Information Security Management System MS ISO/IEC 27001:2007

SECURITY INCIDENT MANAGEMENT PROCEDURE

PROSEDUR PENGURUSAN INSIDEN KESELAMATAN

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
Pn. Ummi Naiemah Saraih	Pn. Rohazna Wahab Deputy Director ICT	En. Nasrudin Abd. Shukor Director ICT Division ISMR

For Dept Use Only

Date: 11th October 2012 **Version 1.0**

Revision History

No	Date of Change	Description	Page	Version	Approved By

SECURITY INCIDENT MANAGEMENT PROCEDURE
PROSEDUR PENGURUSAN INSIDEN KESELAMATAN

1.0 OBJECTIVE
1.0 OBJEKTIF

Security Incident Management is an organized arrangement made to address and manage the aftermath of security breaches or security incidents.

These security incidents could range from intensive attacks from malicious hackers outside the network to internal mistakes leading to hardware failures, misconduct/ negligence of employees violating the policies of University Malaysia Perlis Information and Communication Technology Centre or wilful acts of destruction of data or IT systems functionality. A six-step incident response methodology is adopted, which includes preparation, identification, containment, eradication, recovery, and follow-up.

Pengurusan Insiden keselamatan ialah susunan perancangan yang diatur bagi menangani dan menguruskan akibat dari pelanggaran keselamatan atau insiden keselamatan.

Insiden keselamatan ini boleh berlaku dari serangan-serangan intensif dari penggodam-penggodam di luar rangkaian ke kesilapan-kesilapan dalaman yang membawa kepada kegagalan perkakasan, salah laku / kecuaian kakitangan-kakitangan yang melanggar dasar-dasar Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis atau kemusnahan yang dilakukan dengan sengaja kepada data atau fungsi sistem teknologi maklumat. Enam kaedah gerak balas diambil termasuk persediaan, pengenalpastian, pengurungan, pembasmian, pemulihan, dan lanjutan (susulan).

2.0 SCOPE
2.0 SKOP

The scope covers University Malaysia Perlis Information and Communication Technology Centre and its staff as stated in the security manual. The incident may fall under technical (IT systems related) and or Process and or People related

Skop meliputi Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis dan kakitangan-kakitangannya seperti yang dinyatakan dalam manual keselamatan. Insiden boleh jatuh di bawah teknikal (bersangkutan dengan sistem teknologi maklumat) dan atau bersangkutan Proses dan atau Manusia

3.0 PREPARATION
3.0 PERSEDIAAN

Preparation is paramount important to ensure organized and unambiguous response to a security incident. Preparation also minimizes the potential for damage since the response plan is well known and coordinated. The following steps are required to ensure sufficient preparation.

Persediaan adalah penting untuk memastikan gerak balas yang terancang dan jelas bagi insiden keselamatan. Persediaan juga mengurangkan potensi terhadap kerosakan kerana rancangan gerak balas diketahui dan diselaraskan. Langkah-langkah berikut diperlukan untuk memastikan persediaan mencukupi.

4.0 BASELINE SECURITY
4.0 GARIS DASAR KESELAMATAN

- All systems and processes must be installed with baseline protection as the first line of defensive. (See all the University Malaysia Perlis Information and Communication Technology Centre function flowchart and their relationship with ISMS in the Security Manual)
- Only the respective BU heads/ their appointed reps and IT system administrators have access and or control over the systems and networks.
- System IT administrators must ensure all suitable security countermeasures are in place and all systems are fully patched.
- IT Administrators must monitor and response to intrusion detection alerts.
- Regular backup are critical to ensure business continuity. The integrity of the backup copy must be verified to ensure successful recovery. (See Back-up Policy)

- *Semua sistem dan proses-proses mesti dilengkapkan dengan perlindungan garis dasar sebagai benteng pertahanan pertama. (Lihat semua carta aliran fungsi Pusat Teknologi Maklumat, Universiti Malaysia Perlis dan hubungan mereka dengan ISMS dalam Manual Keselamatan).*
- *Hanya Ketua-ketua Unit Perniagaan berkenaan / wakil-wakil yang dilantik oleh mereka dan pentadbir-pentadbir sistem teknologi maklumat mempunyai akses dan atau kawalan atas sistem-sistem dan jaringan-jaringan.*
- *Pentadbir-pentadbir sistem teknologi maklumat perlu memastikan semua langkah-langkah balas keselamatan yang bersesuaian di tempatkan dan semua sistem-sistem ditampal sepenuhnya.*

