PENGURUSAN INSIDEN KESELAMATAN ICT
&
GP MENGURUS ADUAN SALAH LAKU ICT DI PTJ

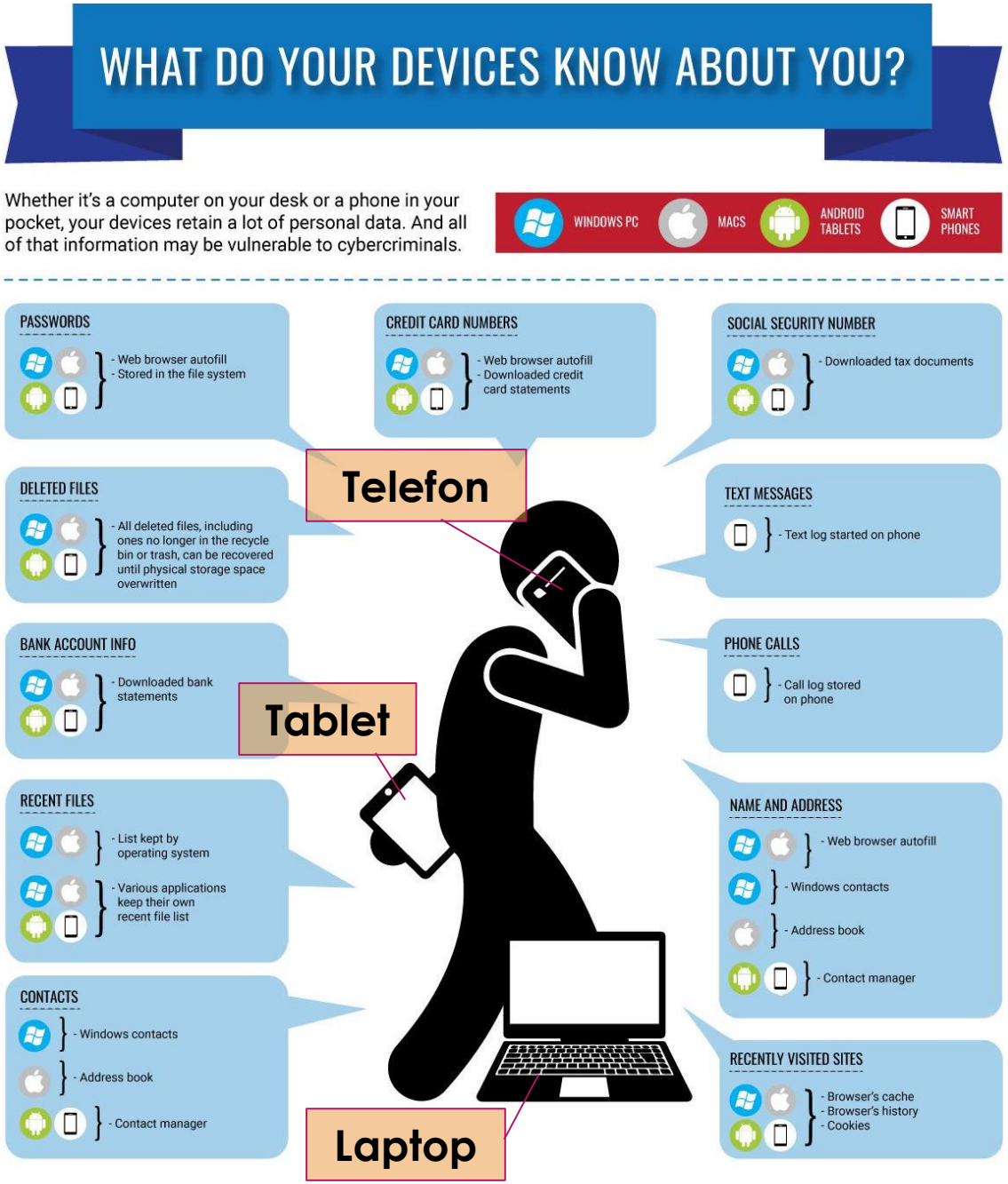
TAKLIMAT KESELAMATAN ICT SIRI 1

Encik Shamsul Abdullah Thani, ICTSO UKM

Isi Kandungan

1. Ancaman Keselamatan ICT
2. Statistik Ancaman Keselamatan ICT
3. Menangani Ancaman Keselamatan ICT

Ancaman Keselamatan ICT



Jenis ancaman :

1. Emel Phishing
2. Denial of Services (DOS)
3. Botnet
4. Man-In-The-Middle
5. Social Engineering
6. Ransomeware

Ransomeware

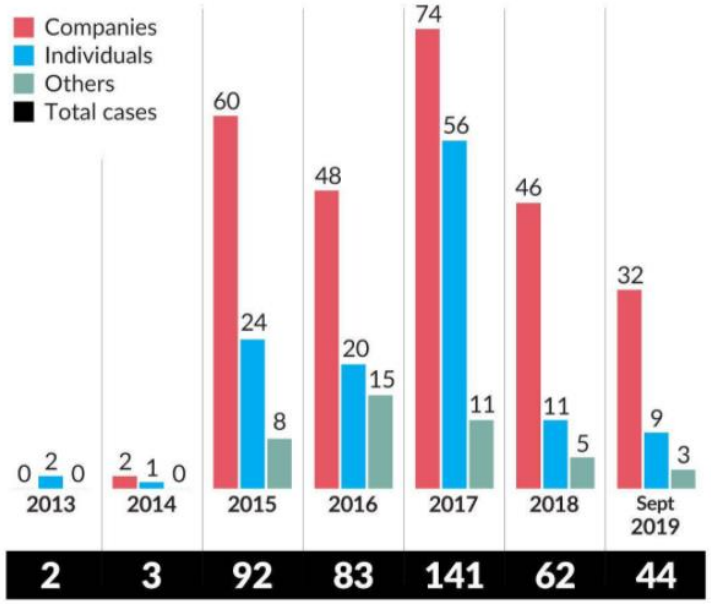
Bits and bytes about ransomware

Ransomware is a type of malware that blocks users from accessing computer systems and files.

