

**SECURITY INCIDENT HANDLING PROCEDURE**

**FOR**

**COMBINED SYSTEM DEVELOPMENT SERVICES**

**OF**

**self-certification system (LSCP)**

**FOR THE**

**BUILDINGS DEPARTMENT**

Version: 0.3

**Jan 2025**

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

|  |  |
| --- | --- |
| **Distribution** | |
| Copy No. | Holder |
| 1 | Buildings Department |
| 2 | Master Concept Limited (MC) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Amendment History** | | | | |
| **Change Number** | **Revision Description** | **Pages Affected on Respective Version** | **Revision / Version Number** | **Date** |
| 1 | 1st draft | All | 0.1 | 7/11/2024 |
| 2 | Incorporated relevant changes suggested by ITU except Table of Content | All | 0.2 | 14/11/2024 |
| 3 | Rename Support Team Name | All | 0.2.1 | 18/11/2024 |
| 4 | Rename SCS to LSCP | All | 0.3 | 16/01/2025 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[**1.**](#_heading=h.qsh70q) **Introduction 4**

[**2.**](#_heading=h.3as4poj) **Person responsibility 6**

[2.1 Roles 6](#_heading=h.1pxezwc)

[2.2 RESPONSIBILITY 6](#_heading=h.49x2ik5)

[**3.**](#_heading=h.2p2csry) **General procedureS 7**

[3.1 KEEP A LOG BOOK 7](#_heading=h.147n2zr)

[3.2 INFORM THE APPROPRIATE PEOPLE 7](#_heading=h.3o7alnk)

[3.3 Follow-up analysis 8](#_heading=h.23ckvvd)

[**4.**](#_heading=h.ihv636) **Incident prevention procedureS 9**

[4.1 virus PREVENTION POLICY 9](#_heading=h.32hioqz)

[4.2 Password Policy 9](#_heading=h.1hmsyys)

[4.3 Server Security Policy 10](#_heading=h.41mghml)

[4.4 patch / hot fix Update from product Vendor 10](#_heading=h.2grqrue)

[**5.**](#_heading=h.vx1227) **incident Specific procedures 12**

[5.1 VIRUS and WORM INCIDENTS 12](#_heading=h.3fwokq0)

[5.2 Ad-ware and spyware INCIDENTS 14](#_heading=h.1v1yuxt)

[5.3 Illegal access to system 15](#_heading=h.4f1mdlm)

[5.4 Denial of system resources 17](#_heading=h.2u6wntf)

[**6.**](#_heading=h.19c6y18) **APPENDIX 19**

[APPENDIX A -](#_heading=h.3tbugp1) PRELIMINARY INFORMATION SECURITY INCIDENT REPORTING FORM 19

[APPENDIX B -](#_heading=h.28h4qwu) POST-INCIDENT REPORT 20

[APPENDIX C -](#_heading=h.nmf14n) Departmental IT Security Contacts Change Form 22

[APPENDIX D –](#_heading=h.37m2jsg) IDENTIFICATION OF INCIDENT 23

# Introduction

This Security Incident Handling Procedure is one of the deliverables submitted as part of the Licensing Self-Certification Portal (LSCP) System for Buildings Department provided by MC.

The objective of this document is to provide a guideline for handling security incidents that may occur to the LSCP. Some examples of possible incident are listed below:

* Virus infected
* Worm infected
* Illegal access to system
* Denial of system resources

The following shows some common scenarios that may consider as a security incident’s case:

* You see a strange process running and accumulating a lot of CPU time.
* You have discovered an intruder logged into the system.
* You have discovered a virus has infected the system.
* You have determined that someone from a remote machine/site is trying to penetrate the system.

In all the above cases, operator may use this document as a guideline on handling security incidents.

This document is intended to provide general procedures for security incident handling in LSCP for Buildings Department. It is not intended to cover the technical details of the above functional areas.

