



22 Ogos 2024
22 August 2024
P.U. (A) 221

WARTA KERAJAAN PERSEKUTUAN

*FEDERAL GOVERNMENT
GAZETTE*

PERATURAN-PERATURAN KESELAMATAN SIBER
(PELESENAN PEMBERI PERKHIDMATAN
KESELAMATAN SIBER) 2024

*CYBER SECURITY (LICENSING OF CYBER SECURITY
SERVICE PROVIDER) REGULATIONS 2024*

DISIARKAN OLEH/
PUBLISHED BY
JABATAN PEGUAM NEGARA/
ATTORNEY GENERAL'S CHAMBERS

AKTA KESELAMATAN SIBER 2024

PERATURAN-PERATURAN KESELAMATAN SIBER
(PELESENAN PEMBERI PERKHIDMATAN KESELAMATAN SIBER) 2024

PADA menjalankan kuasa yang diberikan oleh seksyen 63 Akta Keselamatan Siber 2024 [Akta 854], Menteri membuat peraturan-peraturan yang berikut:

Nama dan permulaan kuat kuasa

1. (1) Peraturan-peraturan ini bolehlah dinamakan **Peraturan-Peraturan Keselamatan Siber (Pelesenan Pemberi Perkhidmatan Keselamatan Siber) 2024**.

(2) Peraturan-Peraturan ini mula berkuat kuasa pada 26 Ogos 2024.

Pemakaian dan ketidakpakaian

2. (1) Peraturan-Peraturan ini hendaklah terpakai bagi perkhidmatan keselamatan siber yang berhubungan dengan perkhidmatan pemantauan pusat operasi keselamatan terurus dan perkhidmatan pengujian penembusan.

(2) Peraturan-Peraturan ini tidak terpakai jika—

(a) perkhidmatan keselamatan siber itu diberikan oleh Entiti Kerajaan;

(b) perkhidmatan keselamatan siber itu diberikan oleh seseorang, selain suatu syarikat, kepada syarikat berkaitannya; atau

(c) komputer atau sistem komputer yang berkenaan dengannya perkhidmatan keselamatan siber itu diberikan terletak di luar Malaysia.

Tafsiran

3. Dalam Peraturan-Peraturan ini—

“kerentanan” ertinya apa-apa kerentanan pada komputer atau sistem komputer yang boleh dieksploitasi oleh satu atau lebih ancaman keselamatan siber;

“perkhidmatan pemantauan pusat operasi keselamatan terurus” ertinya suatu perkhidmatan sebagaimana yang diperuntukkan di bawah peraturan 4;

“perkhidmatan pengujian penembusan” ertinya suatu perkhidmatan sebagaimana yang diperuntukkan di bawah peraturan 5.

Perkhidmatan pemantauan pusat operasi keselamatan terurus

4. Suatu perkhidmatan pemantauan pusat operasi keselamatan terurus di bawah Peraturan-Peraturan ini ialah suatu perkhidmatan bagi—

- (a) memantau tahap keselamatan siber suatu komputer atau sistem komputer seorang yang lain dengan cara memperoleh, mengenal pasti atau mengimbas maklumat yang disimpan dalam, diproses oleh atau dihantar melalui, komputer atau sistem komputer itu bagi maksud mengenal pasti atau mengesan ancaman keselamatan siber terhadap komputer atau sistem komputer itu; atau
- (b) menentukan langkah-langkah yang perlu untuk bertindak balas terhadap atau pulih daripada apa-apa insiden keselamatan siber itu dan untuk mencegah insiden keselamatan siber itu daripada berlaku pada masa hadapan.

