

# E-Learning Security for Collaborative Academy in Area of ASEAN Community

**Sarawut Ramjan**

Management of Information and Communication Technology,  
School of Science and Technology,  
North-Chiang Mai University, Thailand  
ramjan77@gmail.com

**Abstract** - ASEAN economic community gives a change for academy in the cross-country cooperation. eLearning infrastructure is implemented for educational management in order to overcome an educational and digital divide problems which difference in each country. According to other digital system, there is a cyber threat which attack to eLearning system. Moreover, there is cooperation between academies which have a differential level including higher vocational degree with under-graduate. Certain, there is a difference an eLearning infrastructure that could not be implemented same security system. Thus, this article suggests a security plan that suitable and flexible with differential characteristic of each collaborative academy. This plan could be operated for academy which arrange with other academy in ASEAN economic community in order to protect a system from cyber threat and problem. Furthermore, this article could be used to decency for other analysis design later.

**Keywords** - E-Learning System, Security Plan, ASEAN Economic Community, Academy

## I. INTRODUCTION

Nowadays, there is a collaborative between many academies in 10 countries including Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Vietnam, and Thailand under policy of Asean economic community: AEC which was established for integrated a ability

of each country in order to be high performance region [1]. Thailand improve a telecommunication efficiency by reduce a limit for telecommunication service over AEC countries [4].

It is an opportunity for academy for collaborative together for reducing a digital and educational divides [6]. Besides, there is an across education management between university and high school where are difference area. Therefore, eLearning system is implemented in order to connect resources including course content, presentation, material and digital library [7]. System is established on IT infrastructure such as database, network technology and web application. Higher vocational degree drafts a curriculum with under-graduate over many countries. They reduce a gap between educational level, and digital divide via memorandum of understanding in dimension of eLearning implementation. Unfortunately, there is a cyber threat which attacks to eLearning system such as insider job attack that authority accesses to grad system for change a grad for student who is employer.

This paper picks up a case study from North-Chiang Mai University: NCU which signs a memorandum of understanding with college in Lao that manages an education in higher vocational degree. eLearning system connects between NCU with colleges in Lao. They provide course content in format of multimedia, text and digital library on database which could be accessed via internet channel. Student accesses into eLearning system from Lao in order to take class which

lecture from NCU lecturer. However, there is a cyber threat that blindsides an eLearning system [2]. Security system becomes to issue that chief executive officer emphasizes a security plan [8]. This paper bring a case study from NCU in order to recommend a security plan which suitable with characteristic of eLearning security system that is collaborated from many higher vocational degree college in AEC with university.

## II. INFRASTRUCTURE BACKGROUND

From case study, this section narrates regarding to IT infrastructure of NCU and connection with Lao's colleges as follows:

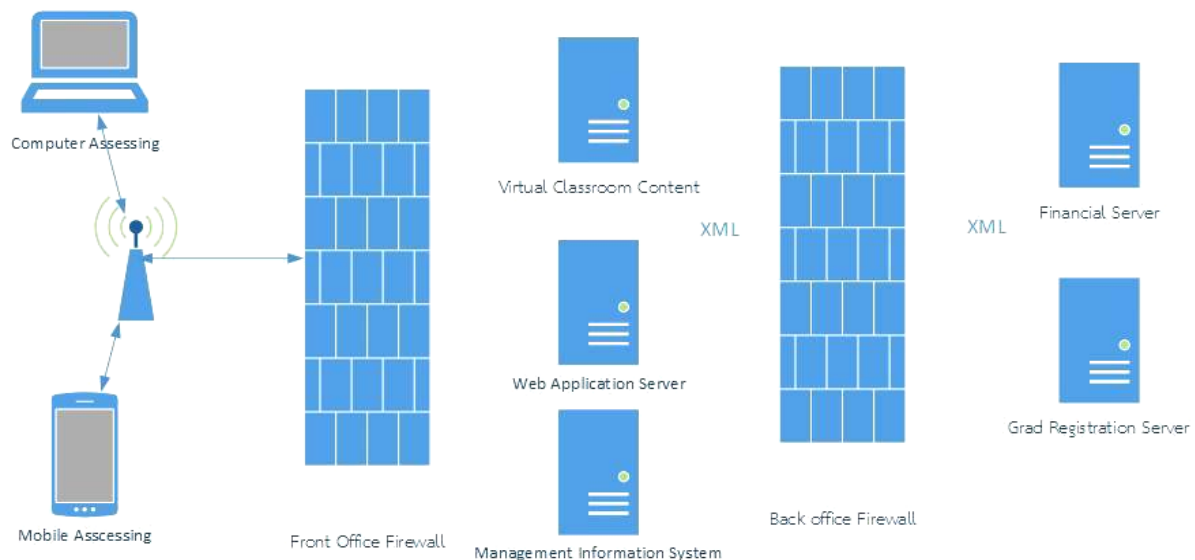


Fig 1. NCU Security Infrastructure

From fig. 1, NCU designs a security system by client assessing via wireless access point which connect to front office firewall that authenticate a user who have an authority for access to provide virtual class content on database server. This database operated with web application server. On the other hand, back office firewall authenticates users who have an authority for access to financial server and grad registration server. They employ an XML technology for exchange a data which difference a format [10].

Student and lecturer rely on a virtual classroom content for provide a subject content. They discuss and fulfill a knowledge

### A. NCU IT Infrastructure

NCU provides an information system in order to manage a virtual classroom including eLearning system, grad registration system, eDocument system and financial management system. All systems are integrated under concept of enterprise resource planning [9] for reduce an educational cost and education divide problem. Those systems are constructed under web applications which operate on network technology. For protect an information system, NCU manages a risk level by firewall double layers architecture as fig. 1 [3].

via eLearning feature including web board and social network. Employee and student access to financial system in order to make a transaction including registration fee, salary and cash management. Executive officers rely on decision report from management information system which brings information from many systems for process to new information. Surely, front and back office firewall are different architecture for stall an attacker who threads a front office firewall until a network technician found them before they thread a back office firewall. Not only main study which use an IT infrastructure but also overtime study including Ph.D. Dissertation, thesis, independent study, senior

project and academic services, eLearning system is accessed 24 hours 7 days as same as there is a possibility that it is bombard every time.

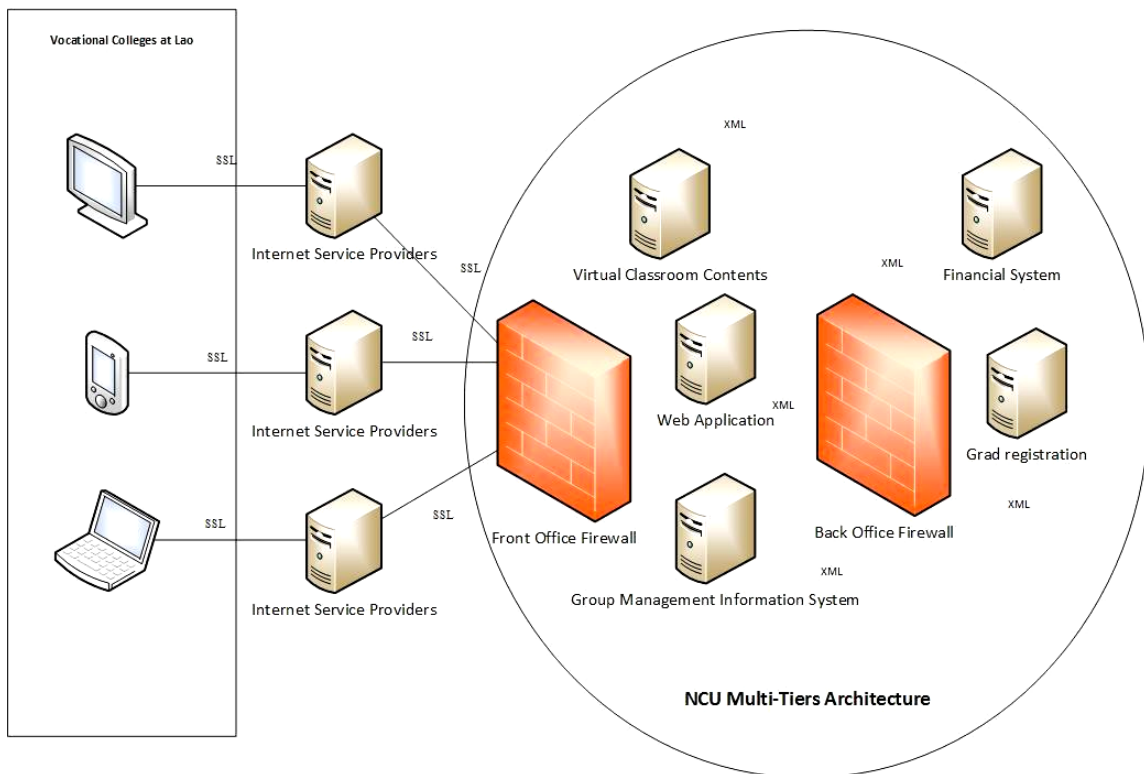
NCU reduced a digital divide problem and, expand an education opportunity for other country in AEC such as vocational college in Lao. So, this paper narrates a collaborative background between NCU with colleges in Lao in section B.

