Cyber Security Policy

ArtSciLab

Spring 2025

Lead Author:

Collins Mwange

Co-Authors:

Farai Chivasa

Venkatesh Prasad

ARTSCILAB

HARRY W. BASS JR. SCHOOL OF ARTS, HUMANITIES, & TECHNOLOGY
THE UNIVERSITY OF TEXAS AT DALLAS

ArtSciLab

POLICY MANUAL

Subject: **CYBER SECURITY POLICY**

Approved: Under Review - Jan 15, 2025 Effective Date: TBD

Table of Contents

1 DEFINITION

The use of the term “lab” is in reference to the following entity: ArtSciLab. This is a transdisciplinary laboratory based in the Harry W. Bass Jr. School of Arts, Humanities, and Technology at The University of Texas at Dallas.
The use of the term “Policy” is in reference to this cyber security policy document.

2 INTRODUCTION

This policy is a formal set of rules by which those people who are given access to lab technology and information assets must abide by.

The policy serves several purposes. The main purpose is to inform lab users: faculty, staff, students, visiting researchers, and other authorized users of their obligatory requirements for protecting the technology and information assets of the lab. The policy describes the technology and information assets that must be protected and identify many of the threats to those assets.

The policy also describes the user’s responsibilities and privileges, what is considered acceptable use, and what the rules regarding Internet access are. The policy answers these questions, describes user limitations, and informs users that there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the lab computer systems and network.

3 WHAT WE ARE PROTECTING

It is the obligation of all users of the lab systems to protect the technology and information assets of the lab. This information must be protected from unauthorized access, theft, and destruction. The technology and information assets of the lab are made up of the following components:

- Computer hardware, CPU, Email, websites, application servers, PC systems, printers, TV screens, projectors, application software, system software, etc.
- System Software includes operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the lab. This includes custom written software applications, and commercial off the shelf software packages.
- Video and audio recording equipment includes cameras, microphones, camera stands, and associated software and tools.

3.1 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The lab shall classify the information controlled by them. The lab director shall review and approve the classification of the information and determine the appropriate level of security to best protect it. The lab manager shall foresee the classification of information maintained by the lab.

3.2 Classification of Computer Systems

Security Level	Description	Example
RED	This system contains confidential information – information that cannot be revealed to personnel outside of the lab. Even within the lab, access to this information is provided on a “need to know” basis. The system provides mission-critical services vital to the operation of the lab. Failure of this system may have life threatening consequences and/or an adverse monetary impact on the operation of the lab.	Server containing confidential data and other department information on databases.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access Server and application(s). Management workstations used by systems and web administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
BLACK	This system is externally accessible. It is isolated from RED or GREEN systems by a security system (firewall). While it performs important services, it does not contain confidential information.	A public Web server with non-sensitive information.

3.3 Local Area Network (LAN) Classifications

A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system and all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest-level systems attached to it.

4 ACCESS DEFINITIONS

Externally accessible to the public. The system may be accessed via the Internet by persons outside of the lab without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to "ping" the system from the Internet. The system may or may not be behind a security system (firewall). A public Web Server is an example of this type of system.

Non-Public, externally accessible. Users of the system must have a valid logon id and password. The system must have at least one level of security (firewall) protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet. A private FTP server used to exchange files with partners is an example of this type of system.

Internally accessible only. Users of the system must have a valid logon id and password. The system must have at least two levels of security (firewall) protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address, and it does not respond to a "ping" from the Internet. A private intranet Web Server is an example of this type of system.

Security Administrator. An IT student assistant shall be designated as the Security Administrator for the lab.

5 THREATS TO SECURITY

5.1 Lab members

One of the biggest security threats is system users. They may do damage to lab systems either through incompetence or on purpose. Through security-in-depth, security controls shall be implemented in layers to compensate for this threat. The mitigation shall entail:

- Giving out the minimum access an individual requires to do their job.
- Each user having their own individual account to access systems. Sharing login information with others is prohibited.
- Removing or limiting access to systems for lab members that have been fired, resigned, or undergoing a disciplinary proceeding.
- Maintaining detailed systems logs on to all computer activity.
- Physically securing computer assets, so that only individuals with appropriate authorization can access.