Perkhidmatan pengujian penembusan

5. Suatu perkhidmatan pengujian penembusan di bawah Peraturan-Peraturan ini ialah perkhidmatan untuk menaksir, menguji atau menilai tahap keselamatan siber suatu komputer atau sistem komputer, dengan mencari kerentanan pada, dan menjejaskan, pertahanan keselamatan siber komputer atau sistem komputer itu, dan termasuklah mana-mana aktiviti yang berikut:

- (a) menentukan kerentanan keselamatan siber suatu komputer atau sistem komputer, dan menunjukkan bagaimana kerentanan itu boleh dieksploitasi dan diambil kesempatan;
- (b) menentukan atau menguji keupayaan organisasi untuk mengenal pasti dan bertindak balas terhadap insiden keselamatan siber melalui simulasi percubaan untuk menembusi pertahanan keselamatan siber komputer atau sistem komputer;
- (c) mengenal pasti dan mengukur kerentanan keselamatan siber suatu komputer atau sistem komputer, yang menyatakan kerentanan itu dan menyediakan tatacara mitigasi yang sesuai yang dikehendaki untuk menghapuskan kerentanan itu atau mengurangkan kerentanan itu kepada tahap risiko yang boleh diterima; atau
- (d) menggunakan kejuruteraan sosial untuk menaksir tahap kerentanan suatu organisasi terhadap ancaman keselamatan siber.

Permohonan bagi lesen

6. (1) Tertakluk pada seksyen 28 Akta, suatu permohonan bagi suatu lesen untuk memberikan perkhidmatan keselamatan siber oleh seseorang yang berniat untuk memberikan apa-apa perkhidmatan keselamatan siber atau mengiklankan, atau dalam apa-apa cara mengemukakan dirinya sebagai pemberi suatu perkhidmatan keselamatan siber hendaklah dibuat kepada Ketua Eksekutif melalui cara elektronik dan hendaklah disertakan dengan pembayaran fi sebagaimana yang ditetapkan dalam Jadual.

(2) Suatu permohonan di bawah subperaturan (1) boleh ditarik balik pada bila-bila masa sebelum permohonan diluluskan atau ditolak oleh Ketua Eksekutif.

(3) Fi yang disebut dalam subperaturan (1) hendaklah kena dibayar bagi tiap-tiap permohonan yang dikemukakan dan tidak boleh dibayar balik.

Pembaharuan lesen

7. (1) Suatu permohonan bagi pembaharuan lesen untuk memberikan perkhidmatan keselamatan siber hendaklah dibuat kepada Ketua Eksekutif melalui cara elektronik dan hendaklah disertakan dengan pembayaran fi sebagaimana yang ditetapkan dalam Jadual.

(2) Mana-mana permohonan bagi pembaharuan lesen yang diterima oleh Ketua Eksekutif selepas habis tempoh pembaharuan lesen hendaklah dikira sebagai suatu permohonan baru.

(3) Fi yang disebut dalam subperaturan (1) hendaklah kena dibayar bagi tiap-tiap permohonan yang dikemukakan dan tidak boleh dibayar balik.

Permohonan secara fraud dan maklumat palsu

8. Seseorang yang, berkaitan dengan apa-apa permohonan yang dibuat di bawah Peraturan-Peraturan ini, membuat suatu pernyataan yang palsu atau mengelirukan dengan mengetahui bahawa pernyataan itu palsu atau mengelirukan atau dengan sengaja meninggalkan daripada menyatakan apa-apa perkara atau benda yang tanpanya permohonan itu adalah mengelirukan melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi lima puluh ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

JADUAL
[Subperaturan 6(1) dan 7(1)]

| (1) Bil. | (2) Perihal | (3) Fi (setahun) | |
|-------------|---|------------------------|---|
| | | Individu | Syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain |
| 1. | Permohonan bagi lesen | | |
| | (a) Perkhidmatan pemantauan pusat operasi keselamatan terurus | RM400.00 | RM1000.00 |
| | (b) Perkhidmatan pengujian penembusan | RM400.00 | RM1000.00 |
| 2. | Pembaharuan lesen | | |
| | (a) Perkhidmatan pemantauan pusat operasi keselamatan terurus | RM400.00 | RM1000.00 |
| | (b) Perkhidmatan pengujian penembusan | RM400.00 | RM1000.00 |

Dibuat 16 Ogos 2024
[MKN(S).10.600-9/2/4 Jld.8 (22); PN(PU2)768]

DATO' SERI ANWAR BIN IBRAHIM
Perdana Menteri

CYBER SECURITY ACT 2024

CYBER SECURITY (LICENSING OF CYBER SECURITY SERVICE PROVIDER)
REGULATIONS 2024

IN exercise of the powers conferred by section 63 of the Cyber Security Act 2024 [Act 854], the Minister makes the following regulations:

Citation and commencement

1. (1) These regulations may be cited as the **Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024**.