The following are the goals of the Security Incident Handling Procedure order by its priority:

1. Protect loss or theft of sensitive data.
2. Protect public image of the bureau/department or the Government as a whole.
3. Protect data which are costly when lost or damage
4. Return the system to normal operation in the shortest possible time.
5. Prevent damage to systems with costly downtime and recovery cost
6. Avoid further incidents
7. Collect evidence to support subsequent case investigation
8. Identify the root cause of the incident
9. Assess the impact and damage of the incident
10. Update policies and procedures as needed

The following guidelines and policies have been referred when preparing this document:

* Information Security Incident Handling Guidelines [G54]
* BD’s Information Security Incident Response and Handling Procedures.
* Baseline IT Security Policy
* IT Security Guidelines
* BD IT Security Policy
* Practice Guide for Information Security Incident Handling

# Person responsibility

## 2.1 Information Security incident response team (ISIRT) Roles

Some person(s) who may be involved in the security incident are listed as follows:

|  |  |  |
| --- | --- | --- |
| **Role Name** | **Short Name** | **Parties** |
| ISIRT Commander | ISIRTC | BD |
| ISIRT Incident Response Manager | ISIRTIRM | BD |
| ISIRT Information Coordinator | ISIRTIC | BD |
| ISIRT Information System Manager | ISIRTISM | BD |
| Business Assurance  Coordinator | BAC | BD |
| User Assurance Coordinator | UAC | BD |
| IT System Support Manager | SSM | BD |
| IT System Support Officer | SSO | BD |
| Vendor Support Engineer | VSE | MC |

## 2.2 RESPONSIBILITY

In many cases, more than a single person may be involved. Different persons are responsible on different role. Their responsibilities are listed on the following table:

|  |  |
| --- | --- |
| **Person** | **Role & responsibilities** |
| ISIRT Commander | Provide overall supervision and co-ordination of information security incident handling for all information systems within the B/D.  Make decisions on critical matters such as damage containment, system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery, etc. based on the incident report and analysis provided by the Incident Response Manager.  Trigger the departmental disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the B/D.   * Provide management endorsement on the provision of resources for the incident handling process. * Provide management endorsement in respect of the line-to-take for publicity on the incident. * Coordinate and collaborate with GIRO-SO in the reporting of information security incidents for central recording and necessary follow-up actions in particular with the following characteristics:   (i)  System providing public service and its failure will result in service interruption (e.g. denial of service attack to a government Internet website)  (ii)  System handling classified information  (iii)  System supporting mission critical operation  (iv)  System which would be subject to a highly undesirable impact if a security incident occurs, e.g. affect the Government's public image due to website defacement   * Facilitate experience and information sharing within the B/D on information security incident handling and related matters. * Coordinate and cooperate with investigation authorities in the investigation of security incidents. |
| ISIRT Incident Response Manager | * Overall management and supervision of all matters concerning security incident handling within the B/D * Alerting the ISIRT Commander upon receipt of report on security incident affecting the departmental information systems. * Following up with the Information System Manager and related parties to compile incident report and conduct analysis. * Reporting the progress of the security incident handling process to the ISIRT Commander. * Coordinating various external parties, such as HKPF, PCPD, service contractors, support vendors, and security consultants, etc. in handling the incident. * Seeking necessary resources and support from the ISIRT Commander for the incident handling activities |
| ISIRT Information Coordinator | * handling public inquiries regarding the security incident of the B/D. The Information Coordinator is also responsible for the overall control and supervision of information dissemination to the public, including the media |
| ISIRT Information System Manager | * Oversee the security incident handling process for the functional area in-charge. * Speed up and facilitate the handling process by pre-establishing relevant handling procedures and list of contact points in advance. * Provide a direct channel for receiving reports about suspected incidents. * Provide direct and instant response to suspicious activities. * Assist in minimising damages and recovering the system to normal operation. * Seek advice on security issues from external parties such as service contractors, computer product vendors, HKPF, or PCPD. * Coordinate security incident handling of the respective information system with other external parties. * Conduct impact analysis on the security alerts received from the ISIRT and the GovCERT.HK in respect of the functional area in-charge |
| Business Assurance Coordinator (BAC) | * Overseeing the LSCP |
| User Assurance Coordinator (UAC) | * User co-coordinator for LSCP, all incidents from normal user will be directly report to UAC * Report any abnormal situation that may consider as security incident to SSO * Decision maker of handling minor Security Incident cases. |
| IT System Support Manager (SSM) | * Identify the level of Security Incident cases (Minor/major) * Evaluate the effect of the incident |
| IT System Support Officer (SSO) | * Consult VSE to provide solution for any security incident if necessary * Report any incident to IT System Support Manager * Seek recommendation and assistance from VSE on matters related to the security incident * System Support for LSCP |
| Vendor Support Engineer | * Perform all the appropriate remedial and recovery actions for any security incident is found (note: this is to in line with the requirement specified in Assignment Brief) * Provide security control activity logs and reports * Maintenance support person from MC |