- *Pentadbir-pentadbir teknologi maklumat mesti memantau dan memberi gerak balas kepada amaran pengesanan pencerobohan.*
- *Penduaan (backup) yang kerap adalah kritikal untuk memastikan kesinambungan perniagaan. Integriti salinan penduaan perlu disahkan untuk memastikan pemulihan yang berjaya.*

5.0 PLANNING AND GUIDANCE
5.0 PERANCANGAN DAN BIMBINGAN

- ISMS Committee with a system of reporting Security incidents by e-mail, sending the e-mail to the BU head, and CC to ISMS committee, flow has been established. (Please refer to Security Manual Appendix 2).
- IT administrator assigned by the IT Director takes charge of all technical related incidents.
- Provision must be made in the event of the assigned system administrator is not available. Thus, all administrative passwords to obtain access to all the systems and networks must be recorded in separate sealed envelope and stored in a secure safe with the IT Director.
- Assure the appropriate tools for eradication, detection and system restoration such as malware scanner and removal tools are obtained to reduce the potential damaging delay.
- Incident response guidelines or procedures must be made available to all BU heads and concerned staff to ensure prompt reaction when unexpected incident happened. Include checklist in the procedures to indicate the proper actions that should be taken during an incident.
- Assure all personnel know the point of contacts in the event of incidents. The list of personnel to be contacted during incidents should include home, cell phones, pager, and fax numbers.

(See BU's respective BCP for this info)

- *Jawatankuasa ISMS dengan sistem melaporkan insiden-insiden keselamatan melalui e-mel, menghantar e-mel tersebut kepada ketua Unit Perniagaan dan CC kepada jawatankuasa ISMS,aliran telah ditubuhkan. (Sila rujuk Manual Keselamatan Appendix 2).*
- *Pentadbir teknologi maklumat yang ditugaskan oleh Pengarah bahagian teknologi maklumat, bertanggungjawab terhadap semua insiden-insiden berkaitan teknikal.*
- *Peruntukan mestilah dibuat semasa ketiadaan pentadbir sistem yang ditugaskan. Oleh itu, semua kata laluan pentadbiran untuk memperoleh akses kepada semua sistem-sistem dan jaringan mestilah direkodkan dalam sampul surat berlakri*

berasingan dan disimpan di dalam peti atau bekas yang selamat dengan pengarah bahagian teknologi maklumat.

- *Pastikan alat-alat yang sesuai untuk pembasmian, pengesanan dan pemulihan sistem seperti pengimbas malware dan alat-alat penyingkiran diperolehi untuk mengurangkan kelewatan yang menambahkan kerosakkan berpotensi.*
- *Garis-garis panduan gerak balas insiden atau prosedur-prosedur mesti tersedia untuk semua ketua-ketua Unit Perniagaan dan kakitangan yang berkenaan bagi memastikan reaksi segera apabila insiden berlaku di luar jangkaan. Senarai semakan dimasukkan di dalam prosedur-prosedur untuk menunjukkan tindakan-tindakan sesuai yang patut diambil semasa berlakunya sesuatu insiden.*
- *Pastikan semua kakitangan sedia maklum siapa yang perlu dihubungi jika berlaku insiden-insiden. Senarai kakitangan yang dihubungi semasa insiden merangkumi nombor telefon rumah, telefon mudah alih, kelui , dan nombor faks.*

(Untuk maklumat sila lihat Rancangan Kesinambungan Perniagaan untuk unit perniagaan masing-masing).

6.0 PROCEDURE DETAILS
6.0 BUTIR-BUTIR PROSEDUR

Description *Penerangan*	Documents / Ref. *Dokumen/Rujukan*	Personnel *Kakitangan*
➢ Incident report e-mel send to help desk. Help desk then sends it to the concern department.	- Security Incident Report e-mail	- Help desk
➢ The managers who receive the report shall verify the incident and quickly inform their BU Heads.		- BU Heads
➢ *E-mel laporan Insiden dihantar kepada help desk. Help desk kemudiannya menghantar kepada jabatan yang berkenaan.*	*- E-mel Laporan Insiden Keselamatan*	*- Help desk*
➢ *Pengurus yang menerima laporan tersebut akan mengesahkan insiden dan memaklumkan ketua-ketua unit perniagaan.*		*- Ketua-ketua Unit Perniagaan*

