Information Security on NECTEC Management Information System

Banchong Harangsri, Kwanchai Lumubol, Teera Phatrapornnant, Pairat Chaichanadee, Rachanee Komthip, Yarnawan Nitayajarn,, Chalee Vorakulpipat, Nopporn Suwannuraks, Wisut Kaewthong, Santipong Karukanan
NectecNet : National Electronics and Computer Technology Center (NECTEC)
73/1 Floor 7, Room 714, NSTDA Bldg.,Rama VI Rd., Rajdhevee,
Bangkok 10400, THAILAND
Tel. (662) 644-8155-90, ext 724, Fax: (+662) 644-8027-9
Email : nnetstaff@notes.nectec.or.th

Sunee Pongpinigpinyo
Computer Centre, Silpakorn University, Sanamchan Palace Campus
A.Muang, Nakorn Pathom 73000, THAILAND
Email : sunee@su.ac.th

ABSTRACT
This paper is aimed at increasing the level of security of information stored on NECTEC's management information system. A main mechanism in driving this to occur is a user policy. All NECTEC users who interact with or use this information system are expected to strictly abide by this user policy. It is highly hoped that with this policy in hand, we can in part improve the security over NECTEC's management and administration information, especially sensitive information, stored on a large number of databases.

KEY WORDS **Information Security, Security Policy, MIS, IT Policy and Management.**

บทคัดย่อ
บทความฉบับนี้มีจุดมุ่งหมายที่จะเพิ่มระดับความมั่นคงปลอดภัยของข้อมูลที่อยู่ในระบบสารสนเทศของ NECTEC กลไกอันหนึ่งที่สำคัญซึ่งจะเป็นตัวจักรในการทำให้สิ่งนี้เกิดขึ้นได้ก็คือนโยบายเพื่อให้ผู้ใช้ระบบคอมพิวเตอร์ปฏิบัติตาม เป็นที่คาดหวังว่าผู้ใช้จะปฏิบัติตามข้อกำหนดต่าง ๆที่ตั้งขึ้นมาอย่างเข้มงวด เพื่อจะนำไปสู่การเพิ่มระดับความมั่นคงปลอดภัยของข้อมูลอย่างแท้จริง โดยเฉพาะอย่างยิ่งข้อมูลที่มีความสำคัญมาก ๆต่าง ๆซึ่งถูกจัดเก็บอยู่บนฐานข้อมูลประเภทต่าง ๆซึ่งมีอยู่เป็นจำนวนมากในระบบสารสนเทศของ NECTEC

คำสำคัญ ความมั่นคงปลอดภัยของข้อมูล, นโยบายเพื่อความมั่นคงปลอดภัย, ระบบสารสนเทศเพื่อการจัดการและการบริหาร, นโยบายและการจัดการทางด้านเทคโนโลยีสารสนเทศ

1. Introduction
With the advent of Information Age, IT policy and management plays a critical role to businesses, firms, companies, organisations, institutions, and academia partly in directing how employees work and cooperate so as to increase the operational productivity, efficiency, speed, and flexibility as well as the security of the working environment. Well-planned and well-thought-out IT policy and management will potentially lead the business to the high performance and capacity for the working environment.

This paper is aimed at boosting the level of *security of information* stored on NECTEC's management information system (MIS) [15], as a result safegaurding the invaluable resource, namely large volumes of NECTEC's information against potential threats that can be detrimental to the integrity of the MIS. A main mechanism in driving this to happen is a user policy which we call NectecNet Usage Policy. All NECTEC users are expected to strictly abide by this user policy.

Over recent years information security has gained more and more attention. This is chiefly because electronically accessible information has been stored more and more into computing systems. In computing systems, personal computers, workstations, networks, and any other communication media are used to disseminate,

access, and manipulate information so widely that threats in various forms over information stored can take place if insufficient care is taken. Threats can be non-trivial, especially leading to financial, legal and reputation matters and hence managers should pay great attention on the security over information they maintain.

As an information system, our NectecNet (NECTEC's Intranet) system is one that serves to disseminate and manipulate information mainly for management and administration of NECTEC. The system is thus exposed to information threats. (Readers interested in the foundation, objectives, implementation, progress, and milestones (our achievements) of NectecNet can be found in the lab profile [12].)