# General procedureS

This section provides information on procedures which are common for all types of security incidents.

## 3.1 KEEP A LOG BOOK

Logging of information is critical in situation which may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents which are under investigation. The information should be logged in a location that cannot be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The logbook will be maintained by the SSO. The types of information that should be logged are:

* Dates and times of incident-related phone calls.
* Dates and times when incident-related events were discovered or occurred.
* Amount of time spent working on incident-related tasks.
* People you have contacted or have contacted SSO.
* Descriptions on the reported incidents
* Names of systems, programs or networks that have been affected.
* Level of incident (High/Low)

## 3.2 INFORM THE APPROPRIATE PEOPLE

Informing appropriate person is very important while a security incident is located because the incident may affect the normal operation of the LSCP. If a user experiences a situation that may be a security incident, the user should report the incident to the UAC. The UAC should report the incident to the SSO immediately.

If the SSO has experience a security incident that need suggestion on the case, the SSO may contact VSE for any recommendation. If the SSO consider the priority/ impact of the incident is high, then the SSO should inform the situation to the SSM. In this situation, the SSM should make decision on what reaction should be done for the incident and report to the BAC if necessary.

If the SSO consider the priority/ impact of the incident is low and able to recover the system in a short period of time, then the SSO should inform the status of the incident to the UAC before taking steps to fix the problem and after the incident was fixed.

The list of contacts is provided as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Contact Person** | **Title** | **Phone Number** |
| ISIRT Commander | BD User | TBD | TBD |
| ISIRT Incident Response Manager | BD User | TBD | TBD |
| ISIRT Information Coordinator | BD User | TBD | TBD |
| ISIRT Information System Manager | BD User | TBD | TBD |
| Business Assurance Co-ordinator | Mr. Owen CHAN | SBS/IT | 3842-3521 |
| User Assurance Co-ordinator | Mr. TSUI Ka-km, Kim | SBS/Lic1 | 3842-3282 |
| IT System Support Manager | Mr. Simon CHAN | PM2/CS | 3842-3514 |
| IT System Support Officer | Mr. Simon W CHAN | CSA7 | 3842-3459 |
| Vendor Maintenance Manager | Ernie NG | Maintenance Manager | 5316-2728 |

## 3.3 Follow-up analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, several follow-up activities should be done. The SSO may arrange a meeting to explore the necessary action need to take if necessary. The following lists some follow-up actions:

* Update logbook on incident status, description and solution
* Update anti-virus definition for all the machines if necessary
* Apply security patches for all the machines if available
* Provide a guideline to all users (thru UAC) and refine current incident handling procedure to prevent the incident to happen again
* Report to the technology Crime Division of the Hong Kong Police Force Commercial Crime Bureau of the incident is suspected to be a criminal offense

# Incident prevention procedureS

This section discusses the procedures for preventing incident from happening or minimizes the effect when security incident is occurring. UAC and SSO should follow the below procedure to minimize the possibility on security incident occurring.