Awareness training for everyone associated with the lab, including visiting researchers who need access to lab equipment/network, shall be carried out at least once per semester. The training manual shall be updated before each training cycle to reflect the current threat landscape.

5.2 Amateur Hackers, Hacktivists, and Vandals.

These people are the most common types of attackers on the Internet. The probability of an attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been patched. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target.

5.3 Criminal Hackers, Saboteurs, and Nation-States.

The probability of this type of attack is low, but not entirely unlikely given the current trends where political conflicts are being settled in cyberspace. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

5.4 Vulnerable Systems/Applications

The IT team shall ensure all devices and software are patched to current versions in a timely manner. The comprehensive vulnerability management program shall include:

a) Ongoing network, host, and web applications vulnerability scanning and timely remediation
b) 3rd party penetration testing to validate network, host, and web application security
c) Proactive testing included in software development and vendor selection lifecycles

6 USER RESPONSIBILITIES

This section establishes usage policy for the computer systems, networks, and information resources of the office. It pertains to all users who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the lab.

6.1 Acceptable Use

User accounts on lab computer systems are to be used only for business in the lab and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, the university regulation, and can be punishable by law. Therefore, unauthorized use of the lab computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized people outside of the lab.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to lab systems for which they do not have authorization.

Users shall not attach unauthorized devices to their PCs or workstations, unless they have received specific authorization from the lab members' supervisor and/or the lab security administrator.
Users shall not download unauthorized software from the Internet onto their PCs or workstations.

On 12/7/2022, Texas Governor Greb Abbot ordered all Texas state agencies to ban the use of TikTok on any government-issued devices. TikTok usage is therefore prohibited on all devices belonging to the lab, including laptops, desktops, cell phones, tablets, and any other devices capable of Internet connectivity. In addition, TikTok is prohibited on any device that is connected to a UTD network.

Users are required to report any weaknesses in the lab computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

6.2 Use of the Internet

The lab shall provide Internet access to all lab members who are connected to the internal network ***and*** who have a business need for this access. Visiting researchers must obtain permission from the lab director and file a request with the Security Administrator.

The Internet is a research tool for the lab. It is to be used for research-related purposes such as: communicating via electronic mail with partners, obtaining useful research information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain.

6.3 User Classification

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. Furthermore, all users must conform to the Acceptable Use Policy (AUP) defined in this document. The lab has established the following user groups and defined the access privileges and responsibilities:

User Category	Privileges & Responsibilities
Department Users (Student Lab members)	Access to application and databases as required for job function. (RED and/or GREEN cleared)
System Administrators	Access to computer systems, servers, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.
Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, and network devices as required for job function.
Web Developers and Programmers	Access to applications and databases as required for specific job functions. Not authorized to access routers, firewalls, or other network devices.

Collaborators/Visiting Researchers	Access to applications and databases as required for specific job functions. Knowledge of security policies. Access to lab information and systems must be approved in writing by the lab director/manager.
Other Parties and Research Partners	Access is allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
General Public	Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.

6.4 Monitoring Use of Computer Systems

The lab has the right and capability to monitor electronic information created and/or communicated by persons using lab computer systems and networks, including e-mail messages and usage of the Internet. It is not the lab policy or intent to continuously monitor all computer usage by lab members or other users of the lab computer systems and network. However, users of the systems should be aware that the lab may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and lab member's electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with lab policy.

It is the policy of the state of Texas that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees in accordance with the Texas Public Information Act ("the Act"), *Government Code, Chapter 552*. This procedure shall be liberally construed in favor of granting a request for information. The lab complies with all state laws. For this reason, agreeing to use lab-owned information systems equipment, including the network, is defeating the expectation of privacy.