SECURITY INCIDENT MANAGEMENT PROCEDURE
PROSEDUR PENGURUSAN INSIDEN KESELAMATAN

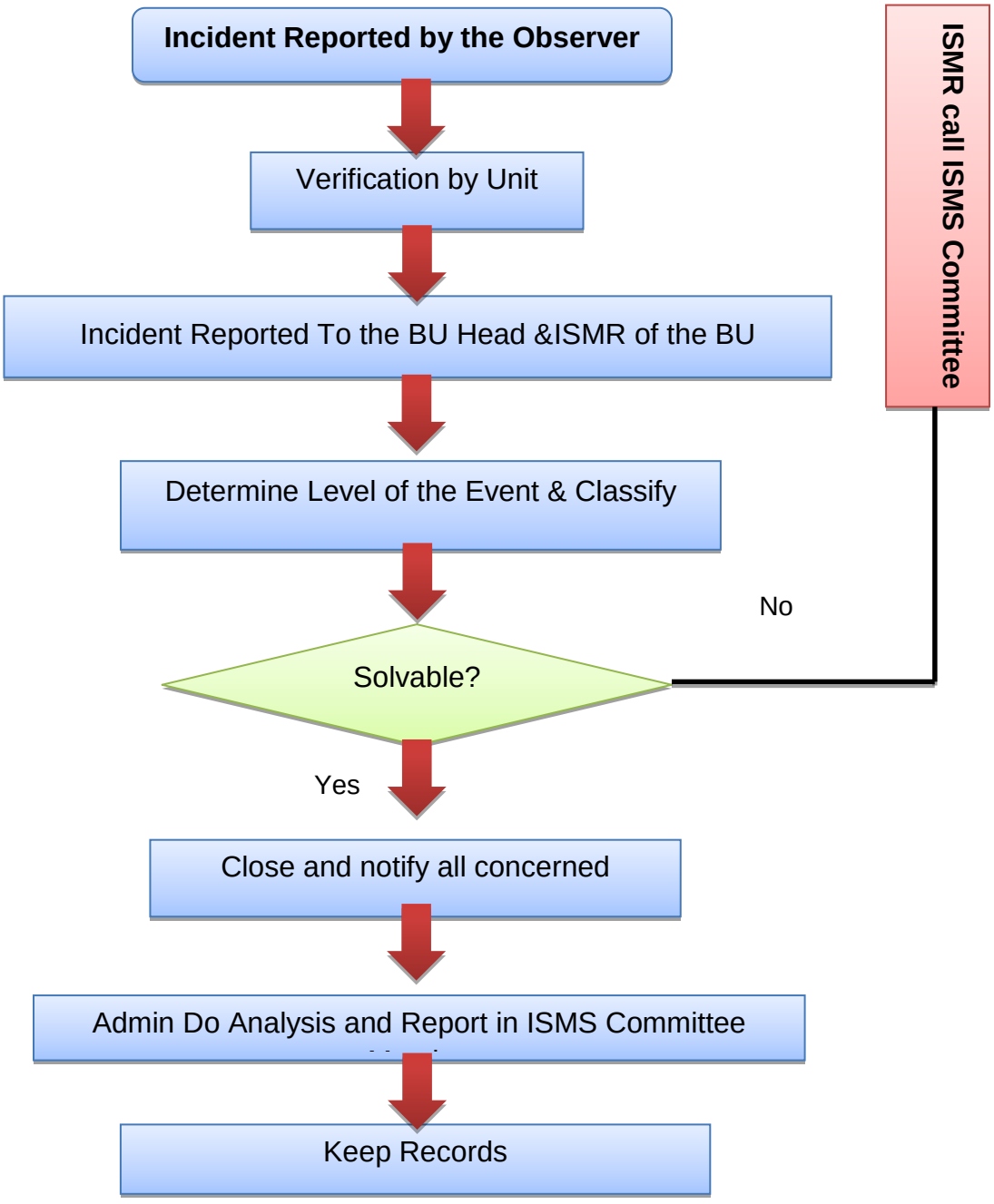
Description *Penerangan*	Documents / Ref. *Dokumen/Rujukan*	Personnel *Kakitangan*
➢ Respective BU Manager along with the ISMR shall classify the Level of the event.Incident, Emergency or Disaster.They shall then classify it as High, Medium or Low.; ➢ *Pengurus Unit Perniagaan masing-masing bersama dengan ISMR akan mengklasifikasi tahap kejadian. Insiden, Kecemasan atau Bencana. Mereka kemudiannya akan mengklasifikasikan ia kepada Tinggi, Sederhana atau Rendah;*	- Incident Management Procedure *- Prosedur Pengurusan Insiden*	- BU Head - ISMR *-Ketua Unit Perniagaan* *- ISMR*
➢ Based on the result, personnel in-charge shall evaluate the need for CA / PA / both and propose appropriate action plan to address the Event. ➢ BU Heads shall review & approve the action to be taken and instruct the person responsible to do so. ➢ The Managers of the units within the BU shall verify the closure of the event and report to the ISMR and the BU Manager. ➢ The ISMR shall verify the full chronology of the event and the action carried out and its result. ➢ The Admin Personnel shall carryout a trend analysis of incidents and measure them for presenting to the ISMS committee. **NOTE:** *If the Event/ Issue is declared as Disaster please refer to the BCP of that specific BU.* *These events does not include generic emergencies and Disasters such as Fire, Floods, epidemics, earthquakes and other similar Non-Security related events.*	- Incident Reporting form *- CA/PA Form* *- Trend Analysis Record*	- Appointed Personnel to take action. - BU Heads - ISMR -ISMR -Admin Personnel