## 4.1 virus PREVENTION POLICY

* Always install the corporate standard, supported anti-virus software. Download and install anti-virus software updates as they become available.
* NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash in the email client.
* Delete spam, chain, and other junk email without forwarding if user’s computer has email client installed.
* Never download files from unknown or suspicious sources.
* Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. For example, images sharing for LSCP desktop module.
* Always scan a floppy diskette/ USB thumb disk or other external media from an unknown source for viruses before using it.
* Back-up critical data and system configurations on a regular basis and store the data in a safe place. For server, at least 1 set of backup tape should be offsite.
* New viruses are discovered almost every day. Periodically check the Anti-Virus definition and update the definition if necessary.

## 4.2 Password Policy

* All system-level passwords (e.g., root, Windows admin, application administration accounts …etc.) must be changed on at least a quarterly basis if possible.
* All user-level passwords (e.g., Windows user, LSCP accounts …etc.) must be changed at least every 90 days.
* User accounts that have system-level privileges granted through group memberships or application password must have a unique password from all other accounts held by that user.
* Passwords must not be inserted into email messages or other forms of electronic communication.
* All user-level and system-level passwords must conform to the guidelines described below
  + Are at least ten alphanumeric characters long including digits [0-9], lowercase characters [a-z] and uppercase characters [A-Z].
  + Are not a word in any language, slang, dialect, jargon, etc.
  + Are not based on personal information, names of family, etc.
  + Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

## 4.3 Server Security Policy

* Services and applications that will not be used must be disabled where practical.
* The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
* Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
* Always use standard security principles of least required access to perform a function.
* Do not use root when a non-privileged account will do.
* Servers should be physically located in an access-controlled environment.

## 4.4 patch / hot fix Update from product Vendor

* When security alert or OS patch from Microsoft is received, the patch will be applied to Hot Standby or DR Server of LSCP first. The Server/ Application/ Database will be full backup before the patching. A CRF for the patching will also be issued to appropriate vendors.
* After applying the patch, the system functions will be tested.
* If the patch is applied successfully, the patch will be scheduled to be applied at Production LSCP. Since there may be service disruption, users have to agree on the scheduled downtime. The Server/ Application/ Database of Internet LSCP will be full backup before the patching.
* After applying the patch, the system functions will be tested.

# incident Specific procedures

This section discusses the procedures on handling some scenarios of incident as listed as follows:

* Virus and worm incidents
* Adware and spyware incidents
* Illegal access to the system
* Denial of system resources

Other security incident may occur to the system, SSO should log all incidents according to procedures given in section 3 and work out the specific procedures for the incident.

## 5.1 VIRUS and WORM INCIDENTS

Although virus and worm attack are very different, the procedures for handling each are quite similar. First of all, we have to isolate the infected system. Viruses are not self-replicating and thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in short time, thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of the attack, then proceed as if the attack was worm related. Procedures for handling virus and worm infections are listed as follows:

1. Isolate the infected system
2. Notify the appropriate people
3. Identify the problem
4. Remove the virus or worm from the system
5. Update the system to prevent the system from re-infection
6. Return the machine to normal operational mode
7. Follow-up Analysis

### 5.1.1 Isolate the Infected System

Virus and worm may spread to other server(s) or workstation(s) quickly. After a system is identified to be infected with virus or worm, SSO should isolate the infected system by disconnect the system from the network. SSO should isolate the system no matter the infected system is a server or normal client workstation.

SSO should not reboot or power off the infected system because many viruses should destroy all disk data while system restarted.

### 5.1.2 Notify the Appropriate People

SSO should notify the incident to UAC. In the meantime, SSO should inform UAC how long the incident will be fixed and the approximate time that server will be resumed normal.