In addition, we have adopted the information infrastructure in [6] developed and used by the U.S. National Information Infrastructure, to use with our information system. (Simply speaking, an information infrastructure means both all hardware and software that supports using information under NectecNet's responsibility.) The adopted information infrastructure has to address the security concerns [7] over the infrastructure. Our information system therefore has also to take account of the security of information maintained in it.

Before we proceed, let us introduce necessary terms that we will frequently refer to in this paper.

Terms

- *The NectecNet system* incorporates the network, all hardware, software, information, data, databases, computing facilities under NectecNet's responsibility.
- *Lotus Notes* [14] Operating as the backbone for NectecNet to provide the Intranet technology, Lotus Notes is software for which the NectecNet staff takes full responsibility.

  Three main tasks performed by this software are document database management, workflow, and messaging among five office locations (see Figure 1 also) belonging to NECTEC.
- *Databases* Otherwise mentioned, referring to this term, we mean document databases created by users via Lotus Notes.
- *A user* means not only a NECTEC's employee who accesses or uses the NectecNet system but also a user who has some cooperation, coordination or collaboration in some way with NECTEC.

Below we discuss about security risks posed over information and point to how to obtain security over it.

1.1 Information Security Risks are Real

A number of security risks posed over the business (NECTEC's) information include:

- *Human errors and omissions* People constitute the greatest threat to their information system [5]. From a source in [13], human errors and omissions take account of 65% which is very high. Potential losses include accidentally deleting files, incorrectly updating files/databases, equipment failures which could also destroy information, and the door of a server room left unlocked.
- *Computer crime* entails unlawful access to information, manipulation of information in a manner that illegally benefits the perpetrator, vandalism of hardware and software, and even deliberate sabotage.

  Below we list a number of security incidents that took place with NECTEC in the past decade.

  One case that occurred to NETCEC about one and a half year ago is that a hacker was able to break into NECTEC's internal network and a major UNIX host and removed all files of the UNIX host from the root directory. This is a very disastrous and devastating security incident and caused a major loss of information to all users at that time.

  Being a lab in NECTEC, High Performance Computing Center (HPCC) got hacked a number of times into its computer system running Linux as its operating system. Luckily little or no information loss occurred.

  Running SunOS 4.1.3, a UNIX SunSparc host of Computer Technology and Automation (CTL) lab's was hacked in 1998. The machine was unable to boot and had to be re-installed from scratch. Fortunately no information loss occurred.

  There was one time that the hacker broke into a NECTEC's UNIX host and left a Trojan horse version of the login program on it. This login version then created the trap door to the hacker to log in to the host at any time.
- *Criminal Mischief* encompasses information pilferage perhaps committed by employees and thus possibly our users in the organisation and thus NECTEC to sell to anyone else outside.
- *Computer Viruses* Software import, e.g., via FTP, downloading attached files from e-mail, downloading Java/ActiveX applets, may introduce viruses, Trojan horses and other related threats to our information system.
- *Policy Weaknesses* [9] incorporates weaknesses or vulnerabilities in the policies used in the organisation, such as about

physical access controls, security administration, disaster recovery and backup.

A security incident about disaster recovery and backup took place with NECTEC in 1997. Lotus Notes, which operates as the backbone for NECTEC's Intranet, crashed in that year which caused a major loss of information to all users.

This catastrophic incident is a nightmare experience to all of us and to remind that a "good" contingency plan, regarding system backup is essential to any computerised MIS.

- *Disasters* such as floods, lightening, fire, power failures, temperature (too high, for example), humidity, sudden surges in electrical power can pose a huge damaging potential for loss of information.

1.2 How to Obtain Information Security

To reduce information security risks to an acceptable level, an information security plan (program) should be developed and address the aforementioned information security risks as a minimum. Such a security plan we have in hand thus far consists of:

- A user policy or NectecNet Usage Policy that codifies how NectecNet's information infrastructure would be used by all users appropriately and securely. This policy is now being considered by the NECTEC Board of Executives to be approved into actual practice after passing through the process of modification, addition and/or adjustment by the board.
- A training course for information security. This course is aimed at educating all users to be aware of and understand about threats to information as well as networks and computers. Users will also learn how to interact with or make use of information, networks, and computers in a secure and efficient manner.

This paper is aimed at creating the user policy mentioned above so that all users will comply. It is highly hoped that by following this policy, information security risks will be reduced to a certain level. (This security means when combined with other means, such as the training above, will potentially reduce the risks to an acceptable level.)

