The National Visualization Laboratory

Information Technology Security Policies and Standards Document

Islam Akef Ebeid

Executive Summary

The objective of this document is to define and describe the responsibilities and required practices for all members of the Laboratory with respect to information security and the protection of the Laboratory information assets.

This document applies to all individuals in the Laboratory and all forms of information resources. It describes the responsibilities of a member of the Laboratory based on roles to prevent unauthorized access to physical and electronic information, consistent with law, regulation and Laboratory policies. The policy outlines the responsibilities of the employees responsible for implementing, enforcing and abiding by this policy. The Procedures for the protection of the Laboratories' Information, incorporated by reference into the policy, describe the specific procedures required to comply with the policy.

Information security is a responsibility shared by employees of the Laboratory. All employees of the laboratory are considered data users. In addition to the responsibilities of data users, members of each role are required to fulfil specific responsibilities, including incident reporting and handling. Data stewards, managers and Information Service Providers are responsible for establishing security policies and procedures. Users are expected to be aware of and to comply with these policies.

Roles:

Data Users: Every employee and member of the Laboratory is a Data User and is responsible for appropriate protection of the Laboratory information. Data Users have the task of understating and complying with the lab policies and best practices in information security as established by the Laboratory Information Security Office.

Data Stewards: Are accountable for the data under their stewardship. Stewards classify data, authorize access, and promote information security within the relevant user community. Each employees are considered stewards of their own work.

Managers and Supervisors: Are responsible for assuring that all individuals who fall within the scope of their authority are appropriately educated in the information security requirements of their roles. They also encourage information security through user training and awareness.

Information Security Office: The ISO is responsible for overseeing the Laboratory network security, establishing required minimum security standards for handling the lab information assets, overseeing technology policy, managing an information security training and awareness program and finally handling information security incidents.

This document and set of policies will be periodically reviewed and updated as needed.

Applicable laws and frameworks:

FISMA:

The Federal Information Security Management Act recognizes the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the laboratory. FISMA focuses on cyber security through emphasizing “risk-based policy for cost effective security”, FISMA defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability.
Therefore the Laboratory will be compliant with the FISMA set of laws and regulations.

NIST Cybersecurity Framework:

FISMA also requires federal agencies to follow a common set of security standards, these standards are provided by NIST and are known as the Federal Information Processing Standards. Therefore the Lab will implement the policies based on the recommendations mentioned in NIST Framework.

The NIST Cybersecurity Framework consists of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks.

Assets:

- 12 Servers running Microsoft Windows Server 2012 R2
- Services provided by the Microsoft Windows Server:
  Active Directory, Domain Name Server, Dynamic Host Configuration Protocol, Enterprise Resource Planning, Oracle Database Server, R&D Server, Microsoft Exchange Server, Symantec E-Mail Filter, Websense for Internet Us,
- 2 Linux Servers running Apache Server with load balancing capabilities
- 490 PCs/Laptops running Microsoft Windows 10, Microsoft Office 2015, Microsoft Visio, Microsoft Project and Adobe Reader.

Policies:

- Information Security Policy for Research
- Acceptable Use Policy
- E-mail policy
- Privacy Policy
- System access policy

Procedures:

- Incident Reporting
- Data Backup
- User ID creation

Guidelines

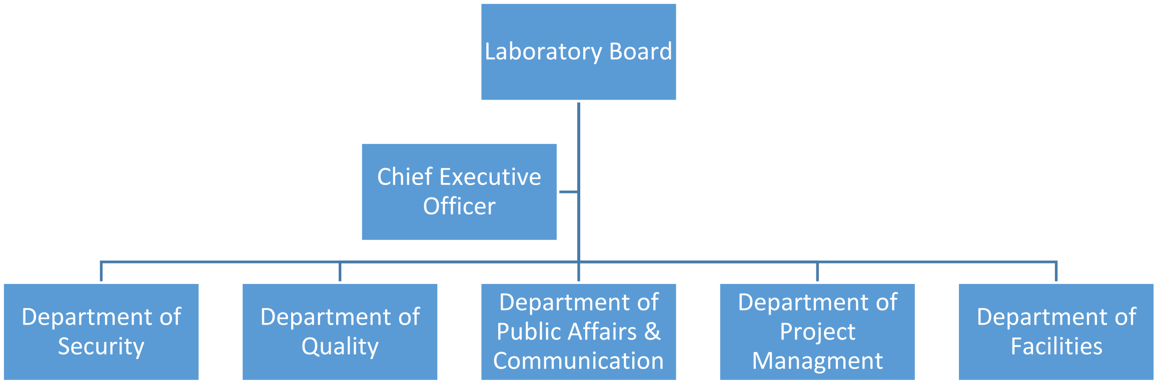
- Web Accessibility Guidelines

Domains

- User Domain
- Workstation Domain
- LAN Domain
- LAN-to-WAN Domain
- WAN Domain
- Remote Access Domain

- System/Application Domain

Plan of Action



Main Controls, Activities and Goals:

- Defining the System
- Identify and Classify critical cyber assets
- Provide active executive sponsorship
- Identify and analyze the electronic security perimeter
- Perform a vulnerability assessment
- Assess risks to system information and assets
- Select security controls
- Monitor and assess the effectiveness of the controls
- Assign responsibility for security risk management to a manager in the department of security

Implementation will include:

- Define roles and responsibilities
- Draft policies, procedures and guidelines
- Provide active executive sponsorship
- Assign implementation and enforcement to the head of the department of security
- Define a policy management plan

Training

- Establish a security awareness program with detailed objectives
- Train all employees in the level based on their responsibilities
- Establish an identity management framework and supporting systems to include physical access and electronic access to major systems
- Ensure that training and recruiting efforts are focused on cyber security

Example Policies, procedures and Guidelines

*Information security policy for research

Scope

Research data include information that is collected or generated by researchers, information that is obtained from third parties pursuant to Data Use Agreements (DUAs) and third party information that is not subject to DUAs. This Policy covers research data that are confidential, by reason of regulation, policy, law, or contractual obligation. The research data release will be investigated over seven domains implemented I the lab. All regulations are under FISMA.

The reasons behind this policy lies in the fact that this is the primary measure that must be taken to reduce the risk of unacceptable use of any of the lab's information resources.

Following the implementation of this policy across the lab is finding the correct controls to enforce the policy and informing staff on the various aspects of their acceptable use, as well as listing prohibited activities.

This will reduce the risk of potential security breaches on the lab's sensitive information due to human factor or other.

This policy will help well define the lab's information assets and protecting them.

Policy Statement

All legal orders involving electronic data shall be expeditiously sent to the Chief of Information Technology Officer. If the request has not been reviewed by the Lab legal department, the Information Security Officer may request a review or clarification of the order. Legal counsel may determine if there is a need for a Litigation Hold Notice, the scope of the Hold to be issued, and formally issue a Litigation Hold Notice.

In conjunction with the legal counsel, the Chief of Information Technology Officer shall

(1) identify the Information Technology Office and records management personnel who can assist in protecting and preserving electronically stored information and other relevant information;

(2) identify the specific individuals (end users) who may have responsive electronically stored information;

(3) identify the categories of information that are to be preserved or;

(4) utilize an electronically stored information questionnaire or discovery survey to facilitate the location of information. Additionally, the legal counsel and the Chief of Information Technology Officer shall review collected information to determine if it is responsive and/or subject to evidentiary privileges; identify and segregate confidential information and release the data as appropriate.

*Acceptable Use Policy

Purpose

The computing resources at the National Visualization Lab supports the research, and administrative activities of the Laboratory and the use of these resources is a privilege that is extended to members of the Laboratory. As a user of these services and facilities, you have access to valuable Laboratory resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the Laboratory will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the employment agreement. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

Scope

This policy applies to all users of computing resources owned or managed by the Laboratory. Individuals covered by the policy include (but are not limited to) employees, guests or agents of the administration and external individuals.