SSO should report the incident to VSE with necessary details. If necessary, VSE should provide recommendation to fix the problem and recover the system.

### 5.1.3 Identify the Problem

The SSO should try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system should be taken and saved. Below is a list of tasks to make a snapshot of the system:

* Navigate to the system log of the Windows system
* Write down any abnormal situation discovered from the system.
* Check the log of the Anti-virus software to see whether a virus is found by the application
* Check any abnormal processes running in the system by launching Windows Task Manager by pressing (Ctrl+Shift+Esc)
* Collect any information from the involved parties (e.g. UAC) as well.

If specific files which contain virus or worm code can be identified, then move those files to an external media (floppy, tape…etc.)

If recommendation is needed from VSE, SSO should notify VSE with the symptoms and his / her observations of the system. VSE should provide recommendations to deal with the situation.

### 5.1.4 Remove the Virus or Worm from the System

After sufficient information was collected and the source of problem is identified, SSO should perform a full system backup if possible before the any removal or recovery operations. The following is some possible procedure of removing the virus or worm:

* Update the virus definition manually using external media
* Update Windows® patches if available using external media
* Other information/steps that collected from the checked sources

If the system was already destroyed by the virus or worm and it cannot be recovered by virus cleanup or patch updates, a full system restore using the former backup of system image is necessary. In order to perform full system restore, machine must reconnect to the network. Make sure that the worm or virus is already removed before reconnect the system to the network. You may need to perform a system format operation to system disk as an effort to recover the system. If possible, backup all the related data such as database and images files before that operation. You can therefore restore data upon finished with the system format.

The system should be restored or recovered to normal operation status after the above procedures applied.

### 5.1.5 Update the System to Prevent the System from Re-infection

After the system is restored to normal operational status, SSO should take steps to minimize the possibility of re-infection of the same virus or worm. Normally if a solution can be found from the reference, an anti-virus definition, worm security patches or other steps should be included in the solution. Simply follow the steps to install the necessary patches to prevent the system from re-infection.

### 5.1.6 Return the Machine to Normal Operational Mode

Reconnect the fixed system to the network after finished with the above operation. SSO should notify UAC and in turn the UAC should notify users the LSCP services have been resumed. The UAC should confirm whether or not the services of LSCP are running properly. The UAC should report to SSO with any missing data or image. Before restoring connectivity to the outside world, verify that all affected machines & all other machines are successfully immunized from the specific virus and worm.

### 5.1.7 Follow-up Analysis

Perform the steps described in Section 3.3

## 5.2 Ad-ware and spyware INCIDENTS

There are many adware and spyware in the Internet world. Mostly of the findings could occur in the workstations that use Internet frequently. Navigating some of the website in the Internet may accidentally get the ad-ware or spyware live inside the machine.

The handling procedure for adware and spyware infections are similar, the procedure can be separate to 4 steps as below:

1. Identify the problem
2. Remove the adware or spyware from the system
3. Update the system to prevent the system from re-infection
4. Follow-up Analysis

The following will provide a more detail description on the above 4 steps. In each step, SSO should record down the situations and description of incident into the logbook.

### 5.2.1 Identify the problem

If the system is function properly, then SSO should collect the following information in order to identify the specific virus or worm is infected the system.

* Navigate the system log of the Windows® system
* Write down any abnormal situation discovered from the system.
* Check the log of the Anti-virus software to see whether a virus is found by the application
* Check any abnormal processes are running in the system by launching Task Manager (Ctrl+Shift+Esc)
* Perform searching using phrase of the symptoms in Microsoft® security page and Symantec® support page to locate any characteristic that match the incident.
* Collect any information from the involved parties (e.g., UAC). For example, the website visited recently.
* Notice any abnormal behavior in the Windows® system and Internet browser.

