

## BAB II

### TINJAUAN PUSTAKA

#### 2.1 Keamanan Informasi

Keamanan informasi adalah suatu tindakan untuk menjaga & melindungi informasi beserta bagian-bagian informasi pada software maupun hardware yang dipakai untuk menyimpan dan mengirimkan informasi. terkait mengenai keamanan informasi terdapat istilah 4R yaitu ;

- a. Right Information adalah suatu ketepatan dan keaslian suatu informasi yang memiliki integritas pada informasi tersebut.
- b. Right People adalah seorang pengguna yang memiliki akses secara sah atau yang dapat menjamin kerahasiaan suatu informasi.
- c. Right Time adalah ketepatan aksesibilitas informasi sekaligus menjamin ketersediaan informasi berdasarkan permintaan suatu entitas yang sah.
- d. Right Form adalah penyediaan informasi dalam format yang tepat.

Tindakan kejahatan yang mengarah pada informasi merupakan asset yang harus dilindungi keamanannya. Keamanan informasi bertujuan untuk menjaga informasi dari

menjaga keamananya. Keamanan informasi berujuan untuk menjaga informasi dari berbagai ancaman untuk proses keberlangsungan usaha dengan mengurangi kerusakan akibat ancaman. Tujuan utama menjaga keamanan informasi adalah kerahasiaan, ketersediaan, dan integritas. Tujuan lain menjaga keamanan informasi agar informasi-informasi yang bersifat privasi tidak disebarluaskan. Privasi informasi terbagi menjadi empat definisi yaitu pribasi sebagai hak asasi setiap manusia, privasi sebagai komoditas atau sesuatu yang dapat diperdagangkan sesuai dengan harga yang telah ditentukan, privasi sebagai keadaan akses terbatas dimana hanya orang-orang terpilih yang dapat memiliki izin akses yang sah, privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri [1][2][3].

6

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 2 Refresh

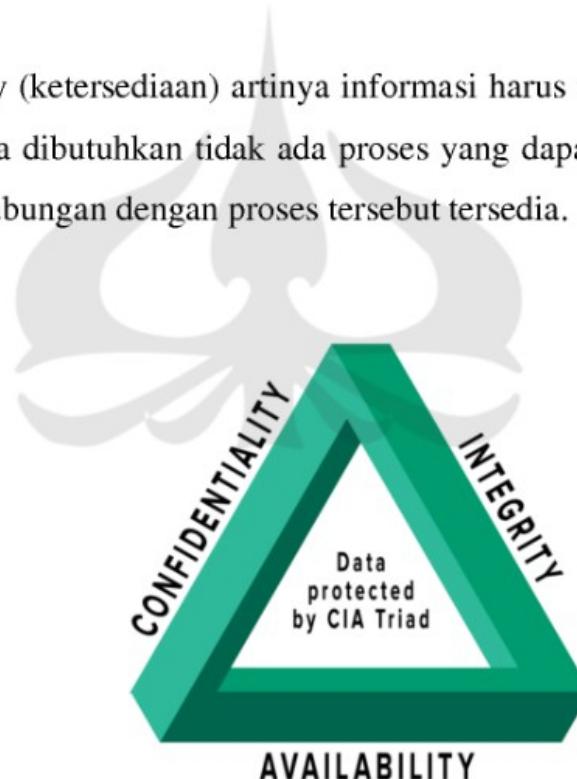
7

Terdapat tiga aspek untuk tercapainya keamanan informasi yaitu [3] ;

- a. Confidentiality (kerahasiaan) artinya informasi hanya tersedia untuk orang atau sistem yang memang perlu akses. Hal ini dilakukan dengan melakukan enkripsi

informasi dimana hanya orang-orang tertentu yang dapat mendeskripsi atau menolak akses informasi dari orang-orang yang tidak membutuhkannya. Kerahasiaan harus ditetapkan pada semua aspek disebuah sistem. Hal ini berarti mencegah akses ke semua lokasi cadangan dan bahkan log files jika file-file tersebut berisi informasi sensitif.