A ransom is demanded by cybercriminals before they allow users to regain access.

The ransom is usually in e-currency such as Bitcoin. Currently, 1 Bitcoin is around RM33,500. For example, some ransomware may demand for 1.7 Bitcoin for a single machine.

Ransomware cases in Malaysia



https://www.thestar.com.my/news/nation/2019/09/29/warning-against-ransomware-attacks

Statistik Pengendalian Insiden : MYCERT

Berdasarkan kepada laporan statistik kes jenayah siber dalam tahun 2020 yang dikeluarkan oleh pihak Siber Sekuriti Malaysia, sebanyak **10, 790** insiden keselamatan siber dicatatkan.

Jumlah itu adalah sedikit lebih tinggi bagi tempoh yang sama berbanding tahun 2019 di mana hanya sebanyak **10,772** kes sahaja dicatatkan. Peningkatan sebanyak 18 kes.

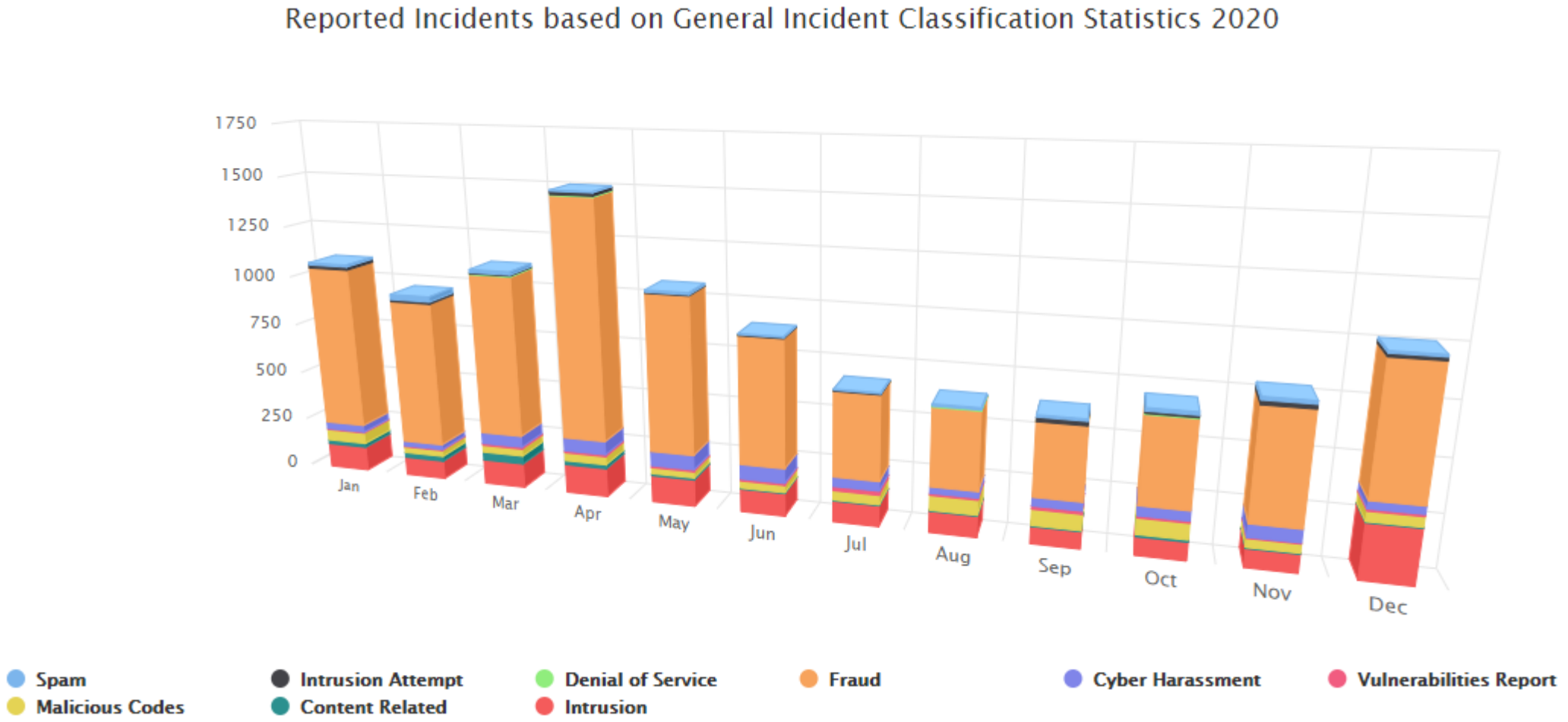
Daripada keseluruhan kes jenayah siber bagi tempoh itu, insiden yang melibatkan **kes penipuan** adalah paling tinggi dengan mencatatkan sebanyak **7,593 kes** atau bersamaan dengan **70%** dari keseluruhan kes.

Diikuti oleh **kes pencerobohan** yang mencatatkan 1,444 insiden dan insiden **jenayah gangguan siber** dengan 596 kes.