### 5.2.2 Remove the Adware and Spyware from the System

After collected enough information and the problem is located. A recovery procedure should be planned to use the collected information. If the problem is unable to locate, SSO should inform the VSE on the incident and VSE should provide recommendation on the incident. The following is some possible procedure of removing the virus or worm:

* Stop the adware or spyware services running in the system. Delete the specific files manually.
* In some cases, the adware or spyware files may be running and unable to delete. If necessary, remove the startup key from the registry. Reboot the system and delete the file(s) afterward.
* Update the virus definition.
* Update Windows® patches if available.
* Other information/steps that collected from the checked sources

### 5.2.3 Update the System to Prevent the System from Re-infection

After the system is restored to normal status, SSO should take action to minimize the possibility of re-infection of the same adware or spyware. Normally if a solution can be found from the reference site (refer to Section 5.1.3), an anti-virus definition, worm security patches or other steps should be included in the solution. Simply follow the steps to install the necessary patches to prevent the system from re-infection.

Inform the UAC after the incident was fixed.

### 5.2.4 Follow-up Analysis

Perform the steps described in Section 3.3

## 5.3 Illegal access to system

### 5.3.1 Identify the Problem

Illegal access is defined by someone was found attempting to, gains unauthorized use or access to the system without proper authorization. Illegal access may be the symptom of hacker/cracker activities as the effort as penetration or intrusion.

Illegal access can be identified by the following symptom:

* A system alarm or similar indication from intrusion detection tools
* Suspicious entries in system or network accounting (e.g., user obtains administrator access without going through the normal sequence)
* Accounting discrepancies or unexpected user accounts creation or deletion. Inability to login due to modifications of account. Unexpected change of user password
* A part of or the entire system log is missing or altered
* System crashes
* Unauthorized operation of a program
* Suspicious probes, such as numerous unsuccessful login attempts
* Suspicious browsing activities, such as account with administrator privilege accessing many files of different user accounts

### 5.3.2 Notify the Appropriate People

SSO should notify the incident to UAC. In the meantime, SSO should inform UAC how long the incident will be fixed and the approximate time that server will be resumed normal.

SSO can report the incident to VSE if help is needed to recover the system.

### 5.3.3 Containment

Impact assessment of the incident on data and information system should be done if the data or service has already been damaged by or infected in the incident. Classified or critical information and system should be protected. For instance, move the critical information to other media (or other systems) which are separated from the compromised system or network.

Operation status of the compromised system should be decided whether it should be suspended.

A case should be built for investigation purpose and as evidence for subsequent follow-up action. All actions taken during this stage should be kept recorded.

Any systems associated with the system through shared network-based services or through any trusting relationship should be checked and suspended if necessary.

ISIRT should conduct review periodically to determine if the incident is under control. If it is not under control or it is going to have a severe impact on the B/D’s core services, follow the predefined escalation procedures for crisis management.

### 5.3.4 Eradication Methods

There are two methods for dealing with an illegal access incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction. The method used to handle an illegal access incident will be determined by the level of understanding of the risks involved.

After considered the risk, you can stop or kill all active processes of the hacker to force the hacker out.

Delete all the fake files created by the hacker. System operators may need to archive the fake files before deletion for the purpose of case investigation.

Update the access passwords of all login accounts that may have been accessed by the hacker.

In some cases, the SSO may need to reformat all the infected media and reinstall the system and data from backup, especially when you are not certain about the extent of the damage in a critical system or it is difficult to completely clean up the system.

The SSO should keep a record of all actions performed.

### 5.3.5 Recovery Procedures

For simple incidents (such as failed intrusion attempt), make sure the systems or the data are not affected or damaged by the incident.

Re-install the deleted/damaged files or the whole system, whenever required, from the trusted source.

Bring up function/service by stages, in a controlled manner, and in order of demand, e.g. the most essential services or those serving the majority may resume first.

Verify that the restoring operation was successful and the system is back to its normal operation.

Prior notification to all related parties on resumption of system operation, e.g., operators, administrators, senior management, and other parties involved in the escalation procedure.