- b. Integrity (keaslian) artinya informasi hanya dapat ditambah atau diperbarui oleh orang yang telah diautorisasi. Perubahan yang tidak sah terhadap data dapat menyebabkan data kehilangan integritasnya dan jika itu terjadi, maka akses terhadap informasi harus dihentikan sampai integritas informasi pulih kembali.
- c. Availability (ketersediaan) artinya informasi harus tersedia dalam waktu yang tepat ketika dibutuhkan tidak ada proses yang dapat dilakukan bila informasi yang berhubungan dengan proses tersebut tersedia.



Gambar 2.1 CIA Triad Model  
(sumber : www. F2.com)

Ketiga aspek tersebut disebut dengan CIA Triad. CIA Triad adalah model design untuk kebijakan keamanan informasi pada suatu organisasi. Unsur-unsur pada CIA triad dianggap sebagai 3 komponen keamanan paling penting[3].

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

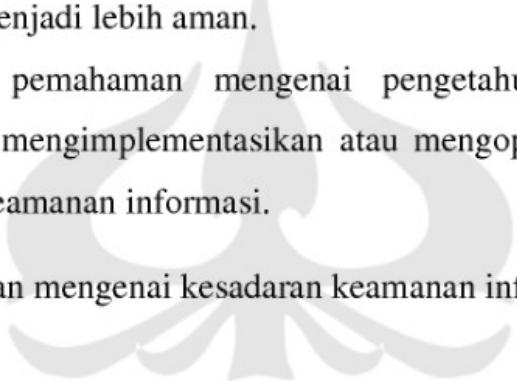
Pilih Lembar ke : 3 Refresh

8

## 2.2 Kesadaran keamanan Informasi

Kesadaran keamanan informasi adalah suatu poin utama untuk seseorang dalam memahami pengetahuan mengenai keamanan informasi. Suatu pemahaman kesadaran keamanan informasi seseorang dapat memfokuskan perhatianya pada masalah keamanan informasi atau ancaman-ancaman yang bisa terjadi. Tujuan kesadaran keamanan informasi adalah untuk meningkatkan dengan melakukan hal berikut [1][4] ;

1. Peran seseorang dalam suatu organisasi harus paham mengenai informasi dan bertanggung jawab terhadap sistem keamanan informasi dan mengajarkan bagaimana bentuk keamanan yang tepat sehingga dapat membantu untuk mengubah sikap atau perilaku menjadi lebih sadar akan keamanan.

- 
2. Meningkatkan kemampuan dan ilmu pengetahuan user dapat melakukan pekerjaan menjadi lebih aman.
  3. Menambah pemahaman mengenai pengetahuan yang diperlukan untuk merancang, mengimplementasikan atau mengoperasikan program pembinaan kesadaran keamanan informasi.

Program penyuluhan mengenai kesadaran keamanan informasi dapat dibagi menjadi 3 bagian yaitu [1] :

1. Pendidikan adalah suatu media utama untuk mendapatkan pemahaman mengenai pentingnya menjaga keamanan informasi dan memberikan pemahaman mengenai tanggung jawab atas keamanan yang mempengaruhi lingkungan mereka masing-masing. Salah satu Pendidikan yang di dapat adalah disekolah atau perguruan tinggi namun bisa juga melalui kursus keamanan informasi.
2. Pemahaman mengenai keamanan informasi juga dapat diperoleh dari pelatihan. Tujuan dari pelatihan ini adalah agar para user mengetahui bagaimana bisa menimbulkan rasa aman, mengetahui bagaimana menggunakan fungsi keamanan didalam sebuah aplikasi dan bagaimana proses kerja.