Selain itu, laporan yang melibatkan **kes jenayah pengkodan jahat** juga merekodkan sebanyak 593 kes.

Rujukan: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=0d39dd96-835b-44c7-b710-139e560f6ae0

Statistik insiden keselamatan tahun 2020 - MYCERT



Statistik insiden keselamatan tahun 2020 - MYCERT

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	11	27	14	8	13	8	6	7	8	16	16	11	145
Intrusion Attempt	13	8	8	11	4	1	2	4	20	14	17	14	116
Denial of Service	0	1	3	7	1	0	0	1	0	2	1	0	16
1 Fraud	807	725	798	1,180	770	626	413	378	351	411	526	608	7,593
Cyber Harassment	37	27	58	65	73	69	48	32	40	50	60	37	596
Vulnerabilities Report	5	7	10	10	7	11	18	9	18	10	5	7	117
3 Malicious Codes	56	32	33	40	35	36	47	72	76	75	40	51	593
Content Related	23	23	42	23	9	7	7	6	7	11	7	5	170
2 Intrusion	122	93	125	144	133	113	101	102	81	87	88	255	1,444
	1,074	943	1,091	1,488	1,045	871	642	611	601	676	760	988	10,790

Cyber attacks - Malaysia

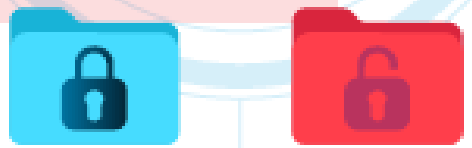
List of Recent Major Data Breaches and Cyber Incidents in Malaysia

1 astro

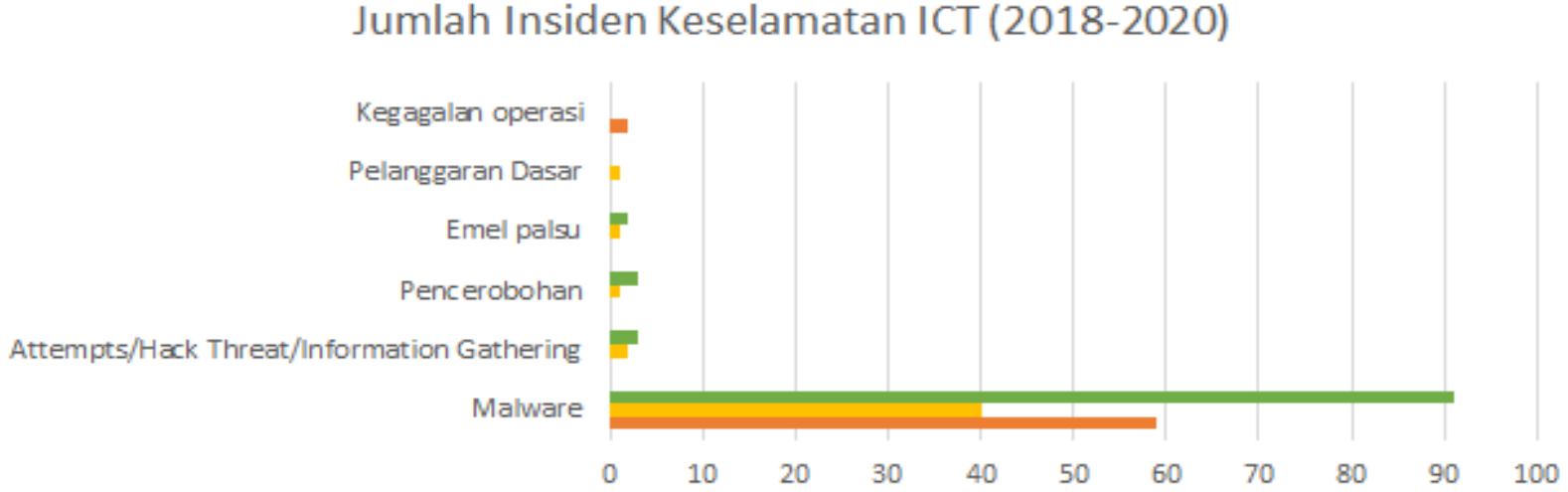
In 2018, Astro's IPTV Customer Database was put up for sale online affecting personal details of over 60,000 of its customers. While the incident was investigated, there were no further developments to it that we were made aware of.

2 media prima

In November 2018, Media Prima became a victim of a ransomware attack which disrupted most of its in-house digital services such as email correspondence. However, the amount of data or financial losses suffered was not revealed to the public.



Statistik Insiden keselamatan: UKM



	Malware	Attempts/Hack Threat/Information Gathering	Pencerobohan	Emel palsu	Pelanggaran Dasar	Kegagalan operasi
2020	91	3	3	2	0	0
2019	40	2	1	1	1	0
2018	59	0	0	0	0	2

Menangani ancaman keselamatan ICT - UKM

1. Dasar Keselamatan ICT UKM
2. Pelaksanaan ISMS UKM
3. Mewujudkan Dokumen atau Prosedur yang berkaitan
4. Peranan UKMCERT

Dasar Keselamatan ICT -DKICT

MENANGANI ANCAMAN KESELAMATAN ICT - UKM

DASAR KESELAMATAN ICT

DKICT

Muatturun dari:
>> Laman Web UKM : https://portalewarga.ukm.my/
>> Laman Web PTM : https://ptm.ukm.my/

DASAR KESELAMATAN ICT

DKICT

- Memelihara kerahsiaaan dan keselamatan maklumat UKM
- Memelihara hak dan had capaian yang diberikan ke atas sistem dan rangkaian
- Mematuhi kawalan keselamatan fizikal
- Pematuhan terhadap Dasar , Peraturan dan Undang-undang
- Memelihara dan melindungi aset ICT UKM
- Melaporkan insiden dan kelemahan keselamatan maklumat

Pelanggaran Dasar Keselamatan ICT

Sebarang **penggunaan aset ICT** selain daripada maksud dan tujuan yang telah ditetapkan di dalam Dasar Keselamatan ICT seperti **pencerobohan dan kecurian maklumat**, adalah merupakan satu pelanggaran Dasar dan akan dikenakan tindakan undang-undang dan tatatertib.

