

Government Information Security (GIS) Rule Book Contents

GIS Rule Book is defined by ministry. The following introduces NiDA GIS Rule Book. It is the specific rule which needs to be done internally and it will be added in the future to get more secured environment. It can be copied and modified for each ministry GIS Rule Book. The initial version of Information Security Rule Book is focused on **client PC security**. (pink shaded part)

1.	Introduction	6.5.	Client PC Security
2.	Three Basic Rules to Secure Information	6.5.1.	Desktop PC
3.	Scope	6.5.2.	Laptop/Mobile PC
4.	Normative References, Terms and Definition	6.5.3.	Storage Devices (Portable Hard Disk / Memory Stick / Memory Card / Floppy Disk)
4.1.	Normative References	6.5.4.	Personal Properties
4.2.	Terms and Definition	6.5.5.	Software
5.	Information Security Organization	6.5.6.	E-mail
5.1.	Information Security Organization Definition	6.5.7.	Web Browsing
5.2.	ISO Member List	6.6.	Network and Server Security (To be fully defined in a future)
5.3.	Communication Route at Emergency	6.6.1.	LAN and Internet
6.	Rule and Procedures	6.6.2.	Server Common
6.1.	Information Classification	6.7.	Application Software Security (To be defined in a future)
6.2.	People Security (To be defined in a future)	7.	Information Security Training
6.3.	Facility Security	7.1.	Information Security Training Execution
6.3.1.	Office Building and Room	7.2.	Promissory Letter Submission
6.3.2.	Cabinet and Desk	8.	Measurement
6.3.3.	Fax Machine and Printer	9.	Breach (To be defined in a future)
6.4.	Physical Information Security	10.	Records List
6.4.1.	Paper		
6.4.2.	Digital Archives (DVD/CD/FD/Tape)		

18

Client PC Security Rule – Desktop PC

Desktop PC

This page is cited from Government Information Security Rule Book.

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.

19

Procedure

This page is cited from Government Information Security Rule Book.

Virus Detection Handling

Step	Description	Owner	Records
b2.1	Detect an information security event such as virus detection.	Official	n/a
b2.2	Physically off-line from a network immediately.	Official	n/a
b2.3	Inform ISO immediately when the event happens.	Official	Information Security Event Report
b2.4	Analyze the effects of an event and take an appropriate action.	ISO	n/a
b2.5	Terminate any network/application services if necessary.	ISO	n/a
b2.6	Execute an emergent anti-virus protection procedure if necessary.	ISO	n/a
b2.7	Record an analysis and an action in a report.	ISO	(Updated) Information Security Event Report
b2.8	File a report and keep for the defined period.	IS In-charge	n/a 20

Records – Information Security Event Report

All information security events should be reported and handled appropriately by the in-charge personnel.

Information Security Event Report

Reporter		Reported		Record Number:
Name: []		Name: []		
Department: []		Department: []		
Contact (Cell/E-mail) : []		Reported Time: []		
Event Type:		Action:		
<input type="checkbox"/> Virus detection <input type="checkbox"/> Inappropriate settings/installation <input type="checkbox"/> Undesirable/unsavory e-mail data <input type="checkbox"/> Others				
Event Time: []				
Situation:				
		Lessons Learned		
		Name: []		
		Department: []		
		Recorded Time: []		
		Lessons Learned:		

Three Basic Rule 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.

22

Information Security Management Example – Disciplinary Action

Details of Disciplinary Action taken in May 2007

TO: All XYZ Company People in Japan

Business ethics are critical for our company's success because they build trust and transparency. Trust and transparency, in turn, build the right environment for our clients, our suppliers, our stakeholders and the communities in which we operate throughout the world.

However unfortunately, there have been some violations of our business ethics here and there within the company.

To prevent such violations, we have revised our business ethics regulation.

Considering insufficient working regulations in Royal Government of Cambodia, GIS Rule Book at the first stage takes no disciplinary actions.

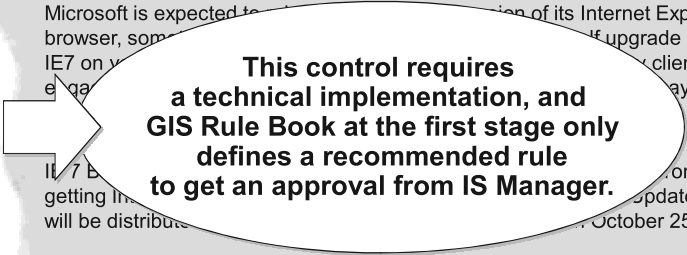
								Dismissal under instruction	Dismissal on disciplinary grounds
Acts of harassment									
Improper/fraudulent claims related to time report								1	
Information security violations	4	7	4		1				
Other		4							
Total	4	15	4		1			1	

23

To: All XYZ Company People in Japan

Microsoft is expected to release a new version of its Internet Explorer browser, some of which may require an upgrade to IE7 on your computer. If you are a client of our service, you may not be able to use our service until you have updated your browser. We will be distributing the new version of the browser to our clients from October 25th.

This control requires a technical implementation, and GIS Rule Book at the first stage only defines a recommended rule to get an approval from IS Manager.



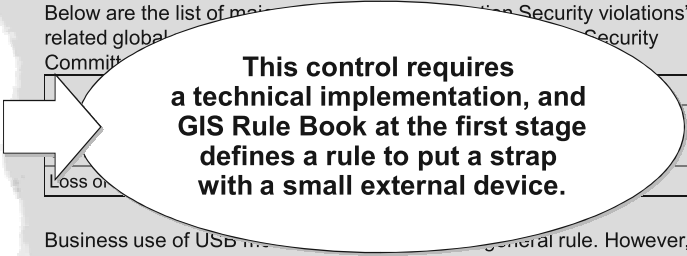
To: All XYZ Company People in Japan

Below are the list of major "Information Security violations" and related global security incidents. The list is part of a document titled "Information Security Committee Report".

Loss of	

Business use of USB memory is a general rule. However, the security administrator may permit such use as project policy if one of the following conditions is met. 1. If the USB memory has a password protection 2. If the USB memory has a biometric authentication function (fingerprint authentication, etc.) 3. If files are always encrypted or password protected when saved in USB memory.

This control requires a technical implementation, and GIS Rule Book at the first stage defines a rule to put a strap with a small external device.



To: All XYZ Company People in Japan

As of December 30, 2007, access to specific non-business websites from the office LAN was blocked.

IT department has been reviewing internet access logs to investigate recent activities. We found large files such as... activities in... traffic. In... reasons... traffic.

This control requires a technical implementation, and GIS Rule Book at the first stage only defines a rule not to access web sites with inappropriate materials.

Example
youtube.co

Company resources provided for business use, although limited personal use is acceptable as stated in Policy 57. Excessive personal use is not allowed. Your good sense is expected for the appropriate use of the Company resources. Failure to comply with XYZ Company policies will be reported and disciplinary action may be taken.

Action Plan