3. Kesadaran merupakan komponen terpenting setelah seseorang mendapatkan pelatihan dan Pendidikan karena pelatihan dan Pendidikan saja tidak menjamin perilaku seseorang dalam menjaga keamanan informasi dalam kehidupan sehari-hari. Menimbulkan kesadaran pribadi dapat disebarluaskan secara umum melalui poster, mouse-pads, dan bolpoin dengan gambar atau kata-kata yang menarik perhatian seseorang untuk membaca dan melihat, dengan cara tersebut dan tanpa disadari merubah seseorang dari “menjadi sadar” menjadi “menyadari” dan berakhir “sadar” mengenai pentingnya menjaga keamanan informasi.

Seorang ilmuan Dhilon dalam kruger mengemukakan bahwa perilaku informal adalah dasar untuk mencerminkan karakteristik seseorang, organisasi, dan tindakan komunikasi yang mempengaruhi informasi. Pola pembelajaran, budaya, dan struktur normal yang ada merupakan elemen perilaku informal konstituen sehingga dapat disimpulkan bahwa manajemen keamanan informasi dapat dilakukan dengan lengkap jika aspek perilaku individu dan kelompok diketahui [1].

Kruger & Kearney berpendapat bahwa kesadaran keamanan informasi merupakan proses dinamis yang berkembang sesuai dengan keadaan yang terjadi, baik karena masalah politik hingga masalah mengenai perekonomian. Kesadaran tersebut mencakup kesadaran untuk melindungi keamanan informasi individu maupun informasi organisasi itu berada. Kruger & Kearney mengelompokan kesadaran keamanan informasi menjadi 3 aspek yaitu [5] ;

1. Knowledge

Knowledge adalah suatu pengetahuan yang dimiliki oleh individu perihal keamanan informasi. Menurut Kamus Besar Bahasa Indonesia (KBBI), Pengetahuan berkaitan dengan segala hal yang diketahui; kepandaian; semua hal yang diketahui mengenai dengan hal tersebut.

## 2. Attitude

Attitude merupakan suatu sikap seseorang dalam berinteraksi atau berkomunikasi dengan lawan bicara. Menurut Notoatmodjo, sikap merupakan kesigapan atau kesediaan untuk melakukan tindakan dan bukan pelaksanaan yang bertujuan pada motif tertentu.

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 5 Refresh

10

## 3. Behaviour

Perilaku adalah suatu tindakan yang dilakukan oleh individu mengenai keamanan informasi dan perilaku bisa dikatakan adalah respon dari stimulus yang mana setiap individu memiliki kemampuan untuk menentukan perilaku yang akan diputuskan.

Penjelasan diatas menjelaskan bahwa menciptakan kesadaran manusia untuk

menjaga keamanan informasi pribadi. Individu akan mendapatkan pengetahuan mengenai keamanan informasi, kemudian individu tersebut memahami dan mengerti pengetahuan yang diterima serta menerapkan keamanan informasi yang didapat sehingga individu memiliki kesadaran untuk menjaga keamanan informasi pribadinya.

Berdasarkan penelitian yang dilakukan Kruger & Kearney bahwa terdapat level of awareness sebagai berikut [5] :

Awareness	Measurement (%)
Good	80–100
Average	60–79
Poor	59 and less

**Gambar 2.1 Level of Awareness**

(Sumber: Jurnal Kruger & Kearney)

Level of Awareness terdiri 3 kategori , yaitu :

1. Good (Baik)

Tingkat kesadaran pada kategori baik menghasilkan angka  $\geq 80\%$ . Pada tingkat ini dapat diartikan bahwa materi pengetahuan yang dapat diterapkan mengenai keamanan informasi (knowledge) telah dikatakan mampu dipahami melalui sikap, dan diimplementasikan dalam kehidupan sehari-hari.

2. Average (Sedang)

Tingkat kesadaran pada kategori sedang menghasilkan angka  $\geq 60\% - > 80\%$ . Pada tingkat ini dapat diartikan bahwa ada salah satu dari tiga aspek dalam kesadaran keamanan informasi, yaitu pengetahuan keamanan informasi yang dipahami lewat sikap dan seharusnya sudah dapat diimplementasikan dalam kehidupan sehari-hari namun belum mampu terpenuhi.

