BAB I
PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Pada era industri 4.0 teknologi informasi sudah menjadi bagian dari kehidupan, perkembangan teknologi informasi tersebut tentunya banyak membawa perubahan yang berdampak positif bagi penggunanya seperti mempermudah dalam memperoleh suatu Informasi yang dibutuhkan setiap saat. Teknologi informasi sudah menjadi bagian dari kehidupan manusia salah satunya dalam bidang Pendidikan yakni pada kalangan mahasiswa. Dari banyaknya teknologi informasi yang masuk dalam kehidupan mahasiswa tentunya tidak akan bermanfaat banyak jika hanya dimiliki saja, teknologi informasi ini akan bermanfaat jika dapat di gunakan secara maksimal namun dibalik kemudahan teknologi informasi ini terdapat hal yang perlu diperhatikan dan di waspadai oleh mahasiswa dan dosen sehingga nantinya dapat mengurangi dampak negatif dalam proses pendidikan di Universitas Pendidikan Ganesha.

Universitas Pendidikan Ganesha atau yang sering disebut Undiksha merupakan salah satu universitas negeri terbesar di bali, Undiksha terletak di bali utara yang beralamat di Jalan Udayana, No 11, Kabupaten Buleleng, Bali. Undiksha memiliki banyak layanan sistem informasi dibidang akademik.

Undiksha memiliki sistem informasi bagi mahasiswa diantaranya E-Ganesha yang merupakan aplikasi yang dapat diakses melalui *mobile* ataupun *website*, aplikasi ini bertujuan untuk memberikan layanan akademik bagi mahasiswa dan dosen yang ada di undiksha, adapun layanan yang tersedia adalah *e-learning* undiksha, sistem informasi PPL, SIAK, Sistem Informasi PKL dan yang lainnya (Undiksha, 2019). Dalam penelitian (Kusumaningrum et al., 2022) menyebutkan bahwa dari sudut pandang Pendidikan tinggi juga telah dilakukan analisis terkait dengan perilaku keamanan siber yang dimana objek penelitiannya adalah perguruan tinggi yang berada di wilayah jawa tengah dengan mendapatkan hasil rata-rata 3,3 dari nilai total 5 untuk kerentanan siber serta dapat disimpulkan masuk pada kategori rentan, sedangkan variable yang digunakan pada penelitian

sebelumnya adalah berfokus pada penggunaan *password*, akses data dan informasi serta penggunaan perangkat internet. Adapun wawancara yang dilakukan terhadap Komang Pramayasa selaku korban dari kejahatan *cyber* menjelaskan bahwa awalnya sudah mengganti *password* pada salah satu sistem informasi yang digunakan dalam aktivitas perkuliahan namun pada saat tertentu setelah sekian lama sudah mengganti *password*nya korban mendapatkan *notifikasi* email bahwasannya terdapat seseorang yang sudah mengakses serta mengganti kembali *password*nya sehingga korban ingin melakukan login kedalam sistem informasi tersebut ternyata aksesnya ditolak karena korban mengira salah ketik dalam memasukkan *password* korban melakukan sebanyak beberapa kali namun hasilnya tidak dapat login kedalam sistem sehingga korban melaporkan kepada pihak UPT TIK selaku pemegang hak akses dari sistem informasi yang ada di undiksha sehingga korban dapat melakukan *reset password* serta mengubah *password*nya kembali, dari fenomena yang sudah di paparkan dapat disimpulkan bahwasannya serangan yang dialami oleh korban dapat dikatakan sebagai *Man in the Middel Attack* mengapa dari definisinya merupakan kejahatan yang memungkinkan peretas menempatkan dirinya berada di tengah-tengah percakapan para korban, dalam hal ini pelaku dapat melihat, mendengarkan serta menyamar sebagai salah satu pihak dan membuat terlihat seperti pertukaran informasi yang berlangsung dengan normal dapat di analogikan seperti seorang kurir pos korban ingin mengirimkan surat-surat penting yang berisikan identitas diri kemudian kurir membuka segel paket tanpa sepengetahuan dari pemiliknya dan mencatat informasi penting yang terdapat di dalam paket lalu kurir akan menyegel kembali paket dan mengirimkannya kembali sesuai tujuan dengan seolah-olah paket belum pernah dibuka sama sekali, dalam kasus ini juga dapat disimpulkan bahwa masih kurangnya kesadaran dari pengguna akan pentingnya keamanan informasi yang terdapat pada suatu sistem informasi serta mengganti kata sandi secara berkala serta dalam fenomena yang