The following is the structure of presentation in order in this paper:

- *Previous related work (section 2):* We mention about the previous related work influencing the development of the user policy in this paper.
- *Policy scope and applicability (section 3)*: Define a policy scope and what the user policy applies to.
- *Security policies (section 4)*: Briefly describe security policies that all users should strictly abide by. For the complete version of these policies, we refer the reader to [10,11].
- *Policy agreement (section 5)*: To enforce the security policies, we need to get any user who wishes to use the NectecNet system to sign agreement with the conditions defined in this section prior to beginning to use the NectecNet system.
- *Conclusion (section 6):* What do we achieve in this paper?, and what next do we plan to do?

2. Previous Related Work

The ideas in this paper of security policy have principally been developed from a number of security policy sources in [1,2,3,4]. The security policies from those sources have been created and used individually in a certain computing environment. That is, security policy will vary from a computing environment to environment and therefore, each computing environment will have its own *unique* security policy.

To our belief, the proposed security policy in this paper is the first and foremost attempt that has ever been created to protect NECTEC's information resources.

3. Policy Scope and Applicability

Scope and Applicability

This policy is applicable to all users who employ the NectecNet system and to others granted the use of this system. This policy refers to or covers all NectecNet information resources, e.g., data, information, news, databases whether such resources are:

- controlled by individual users or shared with other users and
- stand-alone or networked.

The policy applies to all computing and communication facilities under NectecNet's responsibility, such as personal computers, workstations, and peripherals, e.g., tapes, external drives, and printers.

Because of the fact that apprroximately all 400 NECTEC users now have accounts with the NectecNet system, this implies that the scope of applicability of the security policy created here is organisation-wide to be abided by all NECTEC users.

Showing the scope of the network under our responsibility, Figure 1 also shows the connectivity among NECTEC's five office

locations: namely, CNC Building, Gypsum Building, NSTDA Building, Bangkok Thai Tower Building, and TMEC lab. Lotus Notes operates over this network chiefly to perform messaging over it. These office locations contain a large number of document databases created by Lotus Notes. These databases are under our responsibility. The 400 NECTEC users accessing these databases are distributed to work among the five locations.

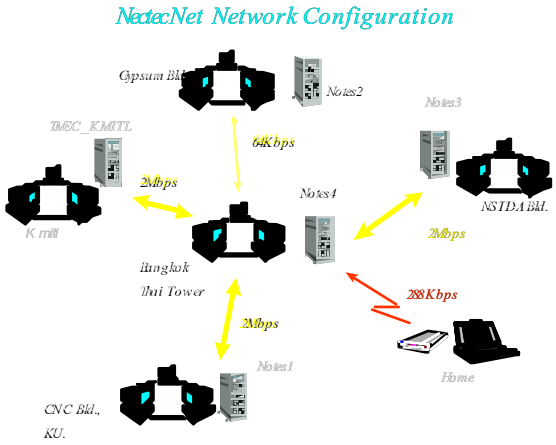

Figure 1. NectecNet's Network Connectivity.

The 400 users can be categorised into two classes. The first is the *general user* class. Users in this class can do whatever they want with their own databases but usually won't be able to do so with the databases of others.

The second is the *administrator* class. Users in this class have the highest access privilege to do whatever they want as appropriate with all databases. Some of the users in the NectecNet staff are in this second class.

Legal Issues

NectecNet conducts all its businesses in cooperation with Thai and other foreign communities, jurisdictions, and laws. Under some circumstances, as a result of investigations, subpoena, or lawsuits related to some misconduct, NectecNet may be required by law to provide electronic or other records or other information related to those records or related to the use of information resources.

4. Security Policies

The following policy issues are addressed in the current NectecNet Usage Policy [10,11] but more policy issues can be added as appropriate in the future.

- Integrity of information resources
- Unauthorised access
- Physical security
- User privacy
- NectecNet system usage
- Personal and commercial use of information infrastructure
- Software import control
- Termination of access and accounts

By nature, security policies are exposed to change, addition, modification, and review after a certain period of time, such as one year. This is partly because of the technological, organisational and perhaps also economic and political changes.

