Note:

Content

Notes on this GISSC:

This document is part of GISMS (Government Information Security Management System), which has been developed by NiDA and JICA for strengthening Information Security of RGC offices.

The stipulations stated here show the minimum requirements that each ministry or agency concerned should take into consideration through strengthening Information Security of the organization.

Various kinds of associated documents, such as guidelines and rule books, should be developed by each ministry and agency concerned.

KINGDOM OF CAMBODIA
NATION RELIGION KING

Government Information Security management System

Version 1.0 Revision 1

December 2009

Office of the Council Of Ministers
National Information Communications Technology
Development Authority
in cooperation with
Japan International Cooperation Agency

(NOT FOR SALE)

PART I
Additional Documents (prepared in 2009)

SECTION 1
Government Information Security Standard Criteria

Fundamental Policies

Government Information Security Standard Criteria

Fundamental Policies

1. Background

- Government ICT infrastructure has encountered the Information Security threats throughout the world, which may cause severe damages to the government information assets. The following are the typical cyberattacks, i.e.
  - Cyber terrorist: skilful and organized, usually having political intentions.
  - Hackers: skilful individuals who look for fun by disturbing people.
  - Cyber thieves/frauds: their purpose is only to grift money.

  Cyber criminals attack government ICT infrastructure, resulting either disabling e-Government services or stealing or destroying valuable information or classified government data base. Also, they will target ICT infrastructure of society, such as the Internet, aiming at just disturbance of citizen's life.

- It is a government emergency, if valuable information is leaked, stolen or changed within the governmental infrastructure by cyber criminals. Therefore it is extremely important for the government to strengthen Information Security and construct a protection system based on a firm and strategic planning.

2. Fundamental Policies

Considering the current information security threats environment, the government should introduce comprehensive and robust information security solutions to all the ministries and agencies at integrated quality level. In order to develop such robust integrated solutions, Information Security Standard Criteria shall be prepared as guideline. It should be aware that all the ministries and agencies are responsible for developing solutions for Information Security to protect their ICT systems in accordance with such a guideline. It is also important to sustain a good and stable quality of the government administration service, harnessing ICT, but combating with information security threats, which is glowing more serious day by day. Hence, the Information Security Standard Criteria should be reviewed and revised at least every year.

(1) Establishment of Government Information Security Standard Criteria (GISSC)

All the ministries and agencies are responsible for their ICT system development including implementation of Information Security protection according to the government common guideline. National Information Security Management Center (NISC) is responsible to prepare and maintain the guideline in principle. This guideline is called Government Information Security Standard Criteria (GISSC), which will be reviewed and elaborated every year, reflected with development of cybercrime

technology and change of nature of threats.
Considering urgency of Information Security issues, NiDA will tentatively act as NISC secretariat after delegation by the Government until the establishment of NISC, subject to fulfillment of limited roles.

The GISSC includes the following items:

- Organization and its responsibility structure
- Administration and Inspection
- Evaluation of Information Assets
- Consideration of Information Security protection to all application system
- Consideration of Information Security protection to all servers and clients
- Consideration of Information Security protection to network infrastructure
- Requirements for all Information Security functions, i.e.

Access control, authentication, encryption, security holes, facilities,

Internet common tools (such as network server (Web, mail, FTP, DNS,
etc.), firewall, router, switch…)

(2) Review of Ministry's Information Security Policies
Since all the ministries and agencies are responsible to develop and maintain their own ICT system, it shall be required to set up their own information security policies according to the GISSC. Integrity is an important key in this context.

(3) Self inspection
All the ministries and agencies are requested to inspect their ICT system periodically at least at the interval of a few months in accordance with the GISSC. If defects and misuse are found, suitable measures, including modifications, shall be taken immediately.

(4) Reviewing on PDCA cycle basis
The NISC shall be required to review the inspection report of each ministry or agency from the viewpoint of integrity with the GISSC. If a mismatch is found, comments and recommendations, advising how to rectify the mismatch, shall be sent back to the ministry or agency.