3. Poor (Buruk)

Tingkat kesadaran pada kategori buruk menghasilkan angka  $- > 60\%$ . Pada tingkat ini dapat diartikan bahwa materi keamanan informasi yang didapat tidak dapat dipahami sehingga mempengaruhi sikap dan diimplementasikan dalam kehidupan sehari-hari untuk menjaga keamanan informasi.

Berdasarkan pada uraian mengenai kesadaran keamanan informasi, maka dapat disimpulkan bahwa kesadaran keamanan informasi adalah Tindakan yang dilakukan secara sadar untuk menjaga informasi pribadi yang dimiliki. Namun Tindakan yang dilakukan untuk menjaga informasi pribadi pada setiap individu dipengaruhi oleh sikap

yang dimiliki dalam privasi masing-masing individu seninggal tingkat kesadaran yang dimiliki dapat berbeda antara satu dengan yang lain [1][9].

### 2.3 Konsep keamanan Informasi

Ada beberapa konsep keamanan informasi yang dipaparkan oleh Chan dan Mubarak sebagai berikut [1] ;

#### 1. Phising

Phising adalah usaha untuk mendapatkan informasi bersifat rahasia atau dengan mencuri identitas dengan memakai email atau website palsu yang meniru alamat situs yang asli. Phising juga dilakukan secara non-teknis seperti Social Engineering atau dilaksanakan bersama Spam sebagai modus untuk melakukan phising. Phising merupakan ancaman umum terhadap aspek keamanan informasi maka dari itu sangat penting bagi setiap individu untuk menyadari dampak dan bahaya phising.

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 7

v

Refresh

Spam adalah surat atau pesan elektronik komersial yang tidak diharapkan oleh penerimanya. Spam banyak dianggap sepele tapi spam bukan hanya mengganggu penerima namun dapat menimbulkan bencana atau mengganggu sistem. Contoh bahaya spam adalah kode berbahaya yang berisi virus atau trojan yang memakai spam sebagai penghubung untuk distribusi. Kode bahaya tersebut dapat mengakibatkan mengurangi perfomance sistem dan membatas akses ke pengguna sehingga melanggar aspek ketersediaan informasi. Selain itu isi pesan dalam spam memuat link yang mengarahkan ke situs phising. Disamping itu kontrol teknis yang ditentukan oleh suatu organisasi untuk mencegah spam masuk ke dalam sistem email organisasi yang mungkin tidak dapat mencegah hingga tuntas. Maka sebab itu, sangat penting bagi setiap individu untuk mengetahui konsep spam dan cara mengatasinya.

### 3. Social engineering

Social engineering adalah penggunaan sarana non-teknis untuk melakukan pencurian informasi rahasia yang biasanya berupa identitas. Attacker dapat menggunakan kombinasi dari manipulasi psikologis dan peniruan dalam rangka mendorong korban tidak bersedia dalam menyediakan informasi yang rahasia. Mitigasi Social Engineering sangat bergantung pada kesadaran karyawan mengenai konsep dan penegakan kebijakan organisasi yang berkaitan tentang keamanan dan privasi.

### 4. Strong password

Password adalah kunci untuk otentikasi pengguna untuk mencegah akses tanpa izin ke dalam sistem. Password juga dapat diambil secara illegal dengan menggunakan dua jenis serangan yang dikenal sebagai password cracking, maka

dari itu untuk menghindari password cracking adalah dengan membuat password tersebut menjadi kuat karena semakin kuat sebuah password maka semakin lama waktu yang dibutuhkan untuk memecahkannya. Password yang kuat dapat mengurangi kemungkinan terjadinya serangan password yang dilakukan oleh attacker. Pengetahuan mengenai konsep password pun menjadi sangat penting dan

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 8  Refresh

13

password kuat harus terdiri dari kombinasi yang cukup Panjang antara huruf, angka, dan simbol.

