SECTION 5
Government Information Security Rule

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

1. Introduction

The Government Information Security Rule Book (GIS Rule Book) at NiDA is defined as NiDA implements the Government Information Security Management System (GISMS) under Information Security Management System Policy and the Government Information Security Management Manual (GISMS Manual).

2. Three Basic Rules to Secure Information

[Rule 1] Always consider whether you acquire, process or save confidential information. Do NOT expose information against any risks of leakage, falsification and inaccessibility.

[Rule 2] Lock up an office entrance, a cabinet and a desk drawer before walking away for any moment.

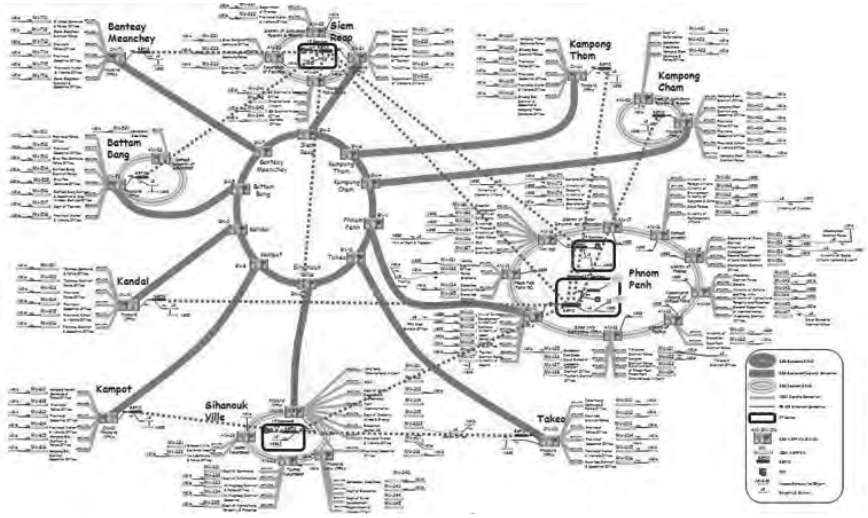
[Rule 3] Activate an auto-detection function of anti-virus software. Update a virus definition file at least weekly. Scan a storage device of your PC weekly and any external storage devices (e.g. FD, Memory Card/Stick and HDD) when to connect to your PC.

3. Scope

The GIS Rule Book covers National Information Communication Technology Development Authority (NiDA), which consists of the following departments; *General Administration, Infrastructure, Network, Enterprise, Content and Applications, Human Capacity Building and FOSS and Policy.* The GIS Rule Book also covers the following organizations under Secretary General; *Secretary General Office, Information Desk, Cambodia Computer Emergency Response Team, Singapore Operation Program, CISCO Training, and The Priority Management Group.*

From a network/system perspective, the GIS Rule Book covers client PC. The scope of GIS Rule Book will be extended to Servers and PAIS in the future.

NiDA has paid attention to develop the project Provincial Administration Information System (PAIS) and connect network system to all provinces.



(National Information Infrastructure Diagram)

4. Normative References, Terms and Definition

4.1. Normative References

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

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

2) The Government Information Security Management System Manual (GISMS Manual)

4.2. Terms and Definition

The followings are the terms and their definitions specifically used in GIS Rule Book.

Client PC:

It is a local PC as a type of desktop PC, laptop PC or mobile PC.

All other terms are referred to Terms and Definition in GISMS Manual or ISO/ISE 27001.

5. Information Security Organization

5.1. Information Security Organization Definition

NiDA sets the following information security roles and responsibilities.

Information Security Office (ISO):

It is set up at NiDA. It is responsible for implementing ISMS at NiDA. ISO members are CISO, IS Manager and IS In-charge, which are defined below.

Chief Information Security Officer (CISO):

One person is assigned at a ministry. He/she is also a member of Government Information Security Office (GISO), which is defined in GISMS.

Information Security Manager (IS Manager):

The role is assigned to an official by department. Its responsibilities are defined both in GISMS Manual and in GIS Rule Book.

Information Security In-charge (IS In-charge):

The role is assigned to an official also by department. Its responsibilities are defined in GIS Rule Book.

Official: All other employees of the in-scope organization.

