ACLs is limited to one single user account.
- High availability routers are in place and configured to provide failover services in the event of primary router failure.

### **3.1.3.2 Monitoring**

iLab has implemented systems to monitor security and immediately alert the iLab team of suspicious activity to allow a response before the first level of defense is breached.

Additionally, the enterprise monitoring application on host machines is configured to alert support staff personnel when pre-defined system thresholds are exceeded that include, but are not limited to, the following:

- Disk space.
- CPU load.
- Memory utilization.
- Backup success and failure.
- Connectivity and availability.
- Hardware issues.