##### 5. Data or information integrity

Integritas data dan informasi yang berkaitan dengan aspek integritas keamanan informasi memiliki ciri sebagai berikut :

- a. Akurasi dan kebenaran informasi harus kuat dan benar dengan maksud data harus tepat dan sesuai dengan kebenaran yang ada , seperti data identitas berupa nama lengkap yang dimasukan ke dalam sistem tidak boleh terdapat kesalahan penulisan ataupun tidak lengkap.
- b. Kepercayaan berkaitan dengan memastikan akurasi dan kebenaran mengenai

- informasi yang tersimpan dalam sistem berdasarkan representasi dari kenyataan sehingga seseorang dapat mempercayai informasi tersebut.
- c. Keberlakuan dan ketepatan waktu menggunakan tanggal lahir merupakan contoh yang dapat digunakan karena tanggal lahir termasuk variable yang dapat berubah dari waktu ke waktu. Keberlakuan dipengaruhi oleh perubahan kenyataan dari waktu ke waktu dan harus dipenuhi.

#### 6. Social networking

Media sosial seperti Facebook dan Twitter sebagai sumber bocornya informasi rahasia sudah semakin umum beberapa tahun terakhir ini. Para pengguna media sosial kerap mencantumkan informasi pribadi, biasanya informasi pribadi berupa tempat kerja, Pendidikan, atau bahkan nomor handphone. Maka dari itu, media sosial merupakan bagian penting untuk setiap rencana keamanan.

### 2.4 Manfaat Keamanan Informasi

Menurut Dony Ariyus, pengamanan informasi sangat diperlukan untuk beberapa hal yaitu [6] :

- 1. Menjaga privasi informasi dari pihak-pihak yang tidak memiliki hak atau keperluan yang memiliki izin terhadap informasi tersebut.
- 2. Menjaga integritas suatu informasi sehingga data tidak mengalami perubahan pada isi informasi baik oleh yang tidak berhak ataupun oleh hal lain yang tidak diinginkan.

3. Memastikan identitas (otentikasi), baik manusia, mesin, ataupun kartu sekaligus menyamarkan identitas kepada yang tidak memiliki izin.

## 2.5 Penelitian Terdahulu

Penelitian ini bertujuan untuk tugas akhir dan berfokus pada kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti. Ada beberapa penelitian yang sudah melakukanya dan dapat digunakan sebagai acuan salah satunya adalah Kruger & Kearney . Beliau telah melakukan penelitian mengenai kesadaran keamanan informasi berjudul A prototype for assessing information security awareness pada tahun 2006. Penelitian ini bertujuan untuk mengukur kesadaran keamanan informasi di sebuah perusahaan besar di bidang pertambangan international dengan pengembangan model prototipe. Metode ukur yang digunakan berasal dari sisi psikolog sosial yaitu pengaruh perilaku dan kognisi yang dikembangkan dengan mengukur pengetahuan, sikap dan perilaku individu terhadap kesadaran keamanan informasi. pengukuran dilakukan memakai pendekatan scorecard sederhana dan penyebaran kuesioner. Hasil yang didapat ialah kesadaran secara keseluruhan diperusahaan tersebut dianggap rata-rata sebesar 65% dengan jumlah 77% kesadaran pengetahuan, 76% kesadaran sikap, dan 54% kesadaran perilaku [5].

Mukhlis melakukan penelitian tentang pengukuran tingkat kesadaran keamanan

informasi pada Pegawai Negeri Sipil Pemerintahan Kota Makasar dengan metode Multiple Criteria Decision Analysis (MCDA). Hasil dari penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi PNS Pemkot Makasar secara keseluruhan berada pada kategori “sedang” sehingga masih perlu dimonitor untuk kemungkinan dilakukan pemberian bantuan atau pelatihan [1].

## 2.6 Populasi dan Sampel

Populasi adalah seluruh objek penelitian yang terdiri atas manusia, benda-benda, hewan, tumbuhan, gejala-gejala, nilai tes, atau peristiwa-peristiwa sebagai sumber data yang memiliki karakteristik nilai tertentu dalam suatu penelitian [12].