Disable unnecessary services.

Keep a record of all actions performed.

### 5.3.6 Return the Machine to Normal Operational Mode

SSO should notify UAC and in turn the UAC should notify users the LSCP services have been resumed. The UAC should confirm whether or not the services of LSCP are running properly. The UAC should report to SSO with any missing data or image.

### 5.37 Follow-up Analysis

Perform the steps described in Section 3.3

## 5.4 Denial of system resources

### 5.4.1 Identify the Problem

Denial of System Resource or Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

In general terms, denial of system resource attacks is implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

The denial of system resource can be identified by the following symptom:

* Unusually slow of server response in opening files
* Unusually slow of network performance in accessing web sites
* Unavailability of the LSCP web site itself
* Inability to access any web site from the Internet connecting servers

### 5.4.2 Notify the Appropriate People

SSO should notify the incident to UAC. In the meantime, SSO should inform UAC how long the incident will be fixed and the approximate time that server will be resumed normal.

SSO can report the incident to VSE if help is needed to recover the system.

### 5.4.3 Containment Methods

If the system has already been compromised, then disconnect the system from Internet, backup the file system, re-install the operating system and restore the file system. You should install operating system updates provided by OS vendor. If the update is security-related, then it is especially crucial to install it.

### 5.4.4 Return the Machine to Normal Operational Mode

SSO should notify UAC and in turn the UAC should notify users the LSCP services have been resumed. The UAC should confirm whether or not the services of LSCP are running properly. The UAC should report to SSO with any missing data or image.

### 5.4.5 Follow-up Analysis

Perform the steps described in Section 3.3

# APPENDIX

## APPENDIX A - PRELIMINARY INFORMATION SECURITY INCIDENT REPORTING FORM

|  |  |
| --- | --- |
| **Background Information** | |
| Name of Department: | |
| Brief description on the affected system (e.g., function, URLs): | |
| Location of the affected system: ❒ In-house system ❒ Outsourced service  System administration/operation by:  ❒ In-house IT team ❒ End user ❒ Outsourced service provider | |
| **Reporting Entity Information** | |
| Name: | Designation: |
| Office Contact: | 24 hours Contact: |
| E-mail Address: | Fax Number: |
| **Incident Details** | |
| Date/Time (Detected): | Date/Time (Reported to BD LSCP Support): |
| Symptoms of Incidents: | |
| Impacts:  ❒ Defacement of web site  ❒ Service interruption (denial of service attack / mail bomb / system failure)  ❒ Massive virus attack  ❒ Lost/damage/unauthorized alternation of information  ❒ Compromise/leakage of sensitive information  ❒ Intrusion/unauthorized access  ❒ Others, please specify: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Please provide details on the impact and service interruption period, if any: | |
| Actions Taken: | |
| Current System Status: | |
| Other Information: | |

## APPENDIX B - POST-INCIDENT REPORT

Incident Ref. No.: \_\_\_\_\_\_\_\_

**Post-Incident Report**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Department :** | |  | | |  |
|  | | | | | |
| **Reporting Officer Details** | | | | | |
| **Report Date :** | |  | | |  |
|  | | | | | |
| **Reported By** | | | | | |
|  | ***Name :*** |  | | |  |
|  | ***Designation :*** |  | | |  |
|  | ***Phone No. :*** |  | | |  |
|  | ***E-mail Addr. :*** |  | | |  |
|  | | | | | |
| **Incident Details** | | | | | |
| **Incident Date :** | |  | | |  |
|  | | | | | |
| **Type of Incident:** | | | | | |
| **System Name and Description:** | | | | | |
| **Summary of Incident:** | | | | | |
| **Event Sequence:** | | | | | |
| ***Date / Time*** | | ***Event*** | | | |
|  | |  | | | |
|  | |  | | | |
|  | |  | | | |
|  | |  | | | |
| **Action Taken and Result:** | | | | | |
| **Current System Status:** | | | | | |
| **Personnel Involved:** | | | | | |
|  | |  |  |  |  |
| ***Name*** | | ***Designation*** | ***Phone No.*** | ***E-mail Addr.*** | ***Role*** |
|  | |  |  |  |  |
|  | |  |  |  |  |
|  | |  |  |  |  |
|  | |  |  |  |  |
|  | |  |  |  |  |
| **Hacker Details (if any):** | | | | | |
| **Virus Details (if any):** | | | | | |
| **Other Affected Sites/Systems:** | | | | | |
| **Damage (including disruption/suspension of service):** | | | | | |
| **Cost Factor (including loss caused by the incident and the recovery cost/manpower):** | | | | | |
| **Recommended Action to Prevent Recurrence:** | | | | | |
| **Other Comments:** | | | | | |
| **Experience Learnt:** | | | | | |