Description ***Penerangan***	**Documents / Ref.** ***Dokumen/Rujukan***	**Personnel** ***Kakitangan***
➢ *Berdasarkan keputusan, kakitangan bertugas akan menilai keperluan CA / PA / kedua-duanya dan mencadangkan rancangan tindakan sesuai bagi menangani kejadian.* ➢ *Ketua unit perniagaan akan mengkaji semula & meluluskan tindakan yang akan diambil dan mengarahkan individu yang dipertanggungjawabkan untuk berbuat demikian.* ➢ *Pengurus-pengurus unit-unit dalam unit perniagaan akan mengesahkan penutupan kejadian dan melaporkan kepada ISMR dan Pengurus unit perniagaan.* ➢ *ISMR akan mengesahkan kronologi kejadian, tindakan yang diambil dan dilakukan dan keputusannya.* ➢ *Kakitangan Tadbir akan melakukan satu analisis trend insiden-insiden dan ukurannya untuk dikemukakan kepada jawatankuasa ISMS.* ***NOTA*** *Jika kejadian / Isu diisytiharkan sebagai Bencana, sila rujuk BCP untuk unit perniagaan tersebut. Kejadian-kejadian ini tidak termasuk kecemasan generik dan bencana-bencana seperti kebakaran, banjir, wabak, gempa bumi dan lain-lain kejadian serupa yang tidak berkaitan dengan Keselamatan.*	*- Borang Laporan Insiden* *- Borang CA/PA* *- Rekod Trend Analysis*	*- Kakitangan yang ditugaskan untuk mengambil tindakan.* *- Ketua unit perniagaan* *- ISMR* *- ISMR* *- Kakitangan Tadbir*
➢ If the event, Issue cannot be closed due to any reason, the ISMS committee shall be convened and issue discussed to find out a best possible solution. This may even require the Director to		

Description ***Penerangan***	**Documents / Ref.** ***Dokumen/Rujukan***	**Personnel** ***Kakitangan***
step in depending on the seriousness of the issue. ➢ *Sekiranya isu tidak dapat ditutup atas sebab-sebab tertentu, jawatankuasa ISMS akan dimaklumkan dan isu tersebut akan dibincangkan untuk mencari penyelesaian terbaik. Bergantung kepada keseriusan isu, penglibatan pengarah mungkin diperlukan.* ➢ Closed CA/ PA should be kept, which will be presented & discussed in the ISMS committee meeting for Continual Improvement Program. ➢ *Menutup CA / PA harus disimpan, ianya akan dibentangkan & dibincangkan dalam mesyuarat jawatankuasa ISMS untuk Program Penambahbaikan Berterusan.*	*- minutes of the committee meeting* *- minit mesyuarat jawatankuasa*	- ISMS Committee Head *- Ketua Jawatankuasa ISMS* -ISMS Commitee *-Jawatankuasa ISMS*

7.0 PROCESS FLOW

7.0 ALIRAN PROSES



8.0 TRAINING
8.0 LATIHAN

- All personnel involved in recovery must be trained on how to response to different type of incidents.
- Personnel need to engage in periodic mock incidents in which the incident response procedure is followed to ensure systematic and fast response during the course of actual incident. (Drill followed as per BCP)