(5) Promotion to support Information Security sustainability
It shall be required to confirm certification issued by internationally recognized accreditation or qualification organization on Information Security, when the government purchasing ICT products, such as routers, switches, firewall appliances, etc., and/or also when employing ICT consulting or engineering firms, whenever possible. It shall be required to verify software firms, whether or not such firms are keeping the same level of Information Security policies and management process.

(6) Promoting Information Security of government related organizations

It shall be required for government related organizations to keep the same level of Information Security management process, referring to the GISSC.

(7) Coordination scheme between the NISC and all the ministries and agencies related to software vulnerability
The NISC should have a good communication with all the ministries and agencies, especially with the ministries which have controlled important ICT infrastructure, in order to exchange information on finding and analyzing new software vulnerability. Protective measures and procedures should be studied by the NISC and then the necessary information shall be forwarded to all the ministries and agencies as early as possible.
The NISC should deeply coordinate with National ICT Development Authority (NiDA) in this context, considering its roles and duties in developing Information Security framework at government level.

(8) Information security HRD scheme
It is difficult that the government keeps sufficient number of Information Security officers and/or engineers to satisfactorily perform Information Security management. Hence, the NISC should make a plan for required human resources development on Information Security upkeep. The NISC is also required to distribute to all the ministries and agencies a detailed software development guideline for Information Security protections, which will contribute to their software development.

(9) Intermediate-term planning for the government
The NISC should organize various kinds of taskforces for the government in order to combat against unexpected Information Security incidents. It should also be required that the NISC issues a guideline for basic Information Security requirements for procurement on ICT in the government, which is commonly applicable to all the ministries and agencies. It shall be considered that the essential mission of the NISC is to collaborate, control, cooperate and coordinate among the ministries and agencies related to Information Security issues.

[End of GISSC Fundamental Policy]

SECTION 2
Government Information Security Standard Criteria

Government Information Security Standard Criteria

1. Fundamentals

1.1 General Rules

1.1.1 A Need for management documentation on Information Security

As a basic rule, all the ministries and agencies are responsible to plan and implement Information Security measures to avoid any incident which may occur on ICT (Information and Communications Technology) infrastructure of the organizations concerned.

The government should provide all the ministries and agencies with "Fundamental Policies" and an integrated framework as the standardized guideline so that all the ministries and agencies can develop and improve their Information Security measures with high integrity considering their own priorities.

Since Information Security environment changes quickly, such a guideline should be reviewed periodically in order to avoid and prevent occurrence of new security incidents.

It is extremely important to define information data handling regulations which describe a handling scheme of information asset and information processing system with classification. It is also required to define rules not to create a breach of the regulations.

Government Information Security Standard Criteria (GISSC) is prepared for the purpose of guiding how to consider and implement a minimum requirement for Information Security Management at the government level in this context.

1.1.2 How to apply the documentation to all the ministries and agencies

The GISSC is designed to protect the government information asset. Information asset includes the following:

- Data stored in computers and electric storage media.
- Printed documents containing ICT system descriptions.
- Printed computer outputs.

Intended users of the GISSC are all government personnel and the like, including hired ICT consultants, who have a possibility of handling confidential data and materials.
Information Security measures shall be taken with priority. The priority varies depending on either or both importance of the information asset or impact of the Information Security threats.

Information Security measures should be sustainable enough. Therefore, each measure should be reviewed periodically referring to consistency with this GISSC.

1.1.3 Information Asset evaluation and its handling rules

In order to protect information on the government services from the incidents safely and securely, all information assets are evaluated and defined with classified numbers (priority) considering vulnerability. Those numbers are utilized to provide a rule of information handling as well. To classify the government services information, **CIA** shall be taken into account:

- **C (Confidentiality)**: leakage of top secret data, information and documents will cause a severe damage to either or both the government or the state of Cambodia.
- **I (Integrity)**: falsification of or damage to the information will cause damage to the government or the state of Cambodia.
- **A (Availability)**: ban on accessing or inability to access the information will cause damage to the government or the state of Cambodia.

All of information (database unit) shall be classified properly depending on its importance and vulnerability. Handling of the information, such as copying, delivery, transfer, should appropriately be managed so that it may result in proper restrictions according to its classified categories.