Malah boleh **dihalang atau digantung** daripada menggunakan atau mendapatkan **kemudahan ICT** yang disediakan

Pelanggaran Dasar Keselamatan ICT -Tindakan

- **Pelajar**
  - Pelajar yang melanggar dasar ini boleh dikenakan tindakan tatatertib di bawah **Akta Universiti dan Kolej Universiti 1971** Kaedah-Kaedah Universiti Kebangsaan Malaysia (Tatatertib Pelajar–Pelajar) 1999 [P.U.(A)209/1999];
- **Kakitangan UKM**
  - Kakitangan berstatus tetap Universiti boleh dikenakan tindakan tatatertib di bawah **Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605)** atau mana-mana peruntukan undang-undang yang berkaitan.
  - Kakitangan berstatus kontrak, sementara dan sambilan pula boleh dikenakan tindakan sewajarnya termasuklah ditamatkan perkhidmatan.

***kes yang diputuskan oleh Pengurusan Universiti jika perlu dilaporkan kepada pihak berkuasa**

Pelaksanaan ISMS di UKM

MENANGANI ANCAMAN KESELAMATAN ICT - UKM

Objektif pelaksanaan Keselamatan Maklumat (ISMS) UKM

1. **Menyediakan satu pendekatan yang teratur** dan **sistematik** dalam menilai risiko dan mengawal keselamatan maklumat universiti dari segi kerahsiaan, integriti dan kebolehsediaan
2. **Mengenal pasti ancaman dan risiko** yang wujud di dalam persekitaran ICT serta meningkatkan tahap keselamatan maklumat universiti
3. **Memberi jaminan dan meningkatkan keyakinan** kepada pelanggan dan pihak berkepentingan mengenai tahap keselamatan maklumat universiti

Komponen utama dalam keselamatan maklumat

MEMELIHARA

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
C	I	A
Maklumat tidak didedahkan sewenangnya atau dibiarkan diakses tanpa kebenaran	sentiasa lengkap, tepat dan terkemaskini	sentiasa boleh diakses pada bila-bila masa oleh pengguna yang sah sahaja