- *Semua kakitangan yang terlibat dalam pemulihan mestilah dilatih tentang bagaimana untuk memberi gerak balas terhadap pelbagai jenis insiden-insiden.*
- *Kakitangan perlu terlibat dalam insiden-insiden percubaan berkala di mana prosedur gerak balas insiden diikuti untuk memastikan gerak balas yang pantas dan sistematik semasa kejadian insiden yang sebenar. (Latihan mengikut setiap BCP)*

CLASSIC FIVE (5) STEPS
LIMA (5) LANGKAH-LANGKAH KLASIK

1) Identification phase first starts with validating by the ISMR if a security incident has indeed occurred.

2) Classify the source of the Incident report with the respective BU reps. Clarify the type of incident once the incident has been confirmed.

3) Subsequently, alert the respective BU head and upon consent, inform the ISMS committee.

4) Identify the evidence and protect it if technical help is needed, seek the IT support representative of the site.

5) Last step involve logging and reporting of the incident to the ISMS committee formally by Admin Department.

1) Fasa pertama pengenalpastian dimulakan dengan pengesahan oleh ISMR jika insiden keselamatan telah terjadi.

2) Mengklasifikasikan sumber laporan Insiden dengan wakil-wakil unit perniagaan berkenaan. Menjelaskan jenis insiden sebaik sahaja insiden telah disahkan.

3) *Kemudian, beri amaran kepada ketua unit perniagaan berkenaan dan atas persetujuan, maklumkan jawatankuasa ISMS.*

4) *Bukti dikenal pasti dan dilindungi jika bantuan teknikal diperlukan, cari wakil sokongan IT di kawasan.*

5) *Langkah terakhir melibatkan log dan melaporkan insiden secara rasmi oleh jabatan tadbir kepada jawatankuasa ISMS.*

9.0 DETERMINE THE SYMPTOM IF INFORMATION SYSTEMS RELATED
9.0 MENENTUKAN GEJALA JIKA BERKAITAN SISTEM MAKLUMAT

Determine the type of symptoms or indication that is indicative to an incident, which requires further attention. Typical computer incident symptoms include system crash, anomaly usages, suspicious system logs and intrusion detection alerts.

Observe one of more symptoms to conclusively validate an incident.

Tentukan jenis gejala-gejala atau petunjuk yang menjurus kepada insiden, yang memerlukan perhatian selanjutnya. Gejala-gejala insiden komputer tipikal termasuk keruntuhan sistem, penggunaan-penggunaan anomali, log sistem mencurigakan dan amaran pengesanan pencerobohan.

Perhatikan satu atau lebih gejala untuk mengesahkan dengan pasti sesuatu insiden.

10.0 CLASSIFYTHE TYPEOF SECURITY INCIDENT
10.0 MENGKLASIFIKASIKAN JENIS INSIDEN KESELAMATAN

- System administrators works with BU head of IT and IT networks, IT support personnel to classify the type of incident.
- Associate each incident with an incident severity level to help establish a priority when addressing the incident.

- *Pentadbir-pentadbir sistem bekerjasama dengan ketua unit perniagaan teknologi maklumat dan jaringan-jaringan teknologi maklumat, kakitangan sokongan teknologi maklumat untuk mengklasifikasikan jenis insiden.*
- *Mengaitkan setiap kejadian dengan tahap keseriusan insiden bagi membantu untuk membentuk keutamaan apabila menangani insiden.*

Incident Security Level
Tahap/Peringkat Keselamatan Insiden

High ► Potential to become a disaster covering entire services of University Malaysia Perlis Information and Communication Technology Centre

Medium ► Potential to become an emergency, less than 2 -3 hours.

Low ► Not a serious event, effect minimal (SLA not breached) on critical business processes and can be rectified within 1 hour.