1.2 Organization and responsibility development

1.2.1 Organization and responsibilities

Organization and responsibility on Information Security management shall be considered in line with the following:

(1) **A Chief Information Security Officer (GCIO)** is appointed, who has a supreme responsibility to all Information Security management at each ministry or agency concerned.

(2) **An Information Security Management Committee (ISM Committee)** is organized in each ministry or agency in order to plan, implement, check and review Information Security initiatives of the ministry or agency concerned.

(3) **Information Security Managers (IS Managers)** are appointed in the ministry or agency concerned in order to manage all information security work. IS Managers are responsible to make sure and sustain Information Security rules under the control of GCIO. It is an important duty that those IS Managers always maintain good communication with IS Managers of other ministries and agencies.

(4) Breach of rules
If government personnel become to know a breach of Information Security rules, such misbehavior has to be reported to IS Manager immediately. IS Manager will take appropriate actions. If needed, a fact of the breach of rules should be reported to GCIO.

1.2.2 Breach reporting

If the government personnel find a severe breach of Information Security, he or she should inform one of IS Managers of such a fact. IS Manager will take an appropriate action accordingly as a result of consultation with GCIO. It is also required for IS Manager to relay the breach to IS technical staff immediately, together with the action taken.

1.2.3 Administration

(1) Education on Information Security measures
All IS Managers shall plan and implement the following tasks:

- Prepare and maintain documents of Information Security rules and measures.
- Make plan and organize Information Security training course(s) for government personnel at least once a year in order enhance awareness of importance of Information Security and its practicing.

(2) Dealing with fault or incident

a. Readiness for occurrence of fault or incident
IS Manager shall maintain his or her team to be ready to respond quickly to an information security incident so that damage can be minimized and recovery can be done in the shortest period of time.

b. Report and emergency recovery procedure after fault or incident occurring
When fault or incident occurring is detected by government personnel, he or she should give a report to any IT technical staff immediately for quick response. He or she should also be required to report to the Information Security Manager according to a reporting procedure. At the same time, the IT technical staff should contact and consult with the IT Manager on actions to be taken.

1.2.4 Inspection
All the ministries and agencies shall perform self inspection for Information Security management as quality evaluation and implement such practice twice a year. The results should be reported to GCIO.

All the self inspection reports will be summarized by NiDA, which undertaken the work as the secretariat of National Information Security Management Center (NISC) and then the summary will be uploaded to the government Website for internal information sharing among government personnel. All the ministries and agencies shall be requested to improve their Information Security measures, if and when weakness of the measures has been found.

1.2.5 Review of guidelines
It should always be required for all IS Managers and IT technical staffs to review existing guidelines so that mismatch, inadequacy and out-of-datedness of the

guidelines can be found in the integrity of latest Information Security environment. If serious problematic points are found, those should be reviewed by a higher authority, including GCIO and then adequate actions shall be advised by the higher authority.

1.2.6 Outsourcing
When work for software development, information processing, survey and study work is outsourced, the ministry or agency should keep Information Security of the outsourced by the same level as their own level. In this context, the ministry or agency may provide the outsourced with all requirements of Information Security policies and guidelines available.

1.3 Handling information asset

1.3.1 Data handling

(1) Data creation and input
The government personnel shall follow the information handling rules when information including database is generated.

(2) Use of data
The government personnel shall handle information properly according to the information classification rule. When information is copied, it should be handled according to the original information secrecy classification.

(3) Data storing
The following rules should be defined for accessing to the stored information.

- Access control
- Identification and password control
- Encryption when needed

(4) Data transferring
Transferring of information to another computer needs permission of IS Manager, if the information belongs to high security level. A password protection and information backup are also needed.

(5) Data publication
When the government information is publicized, information handling scheme should be checked and confirmed. Permission of the IS Manager should also be required.

(6) Data deletion
When deletion of the government information is required, it should be confirmed unrecoverable.

1.4 Measures for information processing

1.4.1 Restrictions on use of information processing outside the government
IS Manager should prepare and maintain information security rules for outsourcing, if and when the government information processing is required by outsourcing partly or as a whole. Permission of GCIO, as well as IS Manager, should be required for

the outsourcing implementation.

