Research Labs Security Policy

Contents

1.0 Purpose

This policy establishes information security requirements for research laboratories at the Department of Computer Science, University of Cyprus, to ensure that the Departmental and University information technology infrastructures and confidential information are not compromised, and that IT services, computing assets owned by the Department and the University and their interests are protected from research and testing activities conducted in the labs.

2.0 Scope

This policy applies to all internally networked labs, the Department's faculty, staff, students and third parties who have access to the Department's labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the DMZ Lab Security Policy.

3.0 Policy

3.1 Ownership Responsibilities

1. Each Lab Director (a designated Computer Science faculty member) will designate a "Lab Administrator" who serves as the primary point of contact for information technology issues occurring within the lab. Optionally, a secondary point of contact (POC) may be assigned. The "Lab Administrator" may also have larger responsibilities, such as administration and management of the computing infrastructure within the lab.
2. The Lab Director is responsible for granting and revoking physical access to the lab. Access to labs will only be granted to those individuals with an immediate need as

defined by their affiliation with the lab. The Lab Director is also responsible ensuring that physical access to the lab spaces is terminated when it is no longer required and that all computing assets assigned to the individual are recovered at the time that access is terminated.

3. Lab Administrators are responsible for maintaining up-to-date administrator and POC information with the Departmental Support Organization (DSO). Lab Administrators are also responsible for maintaining updated lists of computing equipment assignments and user contact information for their designated lab.
4. Lab Administrators or their designated backup will be expected to be available during normal University business hours. If the Lab Administrator or backup is unavailable, in case of an emergency, actions will be taken without their involvement.
5. Lab Administrators are responsible for implementing the security procedures, developed by the DSO and adopted by the Department, in their respective labs. Lab Administrators are also responsible for adherence to all University IT policies and associated procedures. Where policies and procedures are undefined or unclear, Lab Administrators should consult with the DSO or the University security office as soon as practical and preferably before taking actions. The following policies are particularly important: Acceptable Use Policy, Password Policy, Wireless Security Policy, Anti-Virus Policy, and physical security.
6. Lab Administrators, in coordination with the DSO, are responsible for establishing an authentication and authorization system for user accounts in the Research Lab.
7. Lab Administrators, in coordination with their Lab Directors and the DSO, are responsible for disposing the IT assets under their control in accordance with defined University procedures.
8. It is possible for the Lab Directors to assign lab administrator functions to the Departmental Support Organization in which case all Lab Administrator functions will be owned by the DSO.
9. The Departmental Support Organization (DSO) is responsible for:
    1. Developing and maintaining the applicable security procedures and guidelines associated with this policy.
    2. Interfacing with the University Information Security Office (UISO) on matters of information security within the Department.
    3. Developing appropriate training on security policies, procedures and guidelines to Department Lab Administrators, Technical support staff and end users.
    4. Consulting with Department faculty, staff and students on matters relating to information security within the Department.
10. The DSO will maintain an access control device between the Departmental production network and the lab equipment. The DSO will work with the Lab Administrator to establish appropriate access control lists (ACL's). The Lab Administrator will be responsible for publicizing the ACL to all the faculty and students who are associated with the lab. Any changes to the access control list must be submitted in writing to the DSO (preferably within the DSO HelpDesk) including appropriate justification and having the approval of the Lab Director. The DSO will consult with the Lab Administrator and University ISO to evaluate the proposed ACL change within two business days. If the requested change is deemed appropriate, the DSO will implement the request within two business days.
11. The DSO and/or University ISO reserve the right to immediately interrupt lab connections that negatively impact the Departmental/University IT network and or services or pose a security risk, internal or external.

12. A “primary user” will be designated by the Lab Administrator for each network-capable device. Network-capable devices include (but not limited to) computers, printers which include a network card and switches/hubs/routers. While the Lab Administrator has the overall responsibility for maintaining devices located in the lab, the primary users are responsible for maintaining and securing the equipment that is assigned to them. This includes:
    1. Providing his/her contact information to the Lab Administrator including current email address and phone number. The primary user is responsible for notifying the Lab Administrator of any changes to their contact information.
    2. Establishing and maintaining strong, confidential passwords for all local user accounts on the assigned systems in accordance with the Password Policy. Only the primary user and the Lab Administrator should have knowledge of the root or administrator account password for the system.
    3. Maintaining standards of responsible computer usage as documented in the Acceptable Use Policy.
    4. Ensuring that any third-party software loaded on computers under their control is properly licensed. Unauthorized copying or distribution of copyrighted software or other copyrighted material is specifically prohibited.
    5. Following the standards and guidelines for proper systems administration as provided by the DSO including the physical administration and repair and hardware reconfiguration procedures of equipment.
    6. Ensuring the physical security of computing assets under his/her control. This includes informing the Lab Administrator when a computer is physically moved, reconfigured or reassigned to another individual.
13. The "primary user" is responsible for any security incidents that involve hardware under his/her control as a result of wilful violation of policy/procedures or negligent system administration
14. Research Labs are designed to provide support to the Department's and University’s academic research mission and should not be used to provide production IT services. Production services are defined as ongoing and shared services to users outside the lab. Examples of this would include email services, externally-accessible websites, file serving, or shared databases. All production services should be managed by the DSO staff.
15. The DSO will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified. Waiver requests (including justification) must be submitted in writing to the DSO (preferably via the DSO HelpDesk and have the Lab Director's approval). If a waiver request is denied, the DSO will attempt to work with the requester to provide an acceptable alternative solution if feasible.