Below we provide and describe a tentative policy in each category above in order. Note that in each category, there may be a number of related policies inside the category. We refer the reader to the complete version of NectecNet Usage Policy in [10,11] for all its details. The term "tentative" above is used simply because all these policies as of this writing have not yet been approved by the NECTEC Board.

4.1 Integrity of Information Resources

Users must respect the integrity of computer-based information resources.

A Tentative Policy for Modification or removal of Lotus Notes software

Users must not attempt to modify or remove without proper authorisation the Lotus Notes software either installed as a client or server of Lotus Notes.

4.2 Unauthorised Access

Users must refrain in any way from:

- seeking to gain unauthorised access to information resources or
- enabling unauthorised access – any attempt to make unauthorised access available.

A Tentative Policy

Users are not to deliberately enable other unauthorised people to access the NectecNet system.

4.3 Physical Security

Users should strictly comply with deeds, such as in the tentative policy below. This is in order to physically secure the NectecNet system.

A Tentative Policy

Normal users (who are not the NectecNet staff) are responsible for refraining from entering the Lotus Notes servers' areas, especially without the existence, accompaniment, or supervision of any of the NectecNet staff unless they are authorised to do so.

4.4 User Privacy

The NectecNet staff will attempt with its best effort to do anything to ensure any user's privacy.

A Tentative Policy

The content of any email message of a user will not be accessed or disclosed to others, except:

- due to any serious addressing errors,
- as a result of maintaining the email system, or
- as required by law.

4.5 User Behavior to the NectecNet system

Users must behave appropriately to interact with or use the NectecNet system.

A Tentative Policy for Password Use

- Users are to use passwords of a length specified by the system administrator – a mix of six (8) alpha and numeric characters.
- Users must keep passwords confidential and must not share passwords with anyone.
- Users never tape passwords to a wall, never keep them under a keyboard, or in other easily discoverable areas.
- Users avoid storing passwords in their computers, e.g., PCs, MacIntosch, etc.

4.6 Personal and Commercial Use of Information Infrastructure

Users must assure the proper use - *personal and commercial* - of NectecNet's information infrastructure.

A Tentative Policy for Commercial Use

NectecNet's information infrastructure should not be used for any commercial purposes except as permitted under NECTEC's written policies, e.g., the training activity provided by Information Technology Education Division. This commercial use is normally related to NECTEC's activities, functions, or businesses.

4.7 Software Import Control

Software import, e.g., via FTP, downloading Java/ActiveX applets, may introduce viruses, Trojan horses and other related threats to the NectecNet system. We need to protect our information system.

A Tentative Policy for Virus Prevention

Users will be trained by the NectecNet staff about the possibility of receiving viruses and other virus-related threats from the Internet and on the use of virus-scanning tools.

As a user's role, all users are expected to attend the training provided by the staff.

4.8 Termination of Access and Accounts

When a user resigns from working with NECTEC by any reason (good or bad), the tentative policy below will be applied.

A Tentative Policy

For any user, access to the NectecNet system will be disabled immediately when the system administrator has been informed from the user's superior(s), e.g., by the user's supervisor. The following applies to the user:

- There is *no grace period* for this disability.
- The user's databases, files, and any other computer-accessible materials stored on the server (where those reside) at the time of disability will be backed up and retained on backup media for a *maximum of 2 years*.

5. Policy Agreement

To enforce all policies codified above, any user who wishes to use the NectecNet system must accept the statements below and sign his/her name for nonrepudiation purpose.

Statements for User Acceptance

A user who wishes to use the NectecNet system must assume responsibility for his or her personal actions. The user must consent to the following:

- I have been given the opportunity to read the NectecNet Usage Policy in [10,11]. I promise that my use of the NectecNet system will conform to behavioral guidelines in this policy.
- The account or access privileges I have requested are solely for my individual use. I will not grant permission to anyone else to use my computer account or access privileges.
- I am personally responsible for all use of the computing facilities on which I have an account or access privileges.

I acknowledge receipt of, understand my responsibilities to, and will strictly comply with all the policies defined in the NectecNet Usage Policy. The result of my infringement will be taken in legal and/or disciplinary action for damages or other punitive action by any injured party, including all NECTEC's users.

_____ _____

User Signature Date

6. Conclusion

In this paper, we've proposed a user policy to secure the use of the NectecNet system. Our future work to enhance the information security over the system includes:

- Develop a security course like in [8] to train or educate all our users to be aware of and understand the secure, effective, and efficient use of the NectecNet system.