1.4.2 Restrictions on using Saas (Software as a service)
Use of Saas shall be considered a kind of outsourcing. The clause 1.4.1 above shall be applied. Confirmation of Service Agreement (SA) is important in this concern. Including GCIO and IS Managers, SA shall be evaluated in detail.

1.5 Measures for information processing system

1.5.1 Requirement for information security
IS Manager should consider the following security items, when an information system development scheme is planned.

- Information Security requirements
- Availability of maintenance personnel who have sufficient knowledge and skill of Information Security
- Information Security measures to be required for both development and operation

1.5.2 Development rules and compliance with information processing system at government level

(1) Documentation and log
IS Manager shall prepare and maintain the following documentations:

- Users list and users record
- Software name list with version/revision numbers and updated history
- Requirements, specifications and design documents
- Response workflow manual against faults and incidents

(2) Procurement of equipments
GCIO and IS Managers shall prepare and maintain procurement procedure to purchase equipment and devices based on the information security requirements.

(3) Software development
IS Managers shall prepare and maintain the following guidelines for software development project:

- Organize development team, including staff(s) that can handle and deal with information security requirements.
- Prepare design documents explicitly on implementation of required Information Security.
- Define scope of design review and implementation procedure.
- Provide an appropriate access control and backup method for source code files.
- Define scope of source code review and implementation procedure.
- Define appropriate testing items and procedures considering Information Security requirements.
- Record and verify test result data.

(4) Standard guidelines for encryption and digital signature
It should be required to set and use government standard encryption algorithm system. Keys used for both encryption and digital signature should be backed up and kept safely.

(5) Keeping good Information Security literacy
IS Managers shall create and maintain adequate measures for not causing breaches in activities outside the government.

(6) Rules for domain name use
The domain name of the government shall be used at all the ministries and agencies of the government without exception. The domain name of the government is "gov.kh" at the moment.

(7) Daily routine work to avoid malware infection of computers
IS Managers shall prepare and maintain the following guidelines for avoiding infection of computer malware, such as virus, spyware, and bot:

- Adequately update operating system. In this context, always use genuine copy of operating system.
- Use security software (anti-virus software and/or anti-spyware).
- Always update anti-virus/anti-spyware definition file.
- Do not download and execute any file which is detected as malware.
- Make automatic updating function of security software available.
- Check files with security software when transferred both inside or outside
- Disconnect communication line (LAN cable) immediately from computer, whenever infection is found by security software, whether it is actual or potential.

2. Information Processing

2.1 Measures for specifying Information Security requirements

2.1.1 Information security functions

(1) Identification management
IS Managers should control all the users with identification (user name and password) in order to manage all the users to access to information processing system with security. Every password shall be changed periodically. The identification system should be configured to alert each user the necessity of change of the password at an interval of specified period, for instance, three months each. Computers shall be set not to run without change of the password in this context.
It is strongly required to encrypt identification and password data when stored or transferred. It is also strongly recommended that IS Manager should maintain and update the users data based on administration rules and according to change of organization.

(2) Access control functions
IS Manager shall manage access control for all the users to the information

processing system in the ministry or agency concerned.

(3) Privilege management functions
IS Manager shall manage privilege control for users as an extension of the identification and password control. The privilege is concerned to the information manipulating operation, such as confirmation, change, update, deletion, transfer, etc.

(4) Log monitoring functions
IS Manager shall monitor information processing system, utilizing log monitoring function for observation. The scope of the log monitoring and its function will include diagnosis, inspection, reporting, etc., which will vary according to the requirements for information processing system.

(5) Assurance functions
IS Manager shall provide a measure of assurance function for all information processing system, such as recovery, backup, duplication, etc.

(6) Encryption and digital signature (including key management)
IS Manager shall consider introducing encryption function for handling high-classified confidential information. Digital signature function and safe key management method should be considered for this purpose as well.

2.1.2 Information security threats

(1) Measures for security holes
IS Manager should always study measures to avoid any security holes of the installed information processing system and communication system. Therefore continuous work for collecting information on updates of security holes shall inevitably be required.

(2) Countermeasures against malware
IS Manager shall install security software into all computers to protect malware infection, including viruses and spyware.