Tinggi ► *Berpotensi untuk menjadi bencana merangkumi seluruh perkhidmatan-perkhidmatan Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis*

Sederhana ► *Berpotensi untuk menjadi kecemasan, kurang daripada 2-3 jam.*

Rendah ► *Bukan kejadian yang serius, kesan minimal (tiada pelanggaran Perjanjian Tahap Perkhidmatan (SLA) ke atas proses kritikal perniagaan dan boleh diperbaiki dalam 1 jam.*

11.0 IDENTIFYING AND PROTECTING THE EVIDENCE
11.0 MENGENAL PASTI DAN MELINDUNGI BUKTI

- Make a full backup of the system with suspicious events or evidence once a security incident has been declared to avoid attacker destroying the evidence.
- Preserve the chain of custody for all evidence at all time.
- Every evidential items or data that is collected should be signed off, time-stamped and comprehensively documented as to who handles the evidence and the location the evidence is stored.
- Preserve the evidence integrity by storing the evidence in tamper-proof media and secure safe. Assure evidence integrity through cryptographic checksum or hash.
- Other relevant information including application logs, firewall logs, intrusion detection logs and CCTV tapes (e.g. physical breach) that provides correlating evidence about the intrusion must be preserved.

- *Membuat sandaran/penduaan penuh sistem-sistem dengan kejadian-kejadian mencurigakan atau bukti sebaik sahaja insiden keselamatan telah diisytiharkan untuk mengelak penyerang dari merosakkan bukti.*

- *Mengekalkan rangkaian jagaan untuk semua bukti setiap masa.*
- *Setiap barang-barang bukti atau data yang dikumpul harus diperakui, ditandakan dengan masa dan didokumenkan secara menyeluruh seperti siapa yang mengendalikan bukti dan lokasi simpanan bukti tersebut.*
- *Mengekalkan integriti bukti dengan menyimpan bukti dalam media yang kalis ubah dan peti atau bekas yang selamat. Pastikan integriti bukti melalui hasil tambah semak kriptografi atau hash.*
- *Maklumat lain yang berkaitan termasuk log-log aplikasi, log-log firewall, log-log pengesanan penembusan dan pita-pita CCTV (contoh: pelanggaran fizikal) yang memberi bukti mengaitkan pencerobohan mesti dikekalkan dan dijaga.*

12.0 CONTAINMENT
12.0 PENGEPUNGAN

The organization primary objective of containment is to limit the scope and magnitudes of attack/impact to ensure business continuity, instead of allowing the incident to continue to gather sufficient evidence to prosecute the attackers.

Objektif utama organisasi bagi pengepungan ialah untuk menghadkan skop dan magnitud serangan/ impak bagi memastikan kesinambungan perniagaan, daripada membiarkan insiden berterusan untuk mengumpul cukup bukti yang membolehkan penyerang-penyerang didakwa.

13.0 DETERMINE OPERATIONAL STATUS
13.0 STATUS OPERASI DITENTUKAN

- Determine operational status of the critical computing services or sensitive data. Possible actions include leaves them unchanged, take them offline or move critical services to other networks which suffer less interruption.
- Determine operational status of the compromised system or networks. Depending on the risk factors of the incident, possible actions includes isolating the affected system by disconnect it from the network, disable the affected service or allowed the system to run as usual under close monitoring.
- Document the incident response

- *Tentukan status operasi perkhidmatan-perkhidmatan pengkomputeran kritikal atau data sensitif. Tindakan-tindakan yang mungkin dilakukan termasuk meninggalkannya tanpa diubah, dibawa ke luar talian atau pindahkan perkhidmatan-perkhidmatan kritikal kepada rangkaian-rangkaian lain yang mengalami sedikit gangguan.*
- *Tentukan status operasi sistem-sistem atau jaringan-jaringan yang dikompromi. Bergantung atas faktor risiko insiden tersebut, tindakan-tindakan yang mungkin dilakukan termasuk mengasingkan sistem yang terjejas dengan memutuskannya dari rangkaian, melumpuhkan perkhidmatan terjejas atau membenarkan sistem berjalan seperti biasa di bawah pengawasan rapi.*
- *Gerak balas insiden didokumentasikan.*

14.0 ADDITIONAL CONTAINMENT STEPS
14.0 LANGKAH-LANGKAH PENGEPUNGAN TAMBAHAN

- Ensure the affected system is fully backup to retain the evidence.
- Avoid tipping off the attacker to reduce further system or evidence damages if still happening.
- Avoid logging in as administrative user on the compromised system to avoid the spreading of malicious codes.
- Change all the passwords on the affected systems, including passwords on other systems that once interact with the compromised system.