- Develop an administrative security guide to be made use of by our system administrators in managing and administering the NectecNet system.
- Perform risk analysis over a large amount of information stored on Lotus Notes in order to classify it based on its sensitivity. From the resulting classes of information, we can then apply appropriate safegaurds to cost-effectively protect those classes from potential information threats that can occur.

Acknowledgements

This user policy has basically been developed using the main sources of information in [1,2,3,4]. Most of the policy issues appearing in this paper (see also Section 4) have been taken from them with major modification to suit our own information system.

References

[1] *A Survey of Selected Computer Policies from Institutions of Higher Education* http://www.brown.edu/Research/Unix_Admin/cuisp/, 1996, Brown University. This document summarises statements from a number of policies from leading institutions of higher education in the United States and Canada.

[2] *Stanford Computer and Network Usage Policy*, Stanford University, http://www.stanford.edu/group/itss-ccs/security/policies/compolicy.html, June 11, 1997. This is a computer and network usage policy used at Stanford University and developed by its Network Security Team.

[3] *Leland Systems Usage Policy*, http://www.stanford.edu/group/itss-ccs/security/policies/leland.usage.html. As part of Stanford Univerity, the Leland Systems support research and degree-granting instructional programs at Stanford University.

[4] *Internet Security Policy,* B. Guttman and R. Bagwill, NIST Special Publication 800-XX, National Institute of Standards and Technology, Sept 27, 1998. This is a draft version whose URL is at: http://csrc.nist.gov/ isptg

[5] *Office Automation: A System Approach,* C. Ray, J. Palmer, and A. Wohl, South Western Educational Publishing, International Thomson Publishing, 1995, third edition.

[6] *An Architectural Framework for the National Information Infrastructure*, Cross-Industry Working Team (XIWT), http://www.xiwt.org/documents/documents.html, September, 1994. This is a white paper for the American Information Infrastructure.

[7] *A Process for Information Technology Security Policy,* Cross-Industry Working Team (XIWT), http://www.xiwt.org/documents/documents.html, March, 1996.

[8] *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, John B. Ippolito, National Institute of Standards and Technology, April 1998, NIST Special Publication 800-16, Mark Wilson – Editor.

[9] *Internet Security for Business,* Terry Bernstein, Anish B. Bhimani, Eugene Schultz, Carol A. Siegel, John Wiley & Sons, Inc, 1996.

[10] *NectecNet Usage Policy*, NectecNet, Technical Report, Feb, 1999, NECTEC, 73/1 Floor 7, Room 714, NSTDA Bldg.,Rama VI Rd., Rajdhevee, Bangkok 10400, THAILAND.

[11] ระเบียบปฏิบัติการใช้งานคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ภายในองค์กร NECTEC, NectecNet, Technical Report, ก.พ. 2542, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC), สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, อาคาร สวทช. ชั้น 7 เลขที่ 73/1 ถนน พระรามที่ 6 เขตราชเทวี กรุงเทพฯ 10400, The Thai version of the NectecNet Usage Policy.

[12] *NECTEC Information Service Center (NectecNet): NectecNet's* Lab Profile, , NectecNet, Jan, 1999, ISBN 974-7578-26-3, NECTEC, 73/1 Floor 7, Room 714, NSTDA Bldg.,Rama VI Rd., Rajdhevee, Bangkok 10400, THAILAND.

[13] *Information Security Management,* Eyal Santo, Director of Sales/Asia Pacific of Voltaire Advanced Data Security. The seminar was held on July 19, 1999 at NSTDA Bldg., 73/1 Rama 6 Rd., Rachathewi, Bangkok, Thailand 10400. Hardcopy in power point format was available. Mr Santo is an expert on IT security both hardware and software from Israel.

[14] *Application Deveoper's Guide for Lotus Notes,* Release 4.5, Lotus Development Corporation, 1996, 55 Cambridge Parkway, Cambridge, MA 02142. Printed in Singapore.

[15] *NNET MIS Model,* NectecNet, Feb, 1999, NECTEC, 73/1 Floor 7, Room 714, NSTDA Bldg.,Rama VI Rd., Rajdhevee, Bangkok 10400, THAILAND. Slides in power point format for NNET's MIS Model presented on Feb 15th 1999 in NectecNet version 2.0's opening.