(3) Countermeasures for DDoS attacks
IS Manager shall always study and prepare all the possible functions to prevent DDoS (Distributed Denial of Service) attacks in coordination and collaboration with telecom carries, ISPs, CSIRT, etc., which are working for Information Security upkeep inside and outside Cambodia.

(4) Measures for stepping-stone attacks

Cyber attackers usually use Stepping-stone attacks in order to hide their identity. To detect these kinds of attacks, IS Manager shall take all kinds of measures available. Since the measures have been studied in laboratories, Information Security firms, carriers, universities, etc. in many countries, IS Manager shall continuously make their efforts to study applicable measures so that reappearance of hacking or attacks can be stopped and then damage to information processing system can be minimized.

2.2 Measures for information system components

2.2.1 Facility and environment

A proper safety space for installing critical server machines and communication equipment should be considered.

a. Facility entrance management
IS Manager shall control unauthorized people regarding access to the restricted area, in which the facilities that require high level security have been installed. In this context, it should be physically required to isolate computers, ancillary equipment and peripheral equipment from other regularly working areas. Adequate physical locking and alarming shall be considered. Access to those facilities should be controlled and recorded as well.

b. Management of visitors
Visitors shall be registered at entrance to make the security sure and this operation shall be done based on a rule properly. At least information on the visitor (name, position and organization purpose of visit and time to enter/leave) and permitter's signature shall be recorded in a blotter, leaving the belongings of the visitor at entrance.

c. Protection agaist theft
Computers, communication equipment, ancillary and peripheral equipment should be protected from theft by adequate measures.

d. Security control within the restricted area
Any personnel should always carry their identification. Without the identification no one shall be permitted to enter the area.

e. Disaster and fault management
IS Manager shall make physical protection for computers and communication equipments and the ancillary and peripheral equipment to avoid or minimize damage from unforeseen circumstances including disasters. It is also required to shut electric power feeding down to the facilities in consideration of safety for all personnel working at the time of such occurrence.

2.2.2 Computers

(1) Capacity planning

IS Manager should study proper planning for computer system performance, checking a load to the computer system, network traffic, fault occurrence, human error occurrence, etc.

(2) Client software arrangement

IS Manager shall manage all client software installation. Both desk top and portable PCs shall be kept at the same Information Security arrangement level in case of the same organization, even though the portable PCs may be used outside the government office. Installation of P2P (Peer to Peer) application shall be limited. Without approval of IS Manager, use of such software shall be prohibited at all in case of government office.

(3) Server maintenance

IS Manager shall consider to arrange tight security access, including use of encryption system, when the server maintenance is implemented through communication line from outside.

2.2.3 Application software

(1) e-mail

IS Manager shall make a proper arrangement for the e-mail server, avoiding malicious use of e-mail relay by hackers. It shall also be required to utilize authentication function with checking user identification and password.

(2) Web

IS Manager shall avoid attacks from malicious hackers to government Web site. All the possible preventive and protective measures should be taken in order to resist and abandon such inadequate illegal accesses to the Web site. All the information processing system shall be constructed tightly against illegal accesses not to be retrieved government information from the government servers, including file downloading.

(3) Domain Name System DNS

IS Manager shall arrange configuration of DNS server(s) properly to provide continuous name solution service (converting domain name to IP address). It should also be considered importance of operation and maintenance of DNS Contents Server to maintain consistent administration procedures.

The following attacks by hackers should be protected:

- DNS Cache Server setting to avoid accepting external request of domain name service.
- Information leakage protection, when providing domain name service.

2.2.4 Communication line

(1) Measures for common communication line

IS Manager shall manage the following items:

- Proven and verified hardware and software products should be selected to set up continuous and stable communication.
- It should be required to classify computers into adequate groups, which are connected to communication equipment.
- It should be defined communication link utilization requirements in order to provide proper access and routing control functions.

(2) Intranet management

IS Manager shall provide an access authorization function for intranet connection, when accessing to communication lines.

The following functions should be studied and implemented:

- Periodic review of access control data.
- Monitoring of quality of signal transmission to detect a malfunction of communication equipment.

- Monitoring of contents of communication.

(3) Extranet management
IS Manager shall provide an access authorization function for extranet connection, when external communication line connection to the outside of the government is requested.