## APPENDIX C - Departmental IT Security Contacts Change Form

|  |  |
| --- | --- |
| **Name of Department** | |
|  | |
| **Role of the Officer** | |
| * Business Assurance Co-ordinator (BD) * User Assurance Co-ordinator (BD) * IT System Support Manager * IT System Support Officer * Vendor Support Engineer | |
| The officer to be replaced: | |
| **Contact Information** | |
| Name: | Designation: |
| Office Contact: | Fax Number: |
| 24 hours Contact: | |
| Internet E-mail Address: | |
| Lotus Notes E-mail Address: | |
| Other e-mail contact for receiving IT security related information from BD LSCP Security Team: | |
| **Submission to BD LSCP IT Security Team** | |
| Signature: Date: | |
|  | |
| *Please return, by contact, the completed change form to the following party:*  *ITU*  *Buildings Department*  *Buildings Department Headquarters, North Tower, West Kowloon Government Offices, 11 Hoi Ting Road, Yau Ma Tei, Kowloon*  *()* | |

## APPENDIX D – IDENTIFICATION OF INCIDENT

TYPES OF INCIDENTS

Information security incident that is of major impact to Government services and/or image should be reported. The following table lists some of the incident types and its description:

|  |  |
| --- | --- |
| **IT Security Incident** | **Description** |
| Denial of service attack | Prevention of the use of information resources either intentionally or unintentionally, which affects the availability of the information resources. Examples of such attacks are SYN flood, Ping O death and Ping flooding, which trying to overload either the computer system or the network connection in order to disable the system from delivering the normal service to its users. |
| Email bombing | By either sending large volume of unsolicited email to a mail server with a view to launching a denial-of service type of attack to the mail server, or using the victim's system as a base to launch such attack to a third party's mail server so as to frame the victim. |
| Large scale malicious code attack | Malicious code attacks include attacks by programs such as computer viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Self-replicating malicious code such as computer viruses and worms can furthermore replicate rapidly, thereby making containment an especially difficult problem. |
| Defacement of web page | Unauthorized alteration of the content of one of more web pages of the website on Internet. |
| Eavesdropping | An illegally capturing and stealing of data, packet through network or other means of communication. |
| Compromise | A violation of a security policy in which an unauthorized disclosure or loss of sensitive information may be resulted. |
| Penetration | The successful unauthorized access to an information system. |
| Intrusion | Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. |
| Masquerading | The use of another person’s identity to gain excess privilege in accessing system. |
| Unauthorized access | Physical or logical access to whole or part of an information system and/or its data without the prior permission of the system owner. |
| Misuse | Misuse occurs when someone uses a computing system for other than the permitted purposes, e.g., when a genuine user uses a Government computer and email account to launch an email bombing attack to others. |
| Fraudulent website or email | The use of fake Government websites or spoofed emails claiming to be sent from the Government which are potentially related to fraudulent activities. Common attack techniques include *phishing*1 and *pharming*2. |
| Leaking of classified data | Classified data was exposed or accessible by unauthorized persons. |