MAKLUMAT

Dokumen atau Prosedur yang berkaitan

MENANGANI ANCAMAN KESELAMATAN ICT - UKM

Dokumen yang diwartakan dalam UKM

Prosedur Kerja Pengurusan Insiden Keselamatan ICT UKM-ISMS-PK04

Garis panduan Mengurus Aduan Salah Laku ICT di PTJ UKM-ISMS-GP04

UKM-ISMS-PK04

PENGURUSAN INSIDEN KESELAMATAN ICT

PENGURUSAN INSIDEN KESELAMATAN ICT

UKM-ISMS-PK04

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

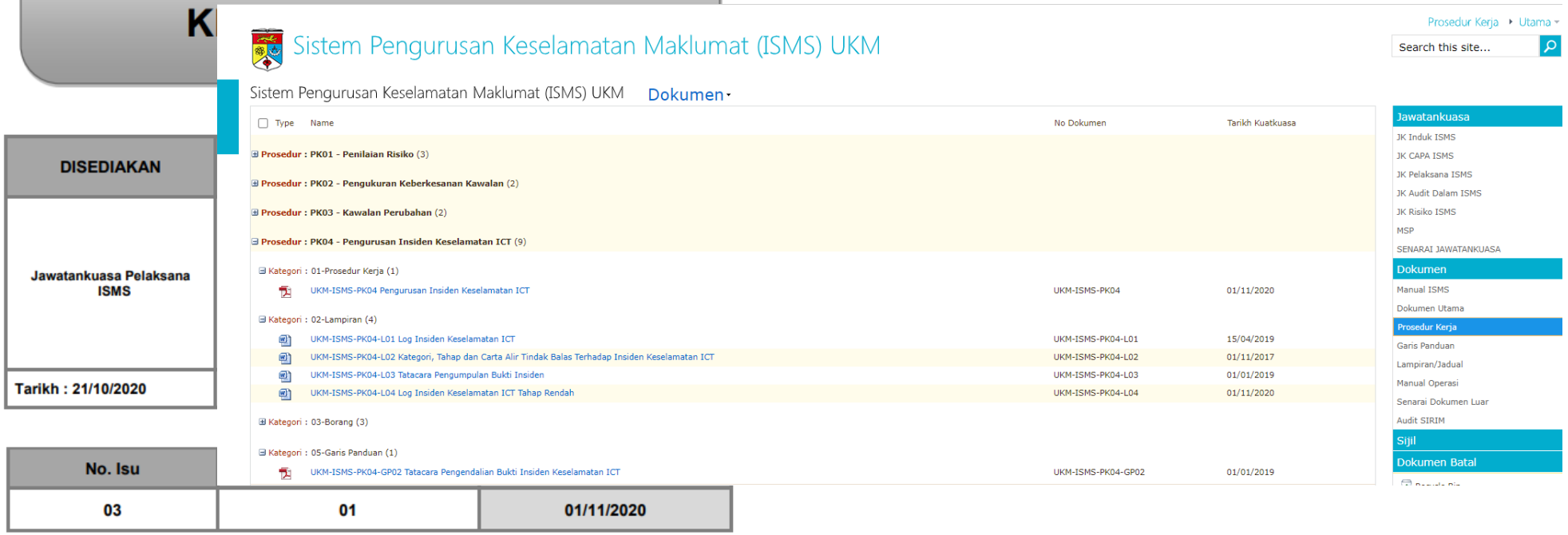
PROSEDUR KERJA

PENGURUSAN INSIDEN K

DISEDIAKAN
Jawatankuasa Pelaksana ISMS
Tarikh : 21/10/2020

No. Isu		
03	01	01/11/2020

Muatturun dari:
>> SPDUKM: https://spdukm.ukm.my/spk/isms/



Takrifan Insiden Keselamatan ICT

Situasi apabila berlakunya **pelanggaran Dasar Keselamatan Teknologi Maklumat** dan Komunikasi (ICT) UKM, kegagalan kawalan atau isu keselamatan lain melibatkan sistem dan rangkaian yang boleh **menjejaskan operasi perkhidmatan atau mengancam keselamatan maklumat**.

Tujuan Pelaporan

- Mendapatkan **maklumat** bagi UKMCERT **menyediakan bantuan teknikal** dalam pengendalian insiden keselamatan ICT;
- Meningkatkan **KEMAHIRAN** dalam pengendalian insiden;
- Membantu pengumpulan dan **PENJANAAN** statistik keselamatan ICT dalam UKM;
- Meningkatkan **KESEDARAN** dan pengetahuan mengenai keselamatan ICT; dan
- Memupuk **KERJASAMA** dan **HUBUNGAN BAIK** antara agensi

Jenis INSIDEN

Bil	Jenis	Penerangan
1	**Pelanggaran Dasar (Violation of Policy)**	Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT.
2	**Penghalangan Penyampaian Perkhidmatan (Denial of Service)**	Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk denial of service (DoS), distributed denial of service (DDoS) dan sabotage.
3	**Pencerobohan (Intrusion)**	Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (system tampering), pindaan data (modification of data) dan pindaan kepada konfigurasi sistem.

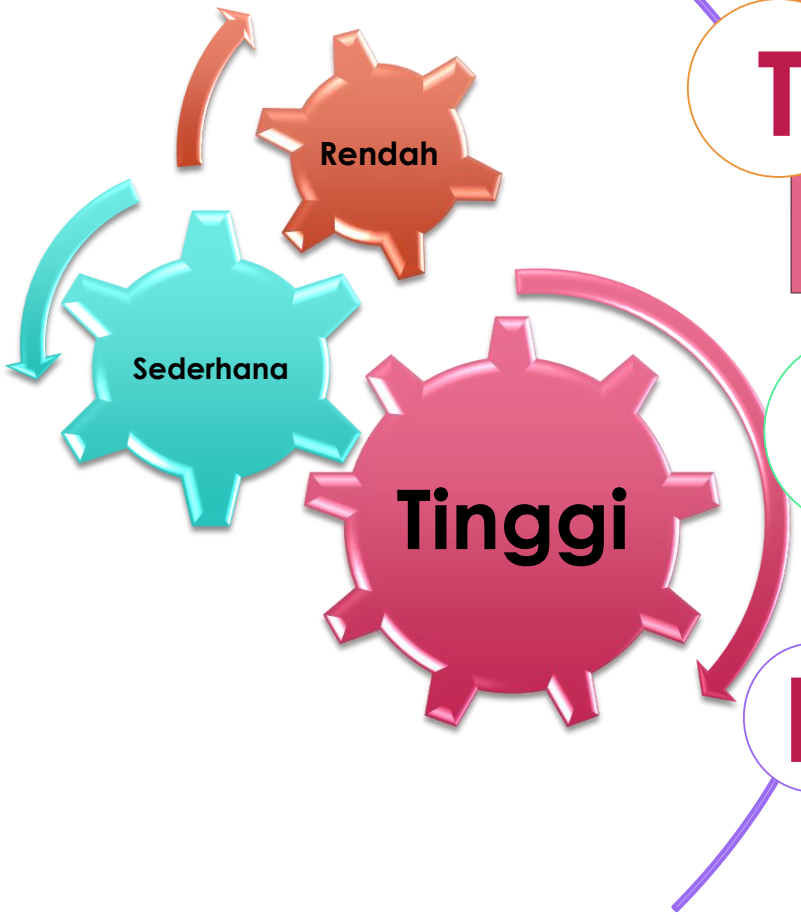
Jenis INSIDEN

Bil	Jenis	Penerangan
4	**Pemalsuan (Forgery)**	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage) dan penipuan (hoaxes).
5	**Spam**	Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.
6	**Malicious Code**	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
7	**Harrassment/Threats**	Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.