**B. Lao’s Colleges Connection**

By the reason that Lao government allows just public university for set up an under-graduate, there are some students who lack an opportunity for study on under-graduate level. NCU connects with many private vocational colleges in Lao in order to overcome an education divide problem. Not only collaborative about continuing education but

also content integration, they combine a content between higher vocational degree with under-graduate degree by amend curriculum at NCU and Lao’s colleges. Moreover, there is a possibility for set up a graduate study at Lao. Once they had signed a memorandum of understanding, they implemented an eLearning system in order to share a resource including internet system, grad registration system, financial system and management information system and virtual class room content.

They concern about security system which should be designed for protect an information asset such as grad or financial transaction. Therefore, they provide a security infrastructure cover on information system as fig 2.



**Fig 2.** E-Learning Security for Collaborative Academy

From fig. 2, NCU provide an IT connection with many vocational colleges in Lao. Lao student access to NCU resource via many devices such as smart phone, laptop and work station on internet service providers. They through 1<sup>st</sup> firewall for take class on

virtual classroom server which serves content with web application server. Moreover, executive chief officer interact between Lao with NCU in order to discus on education management under concept of group management information system.

Once they register a subject, they through 2<sup>nd</sup> firewall [11] in order to complete subject registration that connects with financial system. However, lecturer needs to submit grad in internal side by the reason that NCU protect a person who not has an authority to submit grad from external side. There are many XML which is used for support an exchange between many clients and servers that are different platform.

From background of NCU and connection between NCU with many Lao colleges, they need to plan about security solution and policy which suitable with international connection as next section.

### III. SECURITY PLAN FOR COLLABORATIVE ACADEMY

They are realized concerning to cyber threat and problem which bombard on internet system. Even thought there is firewall security, it not enough for protect under new environment from academic collaboration. Especially, there is a difference infrastructure from 2 countries in dimensions of technology and government policy [12]. Therefore, NCU and Lao colleges connecting brainstorm about security plan as follows:

#### A. Strategy Plan

They buckle to define a strategy of IT security which ease up from main strategy. Best management organization becomes to be one of strategy for NCU and Lao colleges connection. Therefore, they created an aim which is a university and technology development for support an AEC e-Learning in order to respond with strategy.

This section will be evaluated by indicator which is a number of AEC e-Learning curriculums. They define a number in 2016 at 1 curriculum per faculty, and then grow up to all curriculums in 2020.

#### B. Faculty Plan

There is a consideration about AEC e-Learning curriculum in many faculties. However, there is some major which is not suitable with AEC e-Learning. Especially,

curriculum is controlled by federation of profession such as accounting, law and engineering. Therefore, faculty of science and technology navigate by department of business computer which reach to Lao vocational college. NCU manage class content for support a Lao student by ease up from traditional operation which served for Thai student. However, they realize that there is a necessity for meet Lao student by face to face. In begin, NCU went to Lao for create a class room which is facilitated by NCU e-Learning infrastructure.