3.2 General Configuration Requirements

1. All unmanaged lab computers must be segregated from the Department's production network by an access control device. Lab network devices (including wireless) must not cross-connect the lab and the Department’s or University’s production networks. Request for waivers to this requirement must be submitted to the DSO.
2. Any requested changes to the lab ACL’s must be reviewed and approved by the DSO. Requests will be reviewed within two business days. Approved changes will be implemented within an additional two business days.
3. Users within the labs are prohibited from engaging inappropriate usage of network resources, including unauthorized port scanning, packet capture, network auto-discovery,

traffic spamming/flooding and/or access to or distribution of copyrighted materials. If these activities are required to support research efforts, users must request prior approval from the DSO.

4. Traffic between production networks and research lab networks, as well as traffic between separate lab networks, is permitted based on needs and as long as the traffic does not negatively impact any Departmental or University production or external networks. Labs must not advertise network services that may compromise production network services or place confidential or copyrighted information at risk.
5. The DSO reserves the right to audit all lab-related network traffic at any time, and without notice, including but not limited to performing inbound and outbound packet sniffing and reviewing firewall access logs. Lab Administrators and the DSO reserve the right to periodically audit lab computers to ensure adherence to the requirements of section 3.1 above.
6. All external network connection requests must be reviewed and approved by the DSO prior to connecting the equipment to the network.
7. Any equipment requiring an external network connection must not be directly connected to Departmental or University production networks via a wired/wireless connection or any other method. Access must be controlled by the DSO on all external network connections.

4.0 Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action up to and including termination of employment or expulsion from the University in accordance to the disciplinary regulations adopted by the University.

The Department, also, reserves the right to take immediate action, in accordance to its adopted policies, to address any violations of this policy. Action may include any of the following: suspension or termination of user's access, termination of assistantship and/or employment agreements and/or referral to the appropriate University disciplinary process.

5.0 Definitions

ACL
: Access Control List. A filtering mechanism by which access to a network, device or system is controlled by using a rule set on a per application/network port basis.

Access Control Device
: A device that restricts inbound and/or outbound network traffic based on a defined rule set (ACL). It can be a specialized hardware device (e.g., CISCO PIX firewall), a router with access control lists or similar security devices approved by the DSO.

Department
: Department of Computer Science, University of Cyprus

Departmental production network
: Network infrastructure, managed by the DSO which serves routine academic and administrative computing needs of the Department faculty, staff and students.

Departmental Support Organization (DSO)
: The Department's support organization (support group/team) that manages the computing infrastructure for the Department including networks.

DMZ
: DeMilitarized Zone. A special network residing outside the internal network security zone where services provided are visible to the outside world.

External network
: Any network which is logically located outside the boundary of the Department's firewall device and not managed by DSO staff. An external network connection is one which directly connects an internal lab network to the Internet without crossing the Department's gateway.

Internal network
: A Network which is logically located inside the boundary of the lab network access control device (i.e., lab network side of firewall).

Lab
: A Lab is any non-production environment, intended and specifically designed for academic research and development/testing.

Lab Administrator
: The individual responsible for supporting and maintaining IT infrastructure in the lab area. The Lab Administrator is appointed by the Lab Manager/Director.

Lab Manager/Director
: Individual (usually a faculty member) responsible for defining and directing research activities within the lab.

Managed computer
: A computer which is managed by the DSO staff. These computers are primarily used for administrative computing tasks (e.g., email, document editing, web browsing) and are generally configured by the technical support. These include all faculty member office equipment.

Primary user
: The individual who has responsibility for ensuring the security of all computers assigned to him/her. Primary users have access to the root or administrator-level accounts on the computer.

University ISO (UISO)
: University of Cyprus Information Security Office

Unmanaged computer

A computer which is not configured or administered by the DSO staff. These computers are typically used for research, development and testing and may be software reconfigured at will.

6.0 Revision History

Revision 1.0

Preliminary issue – 23 Febrary 2009

Revision 1.0a Minor corrections and additions on preliminary issue - 12 March 2009