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh populasi tersebut. Jika populasi yang dimiliki berjumlah besar dan peneliti tidak mungkin

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 10 Refresh

15

mempelajari semua, baik karena keterbatasan dana, waktu, tenaga, maka peneliti dapat menggunakan sampel yang diambil dari populasi tersebut [12].

## 2.7 Teknik Sampling

Pada umumnya, terdapat dua Teknik sampling yaitu Probability Sampling dan Non-Probability Sampling. Berikut adalah penjelasan dari kedua Teknik sampling [4] ;

1. Probability Sampling

Probability Sampling adalah Teknik pengambilan sampel yang memberikan peluang yang sama bagi setiap unsur (anggota) populasi untuk dipilih menjadi anggota sampel. Teknik ini meliputi ;

a. Simple Random Sampling

Teknik ini digunakan jika pengambilan pada anggota sampel dari populasi dilakukan secara acak tanpa memperhatikan strata yang ada pada populasi. Teknik pengambilan sampel seperti ini biasa dilakukan pada anggota populasi homogen dan dengan cara undian atau memilih bilangan dari daftar bilangan secara acak.

b. Proportionate Stratified Random Sampling

Teknik ini digunakan jika populasi bersifat heterogen atau memiliki jenjang secara proporsional. Sebagai contoh suatu perusahaan memiliki karyawan dari latar belakang yang berbeda-beda yaitu ; 205 orang lulusan Strata 1 (S1), 99 orang lulusan Strata 2 (S2), 45 orang lulusan Strata 3 (S3), 154 orang lulusan SMA/SMK, 39 orang lulusan Sekolah Dasar (SD). Jumlah anggota pada populasi di perusahaan tersebut tidak sama atau bervariasi. Jumlah sampel yang harus diambil meliputi strata Pendidikan yang ada diambil secara proporsional.

c. Disproportionate Stratified Random Sampling

Teknik ini digunakan untuk mengambil sampel dari populasi yang berstrata atau berjenjang tapi kurang proporsional. Sebagai contoh suatu instansi memiliki karyawan dari latar belakang yang berbeda-beda terdiri dari 400

orang lulusan SMP, 500 orang lulusan SMA, 145 orang lulusan D3, 90 orang lulusan S1, 7 orang lulusan S2, 2 orang lulusan S3. Berdasarkan jumlah lulusan

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 11 Refresh

16

S2 dan S3 kurang proporsional (terlalu kecil) dibanding dengan jenjang lulusan yang lain, maka untuk lulusan jenjang S2 dan S1 seluruhnya digunakan sebagai sampel penelitian.

d. Cluster Sampling (Area Sampling)

Teknik ini digunakan untuk menentukan sampel bila objek yang akan diteliti atau sumber data yang sangat luas misalnya penduduk disuatu negara, provinsi, kota atau kabupaten. Misalnya saat sedang melakukan penelitian dengan populasi pelajar SMA disuatu wilayah. Pengambilan sampel tidak secara langsung dilakukan pada pelajar-pelajar SMA namun pada sekolah yang telah ditetapkan. Teknik Cluster Sampling dilakukan dalam 2 tahap penentuan yaitu ;

- 1) Menentukan sampel daerah (misalnya menentukan sekolah-sekolah yang akan dijadikan sampel ).
- 2) Menentukan orang-orang atau anggota sampel yang ada pada daerah

2) menentukan orang-orang atau anggota sampel yang ada pada daftar tersebut ( misalnya menentukan pelajar SMA yang ada pada sekolah-sekolah yang dijadikan ampel).