Thus, faculty plan is drafted by faculty administrated committee including dean, associated dean and head of department. Faculty plan is written that faculty should start up a project in order to respond with strategies as follows:

TABLE I  
FACULTY PLAN FOR 2015

| No. | Strategies                          | Indicators                           | Aims |
|-----|-------------------------------------|--------------------------------------|------|
| 1   | e-Learning Curriculum               | Amount of curriculum                 | 1    |
| 2   | Security System                     | Level of Satisfaction of stakeholder | 3.5  |
| 3   | Online content evaluation mechanism | Mechanism                            | 1    |

Table I said that there are 3 strategies which respond with an academy cooperation. e-Learning curriculum is evaluated by amount of curriculum which is driven for support a cooperation between NCU with Lao colleges. Security system is evaluated by feature which is provided for e-Learning and IT infrastructure protection, and level of satisfaction of stakeholder in order to show about acceptance level that meet with security requirement of CEO. Online content evaluation mechanism is interested from lecturers who need to evaluated an online content which is produced for overcome a cross culture.

**C. Action Plan**

Faculty of science and technology drafted an action plan which obtains a project as follows:

**TABLE II  
ACTION PLAN 2015**

| No. | Project  | Objectives   | Indicators                                 |
|-----|--|--|--|
| 1   | e-Learning curriculum development for business computer department | 1. to created a curriculum that support with academy cooperation between NCU with Lao colleges   | 1. amount of curriculum (1 curriculum)     |
| 2   | Security system development for academy cooperation                | 1. to evaluate a risk level for e-Learning system<br>2. to provide a security solution and policy for e-Learning system<br>3. to evaluate a risk level for IT infrastructure<br>4. to provide a security solution and policy for IT infrastructure | 1. satisfaction level of Stakeholder (3.5) |
| 3   | Online content evaluation mechanism development                    | 1. to develop online content Evaluation mechanism  | 1. mechanism (1 mechanism)                 |

From action plan, there are 3 projects that are constructed for respond to faculty strategy. e-Learning curriculum development for business computer department project was initiated for pilot a cooperation between NCU with Lao colleges. Business computer lectures went to Lao in order to set up a bachelor degree curriculum which according with higher vocational degree in computer. Moreover, there is a possibility for Lao lecturer development by serve graduate-study level. This project reduces an education divide problem over AEC country. Security system development for academy cooperation project evaluates a risk level on eLearning system as follows:

**TABLE III  
RISK MATRIX FOR ELEARNING SYSTEM**

| Impact | Likelihood     |                  |                |
|--------|----------------|------------------|----------------|
|        | High           | Medium           | Low            |
| High   | H,H<br>1 x 1   | H,M<br>1 x 0.5   | H,L<br>1 x 0   |
| Medium | M,H<br>0.5 x 1 | M,M<br>0.5 x 0.5 | M,L<br>0.5 x 0 |
| Low    | L,H<br>0 x 1   | L,M<br>0 x 0.5   | L,L<br>0 x 0   |

From table III, this project relies on risk matrix under NIST standard 800-30 in order to evaluate a risk level [5]. This article define a degree of likelihood and impact level by

divide to 3 scales including high at 1, medium at 0.5 and low at 0. Evaluation founds that there is a low motivation to attack eLearning system. There is a vulnerability point that current control could be used for protection. So, there is a likelihood level at low that degree of likelihood is 0. On the other hand, when system is attacked, they concern about content integrity which served to student. So, there is an impact level at medium that impact level is 0.5. Risk level of eLearning system is low level which is 0.

From risk level, this project brainstorm many IT lecturers and IT technician in order to recommend a security solution and policy which according to risk level and characteristic of academy cooperation as follows:

- Authentication system [13] is provided for Lao student and lecturer who access to eLearning system thought 1<sup>st</sup> firewall.
- Lao college side should be take care by IT technician who service about system availability, and connect about content integrity problem with NCU.

Not only eLearning system but also IT infrastructure which should be evaluated a risk level as table IV.