(2) These Regulations come into operation on 26 August 2024.

Application and non-application

2. (1) These Regulations shall apply to cyber security service relating to managed security operation centre monitoring service and penetration testing service.

(2) These Regulations shall not apply if—

(a) the cyber security service is provided by a Government Entity;

(b) the cyber security service is provided by a person, other than a company, to its related company; or

(c) the computer or computer system in respect of which the cyber security service is provided is located outside Malaysia.

Interpretation

3. In these Regulations—

“vulnerability” means any vulnerability on a computer or computer system that can be exploited by one or more cyber security threats;

“managed security operation centre monitoring service” means a service as provided under regulation 4;

“penetration testing service” means a service as provided under regulation 5.

Managed security operation centre monitoring service

4. A managed security operation centre monitoring service under these Regulations is a service for—

- (a) monitoring the level of cyber security of a computer or computer system of another person by acquiring, identifying or scanning information that is stored in, processed by or transmitted through, the computer or computer system for the purpose of identifying or detecting cyber security threats to the computer or computer system; or
- (b) determining the measures necessary to respond to or recover from any cyber security incident and to prevent such cyber security incident from occurring in the future.

Penetration testing service

5. A penetration testing service under these Regulations is a service for assessing, testing or evaluating the level of cyber security of a computer or computer system, by searching for vulnerabilities on, and compromising, the cyber security defences of the computer or computer system, and includes any of the following activities:

- (a) determining the cyber security vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of;
- (b) determining or testing the organization’s ability to identify and respond to cyber security incident through simulation of attempts to penetrate the cyber security defences of the computer or computer system;

- (c) identifying and measuring the cyber security vulnerabilities of a computer or computer system, indicating vulnerabilities and preparing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk; or
- (d) utilizing social engineering to assess the level of vulnerability of an organization to cyber security threats.

Application for licence

6. (1) Subject to section 28 of the Act, an application for a licence to provide cyber security service by any person who intends to provide any cyber security service or advertise, or in any way hold himself out as a provider of a cyber security service shall be made to the Chief Executive through electronic means and shall be accompanied by payment of the fee as prescribed in the Schedule.

(2) An application under subregulation (1) may be withdrawn at any time before the application is approved or refused by the the Chief Executive.

(3) The fee referred to in subregulation (1) shall be payable for every application submitted and shall not be refundable.

Renewal of licence

7. (1) An application for the renewal of licence to provide cyber security service shall be made to the Chief Executive through electronic means and shall be accompanied by payment of the fee as prescribed in the Schedule.

(2) Any application for the renewal of licence which is received by the Chief Executive after the expiry of the licence shall be treated as a new application.

(3) The fee referred to in subregulation (1) shall be payable for every application submitted and shall not be refundable.

Fraudulent application and false information

8. A person who, in connection with any application made under these Regulations, makes a statement that is false or misleading knowing it to be false or misleading or wilfully omits to state any matter or thing without which the application is misleading commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding two years or to both.

SCHEDULE

[Subregulations 6(1) and 7(1)]

| (1) No. | (2) Description | (3) Fee (per year) | |
|------------|--|--------------------------|--|
| | | Individual | Company, limited liability partnership, firm, society or other body of persons |
| 1. | Application for licence | | |
| | (a) Managed security operation centre monitoring service | RM400.00 | RM1000.00 |
| | (b) Penetration testing service | RM400.00 | RM1000.00 |
| 2. | Renewal of licence | | |
| | (a) Managed security operation centre monitoring service | RM400.00 | RM1000.00 |
| | (b) Penetration testing service | RM400.00 | RM1000.00 |

Made 16 August 2024
[MKN(S).10.600-9/2/4 Jld.8 (22); PN(PU2)768]

DATO' SERI ANWAR BIN IBRAHIM
Prime Minister