## 2. Non-Probability Sampling

Non-Probability Sampling merupakan Teknik penarikan sampel yang tidak memberikan peluang yang sama bagi setiap unsur atau anggota populasi untuk terpilih menjadi sampel. Teknik Non-Probability Sampling meliputi berikut ;

### a. Sampling Sistematis

Teknik pengambilan sampel dengan menggunakan sampling sistematis berarti berdasarkan urutan anggota populasi yang telah diberi nomor urut. Sebagai contoh jumlah anggota populasi sebanyak 200 orang yang telah memiliki nomor urut 1,2,3 hingga nomor 200. Pengambilan sampelnya dilakukan dengan ketentuan mengambil nomor ganjil saja , genap saja, atau kelipatan dari bilangan tertentu. Misalnya dari anggota populasi yang telah diberi nomor urut sejumlah 200 tersebut diambil nomor dengan kelipatan 3. Maka yang diambil sampelnya adalah nomor 3,6,9,12,15,18, dan seterusnya hingga sampai nomor 200.

### b. Sampling Kuota

Sampling Kuota adalah Teknik sampling yang menentukan jumlah sampel dari populasi yang memiliki ciri tertentu sampai jumlah kuota yang diinginkan. Contohnya akan dilakukan penelitian tentang pendapat masyarakat terhadap pelayanan pembukaan E-Ktp. Jumlah sampel yang ditentukan adalah 300 orang. Dalam hal ini, jika pengumpulan datanya belum tercapai 300 orang maka penelitian dianggap belum selesai karena belum mencapai kuota yang ditentukan yaitu 300 orang.

c. Sampling Insidental

Sampling Insidental adalah Teknik yang pengambilan sampel dilakukan secara kebetulan bertemu dengan peneliti kemudian dianggap cocok dengan karakter sampel. Misalnya penelitian tentang kepuasan pelanggan pada pelayanan Mall “ X “. Sampel ditentukan berdasarkan ciri-ciri usia diatas 15 tahun dan abru pernah ke Mall “ X “ dengan ciri-ciri tersebut dapat dijadikan sampel.

d. Sampling Purposive

Sampling Purposive adalah Teknik penarikan sampel yang dilakukan dengan pertimbangan tertentu saja. Misalnya peneliti akan melakukan peneltiiian tentang kualitas kosmetik, maka sebagai sampelnya adalah orang-orang yang ahli dalam bidang kecantikan.

e. Sampling Jenuh

Sampling jenuh adalah sampel yang mewakili jumlah populasi atau dengan kata lain semua anggota populasi dijadikan sampel. Hal ini dilakukan apabila jumlah anggota populasi berjumlah sedikit, kurang dari 30 orang. Sampling jenuh ini sering disebut dengan sensus dimana semua anggota populasi

dijadikan sampel penelitian.

f. Sampling Snowball

Sampling snowball adalah Teknik penarikan sampel yang pada awalnya berjumlah kecil kemudian bertambah menjadi besar. Dalam penentuan sampel, awalnya hanya dipilih satu atau dua orang tetapi peneliti merasa data yang didapat belum lengkap dari satu atau dua orang tersebut maka dicari lagi orang lain yang dianggap lebih tahu dan dapat melengkapi data.

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti  
Devi Febrita Sari Hoesadha, 2021

Pilih Lembar ke : 13  Refresh

18

## 2.8 Kuesioner

Kuesioner atau angket adalah instrument penelitian atau Teknik pengumpulan data dengan berupa daftar pernyataan atau pernyataan secara tertulis yang harus dijawab

3) Netral

4) Tidak Setuju

5) Sangat Tidak Setuju

c. Kombinasi Tertutup dan Terbuka

Kuesioner yang memberi jawaban yang sudah ditentukan namun ditambah dengan kolom pertanyaan tambahan yang terbuka. Contoh ;

Apakah warga Indonesia sudah menerapkan protocol Kesehatan selama covid 19 ini sesuai dengan anjuran pemerintah ?

- a. sudah sesuai
- b. belum sesuai

2. Kuesioner Berstruktur

- a. Kuesioner tertutup

Faktor penentu tingkat kesadaran keamanan informasi mahasiswa Fakultas Teknologi Industri Universitas Trisakti

Devi Febrita Sari Hoesadha, 2021

---