- *Memastikan sandaran/penduaan sistem yang terjejas telah dilakukan sepenuhnya untuk membendung bukti.*
- *Elakkan dari memberi maklumat kepada penyerang untuk mengurangkan kerosakkan yang lebih lanjut kepada sistem atau bukti jika masih terjadi.*
- *Elakkan dari pengelogan masuk sistem yang dikompromi sebagai pengguna tadbir untuk mengelakkan penyebaran kod-kod perosak.*
- *Menukar semua kata laluan sistem-sitem yang terjejas, termasuk kata laluan sistem-sistem lain yang pernah berinteraksi dengan sistem yang dikompromi.*

15.0 ERADICATION
15.0 PEMBASMIAN

Once the incident is contained, eradication is required to remove the cause of the security incident to resume business operation.

Sebaik saja insiden dikepung, pembasmian diperlukan untuk menghapuskan penyebab insiden keselamatan bagi meneruskan operasi perniagaan.

16.0 DETERMINE THE CAUSE AND ROOT CAUSE
16.0 MENENTUKAN SEBAB DAN PUNCA SEBAB

- Before eradicating the affected system, gather sufficient information about the affected system and the cause of incident, as such information may be lost after the eradication process.
- If the affected system were taken offline, acquire bit-level images on the affected system to secure all possible evidence and to perform comprehensive forensic analysis on the security incident. The integrity of the image must be preserved if prosecution is required.

- *Sebelum pembasmian sistem yang terjejas dilakukan, kumpulkan maklumat secukupnya tentang sistem yang terjejas dan penyebab insiden, kerana kemungkinan maklumat hilang selepas proses pembasmian.*
- *Jika sistem yang terjejas diambil luar talian, dapatkan imej-imej bit-level di sistem yang terjejas untuk memperolehi semua bukti yang mungkin dan untuk melakukan analisis forensik yang komprehensif ke atas insiden keselamatan. Integriti imej mesti dikekalkan jika pendakwaan diperlukan.*

17.0 RECOVERY
17.0 PEMULIHARAAN

Recovery is aim to restore the system to a secured and fully operational condition.

Pemuliharaan bertujuan untuk mengembalikan sistem kepada keadaan yang selamat dan beroperasi sepenuhnya.

18.0 FINALIZE INVESTIGATIVE ACTIVITY
18.0 MENYELESAIKAN AKTIVITI SIASATAN

Since recovery process will destroy all possible evidence, complete any investigative activities before proceeding with restoration.

Memandangkan proses pemuliharaan akan memusnahkan semua bukti yang mungkin, selesaikan sebarang aktiviti siasatan sebelum membaik pulih dimulakan.

19.0 RESTORE THE SYSTEM
19.0 MENGEMBALIKAN SISTEM

- Depending on the severity of the incident and eradication methods, recovery may include restoring the system from a clean backup or restoring the system from scratch.
- Verify the integrity of the backup copies and ensure they are uncontaminated.
- Tighten the network perimeter security and perform system hardening if applicable.

- *Bergantung kepada keseriusan insiden dan kaedah-kaedah pembasmian, pemuliharaan boleh termasuk mengembalikan sistem dari sandaran/penduaan yang tidak tercemar atau mengembalikan sistem dari mula.*
- *Mengesahkan integriti salinan-salinan penduaan dan pastikan ianya tidak tercemar.*
- *Ketatkan keselamatan sempadan rangkaian dan melakukan pengukuhan sistem jika berkenaan.*

20.0 VALIDATE THE SYSTEM
20.0 MENGESAHKAN SISTEM

- Verify the success of system restoration to ensure fully operational system.
- *Mengesahkan kejayaan pemuliharaan sistem bagi memastikan sistem beroperasi sepenuhnya.*

21.0 FOLLOW-UP
21.0 SUSULAN/LANJUTAN

The final stage, follow-up is necessary to improve the incident response procedures to maintain effective incident handling in future.

Peringkat terakhir, susulan/lanjutan adalah perlu bagi meningkatkan prosedur-prosedur gerak balas insiden untuk mengekalkan pengendalian insiden yang berkesan dimasa hadapan.

22.0 DOCUMENT INSIDEN RESPONSE QUALITY
22.0 KUALITI GERAK BALAS INSIDEN DIDOKUMENKAN

- Perform assessment on how well the involved personnel response to the incident and obtain feedback from the personnel.
- Identify areas in incident response that required improvement.