Jenis INSIDEN

Bil	Jenis	Penerangan
8	**Attempts/Hack Threats/Information Gathering**	Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk spoofing, phishing, probing, war driving dan scanning.
9	**Kehilangan Fizikal (Physical Loss)**	Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT 'Hak milik UKM'.
10	**Kecuaian atau Kemalangan**	Sebarang insiden yang menjejaskan perkhidmatan maklumat disebabkan oleh kecuaian atau kemalangan tanpa sengaja.
11	**Kegagalan Operasi**	Kegagalan sistem dan rangkaian yang menyebabkan kehilangan capaian dan perkhidmatan atau keraguan pada data/output sistem aplikasi. (pengujian, komponen, data, capaian)

Tahap INSIDEN



	Penerangan	Tanggungjawab Tindakan
T	-Insiden yang memberi **impak yang besar** kepada operasi kritikal, kerosakan kepada peralatan atau kecederaan. -Insiden menyebabkan **perkhidmatan universiti tergendala,** menjejaskan, reputasi universiti dan melibatkan perundangan.	•Pengarah PTM •UKMCERT (koordinasi) **•PKP (kesinambungan perkhidmatan)** •Pegawai yang terlibat dengan insiden
S	-Insiden berimpak sederhana yang memerlukan **siasatan lanjut** dan memerlukan tindakan **UKMCERT** dan petugas **teknikal**. -Insiden yang tidak menjejaskan keseluruhan perkhidmatan, reputasi universiti atau melibatkan perundangan.	**•UKMCERT (koordinasi)** •Pegawai yang terlibat dengan insiden
R	-Insiden yang memberi impak rendah kepada operasi sistem dan memerlukan tindakan penyelesaian dan pemantauan yang minima. -Insiden yang boleh **diselesaikan dengan kadar segera**.	**•Unit helpdesk PTM** •Pegawai yang terlibat dengan insiden

Tindakan Balas terhadap Insiden

- **Tindakan awal:** tindakan segera yang dilaksanakan untuk mengurangkan impak insiden atau menghalang sesuatu ancaman daripada terus berlaku.
- **Tindakan pemulihan:** tindakan untuk memulihkan operasi yang terjejas disebabkan insiden yang berlaku.
- **Tindakan pengukuhan**: Tindakan yang dilaksanakan adalah untuk mengatasi semua kelemahan keselamatan *(vulnerabilties)* yang berkaitan atau menambahbaik polisi atau prosedur sedia ada bagi mengelak atau mencegah ancaman yang sama berlaku.

Tindakan oleh: Petugas Teknikal

Tatacara Pengendalian Bukti Insiden

4 Proses Utama:

- pengenalpastian (*identification*)
- pengumpulan (*collection*)
- pemerolehan (*acquisition*)
- pemeliharaan (*preservation*)

Tindakan oleh: Petugas Teknikal

Tatacara Pengendalian Bukti Insiden

1) Pengenalpastian (*identification*)

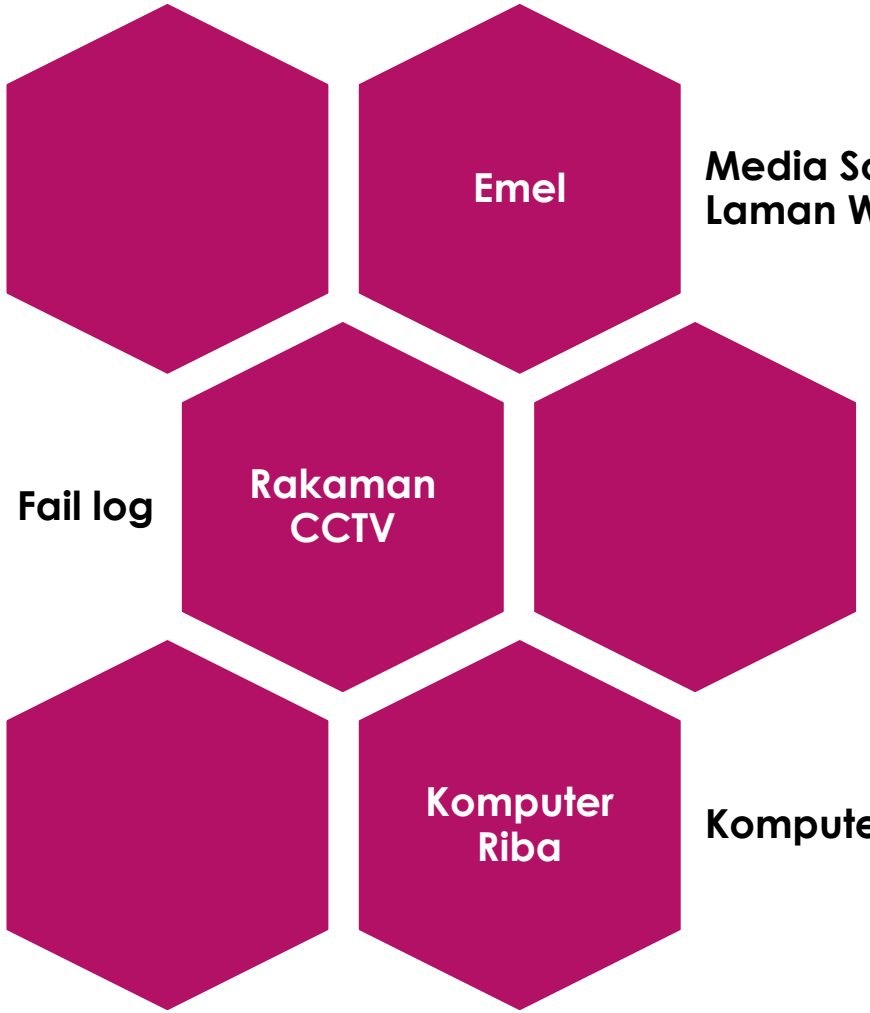
WHAT	Apakah jenis insiden yang berlaku? Apakah sumber yang diperlukan? Apakah dokumen yang diperlukan? Apakah alamat IP yang terlibat?
WHO	Siapakah individu yang terlibat? Siapakah pegawai IT yang terdapat di lokasi? Siapakah pemilik IP atau perkakasan?
WHERE	Di mana insiden berlaku? Di mana lokasi server yang terlibat?
WHEN	Bilakah insiden berlaku? Bilakah insiden mula dikenalpasti?
HOW	Bagaimana insiden berlaku?

