SECTION 3
Government Information Security Management System Manual

- Drafted by Yusuke Tanaka, JICA Expert
- Edited by ICT Security Management Technical Team (iSMTT).

1. Introduction

The Government Information Security Management System Manual (GISMS Manual) is defined that Royal Government of Cambodia establishes, implements, checks and takes actions as a body of Government Information Security Management System, under the Government Information Security Management System Policy (GISMS Policy) declared by its Prime Minister, the chief of the government.

2. Scope

GISMS Manual covers all thirty-one government organizations stated as follows;

1. The Office of the Council of Ministers,
2. Ministry of Agriculture Forestry and Fisheries,
3. Ministry of Commerce,
4. Ministry of Culture and Fine Arts,
5. Ministry of Economy and Finance,
6. Ministry of Education Youth and Sports,
7. Ministry of Environment,
8. Ministry of Foreign Affairs and International Cooperation,
9. Ministry of Health,
10. Ministry of Industry Mines and Energy,
11. Ministry of Information,
12. Ministry of Interior,
13. Ministry of Justice,
14. Ministry of Labor and Vocational Training,
15. Ministry of Land Management, Urban Planning & Construction,
16. Ministry of National Defense,
17. Ministry of Parliamentary Affairs and Inspection,
18. Ministry of Planning,
19. Ministry of Post and Telecommunication,
20. Ministry of Public Works and Transport,
21. Ministry of Religions and Cults,
22. Ministry of Rural Development,
23. Ministry of Social Affairs Veteran and Youth Rehabilitation,
24. Ministry of Tourism,
25. Ministry of Water Resources and Meteorology,
26. Ministry of Women Affairs,
27. Municipality of Phnom Penh,
28. Secretariat of Public Service,
29. Secretariat of Civil Aviation,
30. National Information Communications Technology Development Authority (NiDA) and
31. Permanent Mission of the Kingdom of Cambodia to the United Nations.

3. Normative References, Terms and Definition

3.1. Normative References

The following referred documents are indispensable for the application of this document.

ISO/ISE 27001: 2005 Information technology – Security techniques – Information security management systems – Requirements

3.2. Terms and Definition

The followings are the terms and their definitions specifically used in GISMS.

Government Information Security Management System (GISMS):
It is ISMS for Royal Government of Cambodia in this manual. ISMS is referred to ISO/ISE 27001.

Government Information Security Office (GIS Office):
It is set up as a secretary at GCIO Committee and NiDA takes the role of GIS Office as part of its responsibility. It is responsible for setting up the policy, standards and guidelines of GISMS and is also responsible for all ISMS related topics in Royal Government of Cambodia. *This definition is a draft. GCIO patronage will be settled in GCIO development project.*

Chief Information Security Officer (CISO):
It is assigned to one official by ministry. Responsibilities are explicitly defined in GISMS Manual and Information Security Rule Book.

Information Security Manager (IS Manager):
It is assigned by ministry. Responsibilities are explicitly defined in GISMS Manual and Information Security Rule Book.

Risk Check Book:
It is a check book which identifies information assets, evaluates information assets, checks potential risks, identifies risks and evaluates risks.

Government Information Security Rule Book (GIS Rule Book):
It defines rule and procedures which secures each information asset. It is defined by ministry whereas its sample is developed by NiDA and the sample is highly recommended to apply as the minimum level as required to secure information.

4. Government Information Security Management System (GISMS)

GISMS takes the plan, do, check and action (PDCA) cycle as ISO27001 defines. This chapter defines these processes of GISMS.
It also defines document control and record control.

4.1. Plan (Establish)

Plan process consists of 5 sub processes; walkthrough policy and manual, define the scope of GISMS, assessing risks, develop GIS manual and obtain approvals.

4.1.1. Walkthrough GISMS Policy and GISMS Manual

First of all, read GISMS Policy, which declares the objective and policy of Kingdom of Cambodia GISMS. Walkthrough GISMS Manual (this document), which is applied to all government organizations of Kingdom of Cambodia, and which defines the unified rules to mobilize GISMS.

4.1.2. Define the Scope of the ISMS

When a ministry starts developing ISMS, it needs to define the scope for one cycle of PDCA. It is generally applicable to define the scope by physical facilities, such as a land boundary/building. It is also possible to define the

scope by information system network to effectively decide controls and treatments against threats. It needs careful to scope by organization chart, because it sometimes makes difficult to implement. The initial version of GISMS focuses only on Client PC as the minimum subset of fully-scoped ISMS developed in the future.

4.1.3. Assess Risks

Assess Risks procedure consists of five steps; Identify Information Assets, Evaluate Information Assets, Check Potential Risks, Identify Risks and Evaluate risks. The detailed procedure is defined in Risk Check Book. Please refer to an instruction in Risk Check Book. (See Appendix.1 Risk Check Instruction)

Step.1 Identify Assets

Identify assets. Risk Check Book has 6 default assets. 4 assets out of 6, such as Facility, Paper, Client PC, and Network & server assets are supposed to be defined by department for each to check by itself.

Step.2 Evaluate Assets

Next step is to evaluate assets. There are 3 elements of evaluation, Confidentiality, Integrity and Availability. Select one class of each according to the criteria shown below.

1: Confidentiality evaluation				
#	Class	Evaluation		Description
C1	1: General	1		Open information assets which go to public
C2	2: Internal	2		Information used only in a government business operation
C3	5: Confidential	5		Confidential among limited authorized people
2: Integrity evaluation				
#	Class	Evaluation		Description
I1	1: Low	1		No impact on business continuity by falsification
I2	3: Middle	3		Operational cost impact by falsification
I3	5: High	5		Political impact by falsification
3: Availability evaluation				
#	Class	Evaluation		Description
A1	1: Low	1		Out of service allowed over twenty four hours
A2	3: Middle	3		Out of service allowed up to twenty four hours
A3	5: High	5		Out of service allowed up to four hours

The total evaluation of an asset determines the total points of 3 elements. Review and revise confidentiality, integrity and availability evaluation if you feel a total asset value is different from actual.

4: Asset evaluation (Points = Confidentiality + Integrity + Availability)				
#	Class	Evaluation	Points	Description
As1	1: Low	1	3 to 6	Assets to impact moderately on an operation
As2	2: Middle	2	7 to 12	Assets to impact enormously on an operation
As3	3: High	3	13 to 15	Assets to impact enormously on an governing

Step.3 Check Assets

Check assets. Just select Yes or No for each check item.