7 ACCESS CONTROL

A fundamental component of this Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

To control physical access, the lab shall grant individuals physical access to the lab through key card and "on a need" basis. Physical access shall be managed by removing or limiting access to the lab for individuals who have been fired, resigned, or no longer need access to the lab.

7.1 Hiring and Vetting

All lab members whose job roles require access to confidential/Personally Identifiable Information (PII) MUST complete and pass a criminal background check prior to being onboarded.

7.2 User System and Network Access – Normal User Identification

All users shall be required to have a unique logon ID and password for access to systems. The user's password shall be kept confidential and MUST NOT be shared with other lab members & supervisory personnel and/or any other persons whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must not be a word in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools."
- Passwords shall not be posted on or near computer terminals or otherwise be readily accessible around the terminal.
- Passwords must be changed every 365 days (1 year).
- Passwords MUST be used in conjunction with a second factor of authentication (2FA) e.g. Duo Authentication app.

Users are not allowed to access password files on any network infrastructure component. Password files on servers shall be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

Users shall not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Lab member Logon IDs and passwords shall be deactivated as soon as possible if the lab member is terminated, fired, suspended, placed on leave, or otherwise leaves the lab.

Supervisors / Managers shall immediately and directly contact the IT Manager to report changes in lab member status that require terminating or modifying lab member logon access privileges.

Lab members who forget their password must call the UTD IT Support Desk to get a new password assigned to their account. The lab member must identify himself/herself by UTD ID number to the IT department.

Lab members shall be responsible for all transactions occurring during Logon sessions initiated by use of the lab member's password and ID. Lab members shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

7.3 System Administrator Access

System Administrators and security administrators shall have root access to host systems as required to fulfill the duties of their job.

All system administrator access shall be revoked immediately after any individual who has such access is terminated, fired, or otherwise leaves their position in the lab.

7.4 Special Access

Special access accounts shall be provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts will be monitored by the lab and shall require the permission of the user’s lab IT Manager. Monitoring the special access accounts shall be done by entering the users into a specific area and periodically generating reports for management. The reports shall show who currently has a special access account, for what reason, and when it will expire.

7.5 Connecting Devices to the Network

Only authorized devices may be connected to the lab network(s). Authorized devices include PCs and workstations owned by individuals who comply with the configuration guidelines of the lab. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-lab computers that are not authorized, owned, and/or controlled by lab/lab member. Users are specifically prohibited from attaching key loggers, infected flash drives, and any external storage medium containing malicious code/penetration tool to the lab network.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g., thumb drives and writable CD’s.

7.6 Remote Access

Only authorized people may remotely access the lab network. Remote access is provided to those lab members who have a legitimate need to exchange information, copy files or programs, or access computer applications. Authorized connection can be a remote PC to the network or a remote network to lab network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID (VPN) or SSH.

7.7 Unauthorized Remote Access

Users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

8 PENALTY FOR SECURITY VIOLATION

The lab takes the issue of security seriously. Those people who use the technology and information resources of lab must be aware that they can be disciplined if they violate this policy. **Upon violation of this policy, a lab member may be subject to discipline up to and including discharge.** The specific discipline imposed will be determined on a case-by-case basis, taking into consideration the nature and severity of the violation of the Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against a lab member shall be administrated in accordance with any appropriate rules or policies and the lab Policy Manual.

A first-time minor innocent violation shall be a cause for the violator to revisit the Cybersecurity Awareness Training Manual and retaking the Cybersecurity Competence Test. Repeat offenders shall be subject to more scrutiny.

In a case where the violator is not a lab member, the matter shall be submitted to the lab director. The lab director may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

9 SECURITY INCIDENT HANDLING PROCEDURES

This section provides some policy guidelines and procedures for handling security incidents. The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the lab network. Some examples of security incidents are:

- Illegal access to a lab computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a lab computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a lab web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computers outside of the lab network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Lab members, who believe their terminal or computer systems have been subjected to a security incident, or have otherwise been improperly accessed or used, should report the situation to the lab’s security administrator immediately. The lab member shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.