Tindakan oleh: Petugas Teknikal

Tatacara Pengendalian Bukti Insiden

2) Pengumpulan (*collection*)

Rujuk UKM-ISMS-PK04-L03: Tatacara Pengumpulan Bukti Insiden



Tindakan oleh: Petugas Teknikal

Tatacara Pengendalian Bukti Insiden

3) Pemerolehan (acquisition)

Imej bukti yang diperoleh terdiri daripada:

- **Imej Fizikal**

  Imej fizikal merupakan imej lengkap bagi keseluruhan kandungan peranti storan yang dikenali sebagai salinan 'bitstream' yang membuat salinan secara bit-by-bit. Imej fizikal ini penting untuk mendapatkan salinan yang betul-betul sama seperti yang asal.

  Contoh:

  Primary source ->original source ->working copy

- **Imej Logikal**

  Imej ini dihasilkan apabila petugas tidak dapat menghasilkan imej fizikal disebabkan oleh kekangan peranti atau bukti yang diperlukan hanya melibatkan fail, folder atau data tertentu (contoh: mailbox, direktori penggguna, fail log)

Tindakan oleh: Petugas Teknikal

Tatacara Pengendalian Bukti Insiden

4) Pemeliharaan (*preservation*)

i. Dokumenkan maklumat bukti rujuk >>
UKM-ISMS-PK04-BO02: Senarai Bukti Insiden.

ii. Label

iii. Dokumenkan *Chain of custody* rujuk >>
UKM-ISMS-PK04-BO03: Chain of Custody.

Tindakan oleh: Petugas Teknikal

Senarai Bukti Insiden

Universiti Kebangsaan Malaysia	UKM-ISMS-PK04-BO02	No. Semakan: 00	Tarikh Kuatkuasa: 01/01/2019
	SENARAI BUKTI INSIDEN		

Kod Insiden: _____

Bil.	No. Bukti	Kondisi	Pengeluar	Model	Nombor Siri	Nilai 'Hash'	Mac Address	Lokasi	Time Offset

BUTIRAN PEMILIK	BUTIRAN PENERIMA	PENGESAHAN (ICTSO/ KETUA)
Nama pemilik : Jabatan/PTJ: Lokasi bertugas: Tarikh: Masa: Emel: No Telefon:	_____ Nama: Jabatan/PTJ: Tarikh: Masa:	_____ Nama: Jabatan/PTJ: Tarikh: Masa:

Tindakan oleh: Petugas Teknikal

Chain of Custody.

Universiti Kebangsaan Malaysia	UKM-ISMS-PK04-BO02	No. Semakan: 00	Tarikh Kuatkuasa: 01/01/2019
	CHAIN OF CUSTODY		

Kod Insiden		Halaman	

Bil.	No. bukti	Butiran bukti

No bukti	Tarikh dan Masa	Diserah oleh:	Diterima oleh:	Tujuan dan Lokasi
		_____ (Tandatangan) Nama:	_____ (Tandatangan) Nama:	
		_____ (Tandatangan) Nama:	_____ (Tandatangan) Nama:	

Tindakan oleh: Petugas Teknikal

Peranan UKMCERT

MENANGANI ANCAMAN KESELAMATAN ICT - UKM

UKMCERT

- **UKM Computer Emergency Response Team**
- Memenuhi keperluan GCERT dan Arahan Teknologi Maklumat 2007;
  - Ketua Pegawai Maklumat – CIO
  - Pegawai Keselamatan ICT – ICTSO
  - Keahlian UKMCERT ditentukan oleh CIO

Peranan UKMCERT

1. **Memantau dan mengesan** risiko keselamatan ICT;
2. **Menerima aduan** dan **menilai** insiden keselamatan ICT;
3. **Merekod** dan **menjalankan siasatan awal** insiden yang diterima;
4. Memberi tindak balas (**respond**) terhadap insiden keselamatan ICT;
5. Mengambil **tindakan baik pulih** yang sewajarnya;

UKM-ISMS-GP04

MENGURUS ADUAN SALAH LAKU ICT DI PTJ

MENGURUS ADUAN SALAH LAKU ICT DI PTJ

UKM-ISMS-GP04

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

GARIS PANDUAN
MENGURUS ADUAN SALAH LAKU ICT DI PTJ
UKM-ISMS-GP04

Muatturun dari:
>> SPDUKM: https://spdukm.ukm.my/spk/isms/

DISEDIAKAN
Jawatankuasa Pelaksana ISMS
Tarikh : 17/12/2020

No. Isu		
01	00	01/02/2021

Sistem Pengurusan Keselamatan Maklumat (ISMS) UKM

Garis Panduan ▸ Utama

Search this site...

