(a2.3) In ways that could be interpreted as representing or being official public statements on behalf of the organization, unless you are a spokesperson explicitly authorized by management to make such statements;

(a2.4) To send a message from anyone else's account or in their name (including the use of false 'From:' addresses). If authorized by the manager, a secretary may send e-mail on the manager's behalf but should sign the e-mail in their own name per pro ('for and on behalf of') the manager;

(a2.5) To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, color, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;

(a2.6) For any other illegal, unethical or unauthorized purpose.

(a3) Apply your professional discretion when using e-mail, for example abiding by the generally accepted rules of e-mail etiquette.

(a4) Review e-mails carefully before sending, especially formal communications with external parties.

(a5) Do not unnecessarily disclose potentially sensitive information in "out of office" messages.

(a6) Except when specifically authorized by management or where necessary for IT system administration purposes, officials must not intercept, divert, modify, delete, save or disclose e-mails.

(a7) Limited personal use of the corporate e-mail systems is permitted at the discretion of local management provided always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all e-mails traversing the government systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.

(a8) Be reasonable about the number and size of e-mails you send and save. Periodically clear out your mailbox, deleting old e-mails that are no longer required and filing messages that need to be kept under appropriate e-mail folders.

Suspension

(The clause will be activated after the government e-mail service installs the auto-scan function.)

(The clause will be activated after the government e-mail service gets stable.)

(b) Procedure
For All Officials
Normal Information Security Events Handling

(b1) The following procedure is defined to report any information security events promptly.

Step	Description	Owner	Records
b1.1	Detect an information security event such as undesirable/unsavory e-mails are delivered.	Official	n/a
b1.2	Inform ISO within an hour after the event happens.	Official	Information Security Event Report
b1.3	Analyze the effects of an event and take an appropriate action. Record those in a report.	ISO	(Updated) Information Security Event Report
b1.4	File a report and keep it for the defined period.	IS In-charge	n/a

6.5.7. Web Browsing

(a) Rule

Overall

(a1) Do not download an executable file without permission from Information Security Manager.

(a2) Download a file only which has a certification.

(a3) Do not click any links in an undesirable web site or e-mail.

(a4) It is highly recommended not to save cookies, which may cause User ID/password leak.

(a5) Set up a web browser associated to the previous clauses.

Inappropriate Materials

(a6) Be sensible! NiDA will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the client PC and steer clear of dubious websites. Information Security Office routinely monitors the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to Chief Information Security Officer, and disciplinary processes will be initiated. If you receive inappropriate material by e-mail or other means, delete it immediately. If you accidentally browse to an offensive website, click ‘back’ or close the window straight away. If you routinely receive a lot of spam, call Information Security Office to check your spam settings.

(b) Procedure

For Information Security Office

Web Browser Setting Patrol Check

(b1) The following procedure is defined to audit web browser setting internally.

Step	Description	Owner	Records
b1.1	Plan and prepare web browser settings patrol check such as the date and sampled PCs. Instruct the setting before a patrol check.	ISO	n/a
b1.2	Check web browser settings one by one. When found a nonconformance, instruct a PC owner fix the setting.	IS In-charge	n/a
b1.3	Submit an Information Security Event Report if found a nonconformance.	Official	Information Security Event Report
b1.4	File a report and keep it for the defined period.	IS In-charge	n/a

6.6.Network and Server Security (To be fully defined in a future)

6.6.1. LAN and Internet

(a) Rule

Suspension

This section will be activated after PAIS is integrated with GAIS and system administration will be operated basically on PAIS. Develop a system administration manual for GAIS/PAIS and CamCERT network respectively which includes the updated network architecture/configuration and detailed operation procedures cooperating with other groups such as Information Security Office.

(b) Procedure

(No procedure is applied for this section.)

6.6.2. Server Common

(a) Rule

Suspension

This section will be activated after PAIS is integrated with GAIS and system administration will be operated basically on PAIS. Develop a system administration manual for GAIS and CamCERT system respectively which includes the updated system architecture/configuration and detailed operation procedures cooperating with other groups such as Information Security Office.

(b) Procedure

(No procedure is applied for this section.)

6.7. Application Software Security (To be defined in a future)

(a) Rule

(This section defines the information security requirements to application software and those to an application software development project.)

7. Information Security Training

7.1. Information Security Training Execution

All officials must get Information Security Training at least once a year. The following procedure is defined to plan and conduct information security training.

	Description	Owner	Records
b1.1	Plan information security training both for the experienced and newly-hired officials	ISO	n/a
b1.2	Conduct a training session.	IS In-charge	n/a
b1.3	Record who took the session and keep it for the defined period.	IS In-charge	Training Record

7.2. Promissory Letter Submission

All officials must once submit Promissory Letter to secure information. It is desirable to sign out at the time of training. The following procedure is defined to submit Promissory Letter.

Step	Description	Owner	Records
b2.1	Distribute promissory letter blank.	ISO	n/a
b2.2	Read through, sign out and submit one.	Official	Promissory Letter
b2.3	File and keep it for the defined period.	IS In-charge	n/a

8. Measurement

The following items will be measured by IS In-charge and reported at ISO at least yearly. The report enables to improve ISMS based on an objective detail.

#	Measurement Name	Definition	Authorized by
1	Training Completion Rate	% of those who has completed training among all NiDA Officials	CISO
2	Information Security Event Mean Time to Process Completion by Event Type	Sum up (Process Completion Time - Event Occurred Time) divided by the number of events by Event Type* (Event Type is defined on an Information Security Event Report blank)	CISO
3	Anti-Virus Scan Execution Rate	% of those who has completed anti-virus scan among all NiDA Officials at the time of an anti-virus protection procedure issue.	CISO
4	Promissory Letter Submission Rate	% of those who has submitted Promissory Letter among all NiDA Officials	CISO
	-End of List-		

9. Breach (To be defined in a future)

(a) Rule

(This section defines the penalty against the information security breaches. It needs internal human resources regulation of government officials.)

10. Records List

#	Records Name	Reference	Blank drafted by	Authorized by
1	Training Record	Chapter 7.1 Information Security Training Execution	ISO	CISO
2	Information Security Event Report	(1) Virus Detection Handling Procedure in Chapter 6.5.1 Desktop PC (2) Lost/Stolen Properties Handling Procedure in Chapter 6.5.2 Laptop/Mobile PC (3) Software Setting Patrol Check Procedure in Chapter 6.5.5 Software (4) Normal Information Event Handling Procedure in Chapter 6.5.6 E-mail (5) Web Browser Setting Patrol Check Procedure in Chapter 6.5.7 Web Browser	ISO	CISO