detection.

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

6.5.2. Laptop/Mobile PC

(a) Rule

Overall

The following rules are for laptop/mobile PC specifically. The laptop/mobile PC is also required to implement the rule and procedures defined in 6.5.1 **Desktop PC**.

(a1) Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

(a2) If you have to leave the PC temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.

(a3) Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.

(a4) Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about! Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

(a5) Government-owned laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.

(a6) Keep a note of the maker, model, serial number and the asset owner label (e.g. NiDA) of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform Information Security Office as soon as practicable (within hours not days, please).

Controls against unauthorized access to laptop/mobile PC data

(a7) Be highly recommended to use approved encryption software on all laptop/mobile PCs, choose a long, strong encryption password/phrase and keep it secure. Contact Information Security Office for further information on laptop encryption. If a laptop/mobile PC is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.

(a8) Do NOT save confidential information on your laptop/mobile PC instead of encrypting described in the previous clause.

(b) Procedure

For All Officials

Lost/Stolen Properties Event Handling

(b1) If a laptop/mobile PC is lost or stolen, follow the procedure described as a normal information security event.

Step	Description	Owner	Records
b1.1	Detect an information security event such as a property lost or stolen.	Official	n/a
b1.2	Notify the Police.	Official	n/a
b1.3	Inform ISO within an hour after the event happens.	Official	Information Security Event Report
b1.4	Analyze the effects of an event and take an	ISO	(Updated) Information

	appropriate action. Record those in a report.		Security Event Report
b1.5	File a report and keep it for the defined period.	IS In-charge	n/a

6.5.3. <u>Storage Devices (Portable Hard Disk / Memory Stick / Memory Card / Floppy Disk)</u>

(a) Rule

Overall

(a1) Put an appropriate strap on those devices to keep them with you firmly. The recent high-tech storage devices are so small that they are easily dropped off and lost.

Virus Protection

(a2) Do NOT auto-run any storage devices when connecting to your computer.

(a3) Always virus-scan any storage devices when connecting to your computer.

Disposal

(a4) Execute a physical formatting of storage or scrap it physically not to leave any information readable.

(b) Procedure

For All Officials

Lost/Stolen Properties Event Handling

(b1) If any storage devices are lost or stolen, follow the procedure described in **Lost/Stolen Properties Event Handling** in **Laptop/Mobile PC** rule and procedures.

6.5.4. <u>Personal Properties</u>

(a) Rule

(a1) Get a permission of Information Security Manager to bring/take personal client PC related properties into/out of an office.

(b) Procedure

(No procedure is applied for this section.)

6.5.5. <u>Software</u>

(a) Rule

Overall

(a1) Install software explicitly allowed by IS manager.

(a2) Configure software according to IS In-charge instruction.

(a3) Apply patches promptly after IS In-charge instructs.

Unlicensed Software

(a4) Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and organizations are being prosecuted for infringing software copyright: do not risk bringing yourself and NiDA into disrepute by breaking the law.

Unauthorized Software

(a5) Do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the NiDA networks as well as affecting the working of your PC. Software packages that permit the computer to be 'remote controlled' (e.g. PCanywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on NiDA equipment properties unless they have been explicitly pre-authorized by management for legitimate business purposes. (e.g. Network Working Group for network auditing operation)

Backups

(a6) You must take your own backups of data on a client PC. The simplest way to do this is to logon and upload a data from the PC to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to FD/CD/DVD, USB hard disk /memory card/sticks etc. Make sure that off-line backups are encrypted and physically secured. Remember, if a client PC is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the PC. Off-line backups will save you a lot of heartache and extra work.

(b) Procedure

For Information Security Office

Patch Application Instruction

(b1) The following procedure is defined to instruct apply patches.

Step	Description	Owner	Records
b1.1	Update a standard software setting and the latest patches information list periodically. (The list may contains a general clause such as "Always apply windows update promptly unless it is prohibited explicitly.")	ISO	(Standard software setting and the latest patches information list)
b1.2	Distribute the list to	IS In-charge	n/a

	Officials and enhance them apply promptly.		
b1.3	Apply patches promptly after IS In-charge instructs.	Official	n/a

Software Setting Patrol Check

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

Step	Description	Owner	Records
b1.1	Plan and prepare software setting patrol check such as the date and sampled PCs. Instruct the setting before a patrol check.	ISO	n/a
b1.2	Check software 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

6.5.6. E-mail

(a) Rule

(a1) E-mail attachments are now the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.

(a2) Do not use e-mail:

(a2.1) To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;

(a2.2) For private or charity work unconnected with the organization's legitimate business;