Sistem Pengurusan Keselamatan Maklumat (ISMS) UKM Dokumen

Type	Name	No Dokumen	Tarikh Kuatkuasa
	Garis Panduan : GP01 - Keselamatan Fizikal (7)		
	Garis Panduan : GP02 - Pemindahan Maklumat (1)		
	Garis Panduan : GP03 - Pemasangan Perisian (1)		
	Garis Panduan : GP04 - Mengurus Aduan Salah Laku ICT di PTJ (1)		
	Kategori : 01-Garis Panduan (1)		
	UKM-ISMS-GP04 Garis Panduan Mengurus Aduan Salah Laku ICT di PTJ	UKM-ISMS-GP04	01/02/2021
	Add document		

Jawatankuasa
JK Induk ISMS
JK CAPA ISMS
JK Pelaksana ISMS
JK Audit Dalam ISMS
JK Risiko ISMS
MSP
SENARAI JAWATANKUASA
Dokumen
Manual ISMS
Dokumen Utama
Prosedur Kerja
Garis Panduan
Lampiran/Jadual

Tujuan Garis Panduan

membantu Ketua PTj dan pegawai-pegawai yang terlibat dalam menyediakan bukti dan **mengambil tindakan terhadap aduan** salah laku melibatkan ICT selain yang dinyatakan dalam

Garis Panduan Mengurus Kes Salah laku Pegawai di Peringkat PTJ - Panduan Mengurus Siasatan Kes di Peringkat Pusat Tanggungjawab (PTj)

Rujukan Dokumen

Sebarang pelanggaran Dasar Keselamatan Teknologi Maklumat (DKICT) Universiti Kebangsaan Malaysia (UKM) atau mana-mana Akta, Pekeliling, Peraturan dan Garis Panduan berkaitan ICT oleh pegawai mestilah diambil tindakan seperti dalam **Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 [Akta 605]**.

Ketua Pusat Tanggungjawab (PTj) perlu jelas dengan proses pengendalian aduan salah laku berkaitan ICT supaya proses siasatan dan seterusnya tindakan tatatertib dapat dilaksanakan dengan berkesan dan teratur.

Jenis-jenis salahlaku melibatkan ICT

Pelanggaran standard, prosedur, langkah dan garis panduan keselamatan

1. Menyalahguna aset ICT milik universiti sehingga memberi kesan mudarat
2. Tidak memberi perlindungan sewajarnya kepada aset ICT milik universiti sehingga menyebabkan kehilangan/kecurian maklumat sulit universiti, dan kebinasaan dan sebagainya.
3. Menyedia, memuat naik, memuat turun, dan menyebar dan menyimpan maklumat yang berbentuk keganasan, lucah, hasutan, perkauman dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak, kebencian dan suasana tidak harmoni.

Pencerobohan

1. Akses secara tidak sah ke mana-mana server milik universiti menggunakan apa-apa kaedah dengan tujuan untuk merosakkan atau mendapatkan kandungan yang terdapat dalam server.
2. Membuat capaian terhadap komputer kakitangan lain tanpa kebenaran dengan tujuan untuk dapatkan capaian ke sistem atau maklumat.

Pengubahsuaian tanpa kebenaran

1. Mengubah data atau maklumat universiti secara tidak sah (gred pelajar, maklumat gaji, maklumat peribadi kakitangan dan sebagainya)
2. Meminda atau memuatnaik bahan atau fail pada server universiti dengan niat jahat.

Jenis-jenis salahlaku melibatkan ICT

Ancaman atau gangguan

1. Menggunakan apa-apa perisian untuk mendapatkan maklumat peribadi pengguna seperti ID dan kata laluan pengguna UKM.
2. Melakukan serangan Denial of Service dengan tujuan untuk menghalang capaian pengguna ke server atau rangkaian.

Penyamaran

1. Menggunakan ID SMU pegawai lain tanpa kebenaran untuk melakukan transaksi yang tidak sah.
2. Menghantar e-mel menggunakan identiti orang lain dengan niat jahat.

Pendedahan Maklumat

Memberi maklumat pelajar yang dicetak daripada Sistem Maklumat Pelajar kepada pihak luar.

Jenis-jenis salahlaku melibatkan ICT

Komunikasi Salah

1. Memberi kata laluan Pentadbir Server kepada kakitangan/ individu lain yang tidak diberi kuasa.
2. Seorang kakitangan beri kad akses pintu miliknya kepada pihak ketiga.

Pensubahatan dan percubaan

1. Kakitangan yang tidak mempunyai kuasa didapati melakukan percubaan untuk mencapai dan meminda gred pelajar.
2. Cubaan membuat imbasan rangkaian UKM tanpa kebenaran sehingga menjejaskan perkhidmatan ICT.
3. Tidak melaporkan kakitangan yang secara jelas telah melakukan kesalahan ICT.

Tindakan dari aduan yang diterima

- **Ketua PTj dan pegawai-pegawai yang terlibat** dalam mengendalikan aduan :
  1. **Mengenalpasti** sumber ICT dan bukti yang berpotensi
  2. Memohon dengan **segera** kepada Pusat Teknologi Maklumat (PTM) untuk menyekat atau **menghalang capaian** oleh pegawai yang disyaki terhadap sumber ICT(jika perlu);
  3. **Mendapatkan bukti daripada PTj** lain bagi melengkapkan siasatan (jika perlu).

Tatacara Pengumpulan Bukti

- Tanggungjawab **Ketua PTj**:
  1. Memastikan semua maklumat dan bukti adalah sulit dan disimpan ditempat yang terkawal.
  2. Merekod menyimpan dan memelihara semua bukti sama ada dalam bentuk fizikal atau digital bagi memastikan bukti tidak terjejas dan boleh digunakan untuk tujuan tindakan tatatertib atau tindakan perundangan
  3. Memastikan bukti diperolehi dengan cara dan kaedah yang bersesuaian

Rumusan

- Ancaman keselamatan ICT
- DKICT
- Pelaksanaan ISMS
- Prosedur Kerja dan Garis Panduan
- UKMCERT

Sekian

JUMPA DI SIRI YANG AKAN DATANG