It is also required to satisfy minimum information security requirements for the external connection. If not secured enough, setting up a dedicated communication line should be installed.

The following functions should be studied and implemented:

- Periodic review of access control data.
- Monitoring of quality of signal transmission to detect a malfunction of communication equipment.
- Monitoring of contents of communication.

[End of GISSC]

SECTION 3
Office Information Security Check Book

Office Information Security Check Results
at [ ]

NiDA
by Mr./Ms.
on

The following checking is prepared just as the first step of Information Security of office management.

Control Category	Item to be Checked	Site Photograph as Evidence	Current Situation (Check Result)	Measures to be Taken	Judgment
Outsourcing	Criteria of selecting contractor(s)			documentation	
	Availability of nondisclosure obligation in contract			documentation	
Private Information or Personal Data	For employer: Availability of nondisclosure obligation in employment contract or other agreement			documentation	
	For employee: Availability of nondisclosure obligation in employment contract or other agreement			documentation	
	For company: Availability of covenant or contract clause on protecting personal data or private information			documentation	
Office Building	Authorization of entering room and availability of record of entering/leaving room	Indispensable		rule establishment	
	Demarcation of office space and other accessible common space			notice board	

	Lockup system	Preferable		high grade locking	
	Work of outsiders			rule establishment	
	Data protection for employees, contract, etc.			rule establishment	
	Record keeping for use of courier service, etc.	Preferable		rule establishment	
Fax machines and Printers	Record of personal use for faxing			rule establishment	
	Neglect of printed materials/faxed materials without care	Preferable		rule establishment	
	Record of faxing (sending/receiving)			rule establishment	
	Record of faxing confidential materials			rule establishment	
Cabinet/Book shelf	Classification/categorization of information			rule establishment	
	Personal data protection by locking function	Indispensable		rule establishment and locking	
	Document protection	Indispensable		rule establishment	
	Document keeping period			rule establishment	
	Record media keeping by locking function			rule establishment and locking	

Desktop PC	Clearing g display screen by setting screen saver function with password	Preferable		rule establishment	
	Availability of criteria of user ID and password management			rule establishment	
	Password setting			rule establishment	
	Common use of user ID and password			don't use	
	Save of personal data			rule establishment	
	Wrong addressing of mail and hacking of mails			rule establishment	
	Use of virus scanning software			to be applied	
	Updating of pattern files of the above			to be applied	
Desktop Itself	Lockup of desk when getting out			rule establishment	
	Clearing desktop without any confidential information, when leaving			rule establishment	
	Disposal/neglect of personal information	Preferable		rule establishment	
LAN and the Internet	Protection of network	Preferable		rule establishment	
	Security measure of network equipment			rule establishment	

	Disconnection of internal network from external network			rule establishment	
	Log of access to network			rule establishment	
Mobile PC or Laptop PC	Permission of taking mobile PC out			rule establishment	
	Save of personal data			rule establishment	
	Keeping of PC when getting out	Preferable		rule establishment	
Servers	Access to server room and its lockup			rule establishment	
	Authorization to access server room			rule establishment	
	Availability of criteria of user ID and password management			rule establishment	
	Use of antiseismic reinforcement			rule establishment	
	Measures for electric power failure			rule establishment	
	Protective measures for server equipment	Preferable		rule establishment	
	Availability of server operation			rule establishment	
	Backup equipment			rule establishment	
	Backup of data			rule establishment	
	Backup media protection	Preferable		rule establishment	

	Access to personal information			rule establishment	
	Access to confidential files			rule establishment	
	Authorization of access to personal data and confidential files			rule establishment	
	Log of access to personal data/confidential files			rule establishment	
	Protection of personal data from unlimited access			rule establishment	
	Verification of access control function of personal data			rule establishment	
	Remote access measures			rule establishment	
Disposal or Scrapping	Use of paper shredder	Preferable		rule establishment	
	Scrapping of media			crashing	
	Scrapping of PC			storage media crashing and disposal certification	

Other Particulars	Notes: 1. About "Judgment" G: Good A: Acceptable P: Poor - to be improved 2. Site Photograph: Indispensable -- Snapshots must be taken Preferable -- Snapshots shall be taken, whenever possible	