Computing resources include all Laboratory owned, licensed, or managed hardware and software, and use of the Laboratory network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments, personally owned computers and devices connected by wire or wireless to the Laboratory network, and to off-campus computers that connect remotely to the Laboratory's network services.

Policy Statement

- Acceptable Use

You may use only the computers, computer accounts, and computer files for which you have authorization.

You may not use another individual's account, or attempt to capture or guess other users' passwords.

You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the Laboratory for all use of such resources. As an authorized Laboratory Laboratory user of resources, you may not enable unauthorized users to access the network by using a Laboratory computer or a personal computer that is connected to the Laboratory network. [Network Connection Policy]

The university is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.

You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing Laboratory's network and computing resources.

You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

You must not use Laboratory computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

On Laboratory network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by the CIS Information Security Group.

See Acceptable Use Examples to clarify Laboratory's interpretation of acceptable use.

- Fair Share of Resources

Department of Facilities and other Laboratory departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The Laboratory network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the Laboratory community is explicitly forbidden.

The Laboratory may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them. Please review the Fair Share of Resources section of the "Acceptable Use Examples" for further clarification.

- Adherence with Federal, State, and Local Laws

As a member of the Laboratory Laboratory community, you are expected to uphold local ordinances and state and federal law. Some Laboratory guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of Laboratory's computing and network resources you must:

Abide by all federal, state, and local laws.

Abide by all applicable copyright laws and licenses. Laboratory Laboratory has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.

Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.

Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

Please visit Laboratory Laboratory's Copyright and Fair Use web pages for full discussion of your legal obligations. See also the Copyright Infringement Policy, which details the policies and procedures Laboratory Laboratory follows in responding to notifications of alleged copyright infringements on the Laboratory network.

- Other Inappropriate Activities

Use Laboratory's computing facilities and services for those activities that are consistent with the educational, research and public service mission of the Laboratory. Other prohibited activities include:

Activities that would jeopardize the Laboratory's tax-exempt status

Use of Laboratory's computing services and facilities for political purposes

Use of Laboratory's computing services and facilities for personal economic gain

- Privacy and Personal Rights

All users of the university's network and computing resources are expected to respect the privacy and personal rights of others.

Do not access or copy another user's email, data, programs, or other files without the written permission of Laboratory's Chief Information Security Officer, who is bound to the procedures outlined at Emergency Access to Accounts and Information.

Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to university discipline as well as legal action by those who are the recipient of these actions.

While the Laboratory does not generally monitor or limit content of information transmitted on the Laboratory network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that Laboratory is not subject to claims of institutional misconduct.

Access to files on Laboratory-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Chief Information Security Officer in conjunction with requests and/or approvals from senior members of the Laboratory, as found in the document Emergency Access to Accounts and Information. External law enforcement agencies and Laboratory Public Safety may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the General Counsel. Information obtained in this manner can be admissible in legal proceedings or in a Laboratory hearing.

- Privacy in Email

While every effort is made to insure the privacy of Laboratory Laboratory email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct Laboratory business, there may be instances when the Laboratory, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user. Please see Laboratory's Electronic Mail Policy for further details.

- User Compliance

When you use Laboratory computing services, and accept any Laboratory issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using Laboratory electronic and print publication mechanisms, and to adapt to those changes as necessary.

References

http://csrc.nist.gov/groups/SMA/fisma/overview.html

https://security.georgetown.edu/technology-policies/executive-summary

http://www.csoonline.com/article/2126072/compliance/the-security-laws--regulations-and-guidelines-directory.html

https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

http://policy.illinoisstate.edu/technology/9-6.shtml

http://www.educause.edu/wiki/e-discovery-guideline-and-toolkit

http://vpr.harvard.edu/pages/harvard-research-data-security-policy

http://policies.iu.edu/policies/categories/information-it/it/IT-12.shtml

http://www.sans.org/security-resources/policies