- *Jalankan penilaian tentang bagaimana cekapnya gerak balas kakitangan terlibat kepada insiden tersebut dan dapatkan maklum balas dari kakitangan.*
- *Kenal pasti perkara-perkara dalam gerak balas insiden yang memerlukan peningkatan.*

23.0 DETERMINE INCIDENT COSTS
23.0 TENTUKAN KOS-KOS INSIDEN

- Determine the cost of the incident which includes personnel, irrecoverable data and equipments. Financial cost can be useful in prosecution or as a justification for future security investment. (Done by Admin Staff)

- *Tentukan kos insiden yang termasuk kakitangan, data yang tidak dapat diselamatkan dan peralatan-peralatan. Kos-kos kewangan mungkin berguna dalam pendakwaan atau sebagai justifikasi untuk pelaburan keselamatan masa hadapan.(Dilakukan oleh kakitangan tadbir)*

24.0 PREPARING REPORT
24.0 PENYEDIAAN LAPORAN

- Prepare a report which includes a description on the incident, actions taken, and the above associated cost analysis. The report can be used as future reference or to increase personnel awareness.

- *Sediakan satu laporan yang merangkumi satu gambaran mengenai insiden, tindakan yang diambil, dan analisis kos yang berkaitan. Laporan itu boleh digunakan sebagai rujukan masa depan atau meningkatkan kesedaran kakitangan.*

25.0 REVISING POLICIES AND PROCEDURES, AND SECURITY COUNTER MEASURE
25.0 MENYEMAK & MENGUBAH DASAR-DASAR DAN PROSEDUR-PROSEDUR, DAN LANGKAH BALAS KESELAMATAN

- In view of the lesson learned from the incident, review/ revise existing policies and procedures, and security countermeasures and make necessary changes for better future incident handling.

- *Merujuk kepada pengajaran dari insiden, semak semula/ubah dasar-dasar dan prosedur-prosedur sedia ada, dan langkah-langkah balas keselamatan dan membuat perubahan yang perlu untuk pengendalian insiden yang lebih baik dimasa hadapan.*

26.0 WORKING WITH LAW ENFORCEMENT
26.0 KERJASAMA DENGAN PIHAK BERKUASA

- If the security incident results in official investigation, the organization is required to support the legal requests and law enforcement. Organization may need to provide the requested logs, reports and incident details and assure the integrity of this information as they may be used as evidence.

- *Jika insiden keselamatan mengakibatkan siasatan rasmi, organisasi diperlukan untuk menyokong permintaan-permintaan perundangan dan penguatkuasaan undang-undang. Organisasi mungkin dikehendaki untuk menyediakan log-log yang diminta, butiran laporan-laporan dan insiden dan memastikan integriti maklumat tersebut kerana ianya mungkin boleh digunakan sebagai bukti.*

27.0 DISCIPLINARY PROCESS
27.0 PROSES DISIPLIN

There is a formal disciplinary process within University Malaysia Perlis Information and Communication Technology Centre, approved by responsible management, for University Malaysia Perlis Information and Communication Technology Centre staff who have intentionally violated the University Malaysia Perlis Information and Communication Technology Centre security policy, standards and/or procedure.

In the event of a breach of the Security Policy responsible managers of respective units within BU's and the ICT Director in cooperation with HRM within the organization, may take disciplinary action.

The ISMS committee shall be involved as per the incident management procedure. Such action may vary from a verbal warning (with or without a note on the personal file) up to and including termination. The severity of the incident shall govern the severity of the action taken.

Please refer to HR Department for further details.

Terdapat satu proses disiplin formal dalam Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis, diluluskan oleh pengurusan yang dipertanggungjawabkan, untuk kakitangan Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis yang telah dengan sengaja melanggar dasar, piawaian dan/atau prosedur keselamatan Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis.

Sekiranya berlaku pelanggaran Dasar Keselamatan pengurus-pengurus yang dipertanggungjawabkan untuk unit masing-masing di dalam Unit Perniagaan dan Pengarah ICT dengan kerjasama dengan Pengurusan Sumber Manusia dalam organisasi, boleh mengambil tindakan disiplin.

Jawatankuasa ISMS akan terlibat seperti yang dinyatakan dalam prosedur pengurusan insiden. Pelbagai tindakan boleh diambil samada berbentuk amaran lisan (dengan atau tanpa notis dalam fail peribadi) sehingga pemberhentian. Keseriusan insiden akan menentukan keseriusan tindakan yang akan diambil.

Untuk maklumat lanjut sila rujuk Jabatan Sumber Manusia.