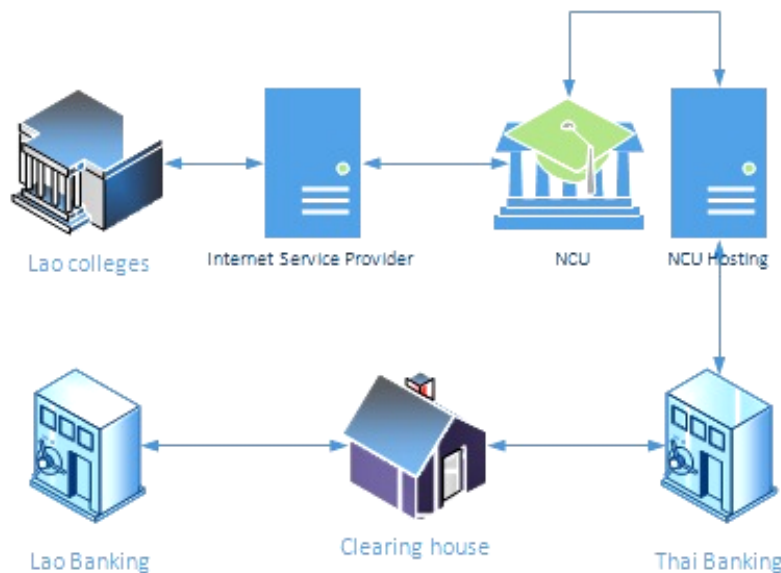
**TABLE IV**  
**RISK MATRIX FOR IT INFRASTRUCTURE**

| Impact | Likelihood     |                  |                |
|--------|----------------|------------------|----------------|
|        | High           | Medium           | Low            |
| High   | H,H<br>1 x 1   | H,M<br>1 x 0.5   | H,L<br>1 x 0   |
| Medium | M,H<br>0.5 x 1 | M,M<br>0.5 x 0.5 | M,L<br>0.5 x 0 |
| Low    | L,H<br>0 x 1   | L,M<br>0 x 0.5   | L,L<br>0 x 0   |

This section determines a vulnerability point found that there are 2 information assets which should be concerned including financial server and grad registration server. Moreover, there is a high motivation for attack to vulnerability point via public channel between

Lao colleges until NCU. They transfer a data on difference internet service providers which connect with many digital signals broadcasting point [15]. So, there is a likelihood level at high. On the other hand, when assets were attacked, it created a big blight for NCU and Lao colleges. So, there is an impact level at high. Risk evaluation for IT infrastructure at high level.

Security solution and policy is provided according with risk level of IT infrastructure in part of financial management which has characteristics of AEC as follows:



**Fig 3.** Financial System for Academy Cooperation

From fig. 3, NCU connect with Thai banking which provide an electronic credit card payment feature for university [14]. Lao student pays a semester fee on NCU website by credit card. Then, clearing house transfer a transaction from Lao bank into Thai bank that NCU provides account. Therefore, they complete a financial transaction by secure payment. These technological solution and policy is accepted from AEC academic partner who concern about cyber threat and problem by provide a secure payment at financial operation. On the other hand, there is another vulnerability point which is a grad registration.

NCU technician inform that there is an attack to grad registration server every day. Even though double firewall architecture could be used for protect a grad registration system, there is a high motivation of attacker especially a current student who desires to change a grad. Grad is an importance information asset which reflects a responsibility of higher education for sociality. CEO of NCU and Lao colleges very concern about grad registration system security. Therefore, they design a technological solution and policy for grad registration system as follows:

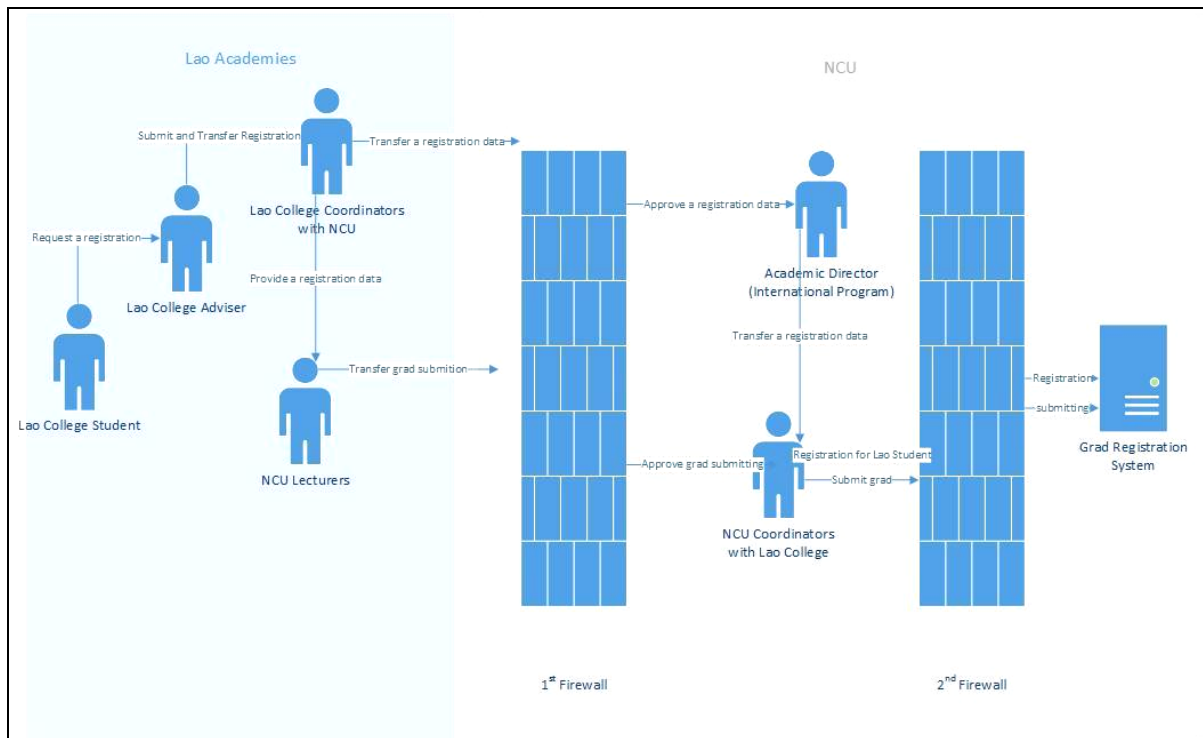


Fig 4. Technological Solution and Policy for Grad Registration System

Firstly, Lao student requests a subject registration with advisor who provides a subject in each semester. Then, adviser approved a transaction, and transfers them into coordinators with NCU. Coordinators transfers a registration data to academic director of NCU via registration system which provide an authentication system that allows user for through 1<sup>st</sup> firewall. Secondly, academic director transfer a registration data which is approved to NCU coordinator with Lao in order to register a student into subject via registration system which allows user through 2<sup>nd</sup> firewall for insert a data into database. Furthermore, 1<sup>st</sup> and 2<sup>nd</sup> firewalls are provided difference architecture in order to reduce a risk level when attacker can attack to 1<sup>st</sup> firewall. Technician could observe an abnormal transaction before attacker attack 2<sup>nd</sup> firewall.

Once lecturers complete a course, they will transfer a grad submitting into Lao coordinator who connects with NCU. Grad will be manage about submitting by NCU coordinator which standby back 1<sup>st</sup> firewall in order to submit a grad into database by grad registration system at 2<sup>nd</sup> firewall.

For concentrated, every transaction will be completed at 2<sup>nd</sup> firewall in order to protect a person who not an authority from other side of NCU. Thus, it is a technological solution and policy which is provided for grad registration system that suitable with education management of academy cooperation on AEC.

The security system development project is weaved to online content evaluation mechanism development project. Security is one part of mechanism which guaranties integrity of online content as follows:

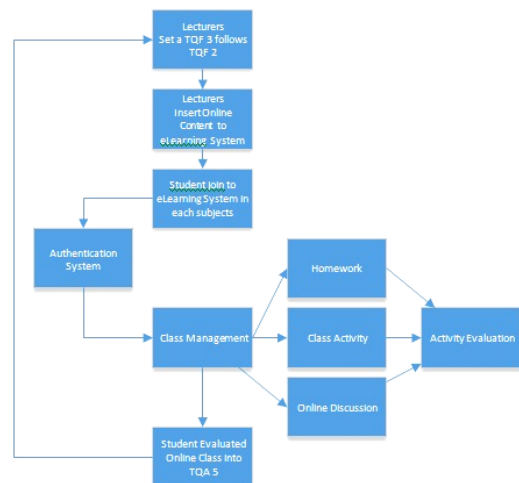


Fig 5. Online Content Evaluation Mechanism

Mechanism eases up from PDCA. Lecturer insert online content in online class room follows TQF3 which is drafted follow TQF2 [16]. Then, Lao student join with eLearning system, and access to virtual class room via authentication system. Every class, student and lecturer evaluated a homework, online discussion and class activity in order to evaluated overall of class in the end of semester. Once they start new class a counsel from TQF 5 will be used to amend new class.