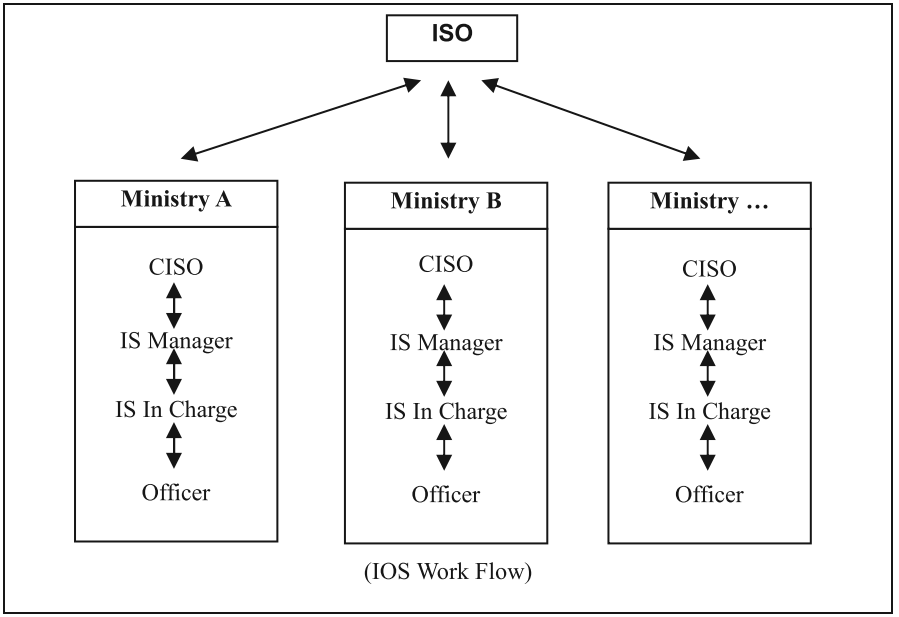
5.2. ISO Member List

ISO members will be assigned by the Secretary General of the National ICT Development Authority (NiDA).

5.3. Communication Route at Emergency

The reporting path is generally defined, from Officials to IS In-charge, IS In-charge to IS Manager, IS Manager to ISO/CISO. The instructing path is generally defined, from CISO/ISO to IS Manager, IS manager to IS In-charge, and IS In-charge to Officials in vice versa.

In the diagram is ISO work flow organization chart:



(IOS Work Flow)

6. Rule and Procedures

6.1. Information Classification

(a) Rule

(a1) Information used in a government business operation is classified into three categories.

1. General:
   Open information which goes public
2. Internal:
   Information used only in a government business operation
3. Confidential:
   Confidential among limited authorized people

(a2) Classify information when you acquire and it is highly recommended one is marked or labeled showing the information classification.

(a3) Always manage information carefully according to the classification.

(a4) Classify privacy information always as confidential.

(b) Procedure

(No procedure is applied for this section.)

6.2. People Security (To be defined in a future)

(a) Rule

(This section defines the security requirements of people matter such as the candidate qualification check in the hiring process, a job description related to information security matters, and the requirements at the termination of employment.)

6.3. Facility Security

6.3.1. Office Building and Room

(a) Rule

(a1) Define those who can enter the facility/room.

(a2) Implement an appropriate key system for an entrance of the facility/room.

(a3) Separate an office space and the other accessible common space.

(a4) Get outsiders with an insider attendant.

(a5) Record an entry and exit.

(a6) Keep records of courier service.

Suspension

(b) Procedure

(No procedure is applied for this section.)

6.3.2. Cabinet and Desk

(a) Rule

(a1) Store information assets with confidential information and lock up cabinets.

(b) Procedure

(No procedure is applied for this section.)

6.3.3. Fax Machine and Printer

(a) Rule

(a1) Dispose printed materials/faxed materials with care.

(a2) Keep record of faxing (sending/receiving).

(b) Procedure

(No procedure is applied for this section.)

6.4. Physical Information Security

6.4.1. Paper

(a) Rule

(a1) Always carefully identify confidential information within each paper/document.

(a2) Save confidential paper/documents in safe against unauthorized access.

(a3) Officials must burn disposing paper by themselves. Or use a paper shredder with disposing paper including confidential information.

(b) Procedure

(No procedure is applied for this section.)

6.4.2. Digital Archives (DVD/CD/FD/Tape)

(a) Rule

(a1) Always carefully identify confidential information within each archive.

(a2) Save confidential archives in safe against unauthorized access.

(a3) Scrap a media (Tape/FD/CD/DVD) physically.

(b) Procedure

(No procedure is applied for this section.)

6.5. Client PC Security

6.5.1. Desktop PC

(a) Rule

Overall

(a1) The physical security of 'your' client PC is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.

(a2) All PCs MUST be assigned to a unique responsible official even if one is used by multiple officials.

(a3) You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. The password must be robust and be changed periodically. Never share it with anyone, not even members of your family, friends or IT staff.

(a4) Avoid leaving a PC unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

Virus Protection

(a5) Viruses are a major threat to NiDA and client PCs are particularly vulnerable if their anti-virus software is not kept up-to-date. The virus definition file MUST be updated at least weekly. The easiest way of doing this is simply to log on to the LAN for the automatic update process to run. If you cannot log on for some reason, contact Information Security Office

for advice on obtaining and installing anti-virus updates.

(a6) Always virus-scan any files downloaded to your computer from any source (FD/CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans must be set to happen automatically. It is also required to initiate scheduled scans at least weekly.

(a7) Report any information security events (such as virus infections) promptly to Information Security Office in order to minimize the damage.

(a8) Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting Information Security Office. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

(a9) Be especially careful to virus-scan your system before you send any files. This includes E-mail attachments and FD/CD/DVDs that you create.

(a10) Connect UPS for all desktop PCs not to lose information.

Disposal
(a11) Execute a physical formatting of storage in a PC not to leave any information readable.

(b) Procedure
For All Officials
Anti-virus Protection
(b1) The following procedure is defined to make sure that all PCs have the updated anti-virus software with a certain frequency.

Step	Description	Owner	Records
b1.1	Instruct the submission of anti-virus software scan log.	ISO	n/a
b1.2	Execute scan.	Official	n/a
b1.3	Print out and submit a scan log.	Official	Anti-virus software scan log
b1.4	File a scan log and keep for the defined period.	IS In-charge	n/a
b1.5	Follow up those who has not executed a scan and submitted a log.	IS In-charge	n/a

Virus Detection Handling
(b2) The following procedure is defined to take actions against virus