#### IV. CONCLUSION

This article narrated regarding to security plan of NCU where arrange with Lao college. They assign to eLearning course, and technological solution and policy which react to security issue. Online content evaluation mechanism build into evaluate an efficiency of online content providing. Those projects are operated under strategy plan which is designed for suitable with academy cooperation in AEC.

This plan could be used for other university where connect with other academy in AEC in order to constructed an eLearning infrastructure which fit with several characteristics of each foreign academy. Moreover, this plan used to be decency other analysis design later.

#### V. ACKNOWLEDGMENT

This article got a research funding from North-Chiang Mai University.

#### REFERENCES

**(Arranged in the order of citation in the same fashion as the case of Footnotes.)**

- [1] (2015). "Asean Economic Community". <[http://www.thai-aec.com./](http://www.thai-aec.com/)>.
- [2] Ramjan, S. "The Conceptual Framework of mLearning Security of University in Thailand". IJCIM International Journal of Computer, Internet and Management, 2010, Vol. 18.
- [3] Ramjan, S. "The mLearning Security Rule-Base System with Social Network on eCampus: A Case Study of North-Chiang Mai University". IJCIM International Journal of Computer, Internet and Management, 2012, Vol. 20.
- [4] New Accesses Advisory Company Limited. (2015). "Final Report for Consulting and defining a competency indicator of consumer surplus in telecommunication business office of the national broadcasting and telecommunication commission".
- [5] Ramjan, S. and Dowpiset, K. (2011). "The conceptual framework of flexible security rule base system on Thai e-Tailer: virtual merchant". International Conference on Computer Research and Development.
- [6] Berrio-Zapata, C.L. and Rojas, H. (2014). "The Digital Divide in the University: the Appropriation of ICT in Higher Education Students from Gogota Colombia". Connicar, 22(43), pp. 133-142.
- [7] Cartelli, A.L., Stansfield, M., Connolly, T., Jimoyiannis, A.L., Magalhaes, H., and Maillet, K. (2008). "Towards the Development of a New Model for Best Practice and Knowledge Construction in Virtual Campuses". Journal of information Technology Education, pp. 7121-134.
- [8] Young, R. and Windsor, J. (2010). "Empirical Evaluation of Information Security Planning and Integration". Communications Of The Association for Information Systems, pp. 26245-566.
- [9] Tian, F. and Sean Xin, X. (2015). "How Do Enterprise Resource Planning Systems Affect Firm Risk?". Post-Implementation Impact. MIS Quarterly, 39(1), pp. 39-A9.
- [10] Bousalem, Z. and Cherti, I. (2015). "Xmap: A Novel Approach to Store and Retrieve XML Document in Relational Databases". Journal Of Software, 10(12), pp. 1389-1401.
- [11] Greg, F. (2015). "Blessay: Designing Enterprise DMZ and Multilayer Firewall Clusters". <<http://etherealmind.com/design-enterprise-dmz-firewall-clusters>>.
- [12] Tham Siew, Y.K. and Sanchita Basu, D.



- (2015). “The ASEAN Economic Community and Conflicting Domestic Interests”. *Journal of Southeast Asian Economies*, 32(2), pp. 189-201.
- [13] Borgohain, T., Borgohain, A., Jumar, U., and Sanyal, S. (2015). “Authentication Systems in Internet of Things”. *International Journal of Advanced Networking & Applications*, 6(4). pp. 2422-2426.
- [14] Sabi, H.S. (2014). “Research Trends in the Diffusion of Internet Banking in Developing Countries”. *Journal of Internet Banking & Commerce*. 19(2), pp. 1-31.
- [15] Roozbahani, F.S. and Azad, R. (2015). “Security Solution Against Computer Networks Threats”. *International Journal of Advanced Networking & Applications*, 7(1), pp. 2576-2581.
- [16] (2006). “National Qualifications Framework for Higher Education in Thailand”.  
<<http://www.mua.go.th/users/tqf-hed/news/FilesNews/FilesNews8/NQF-Hed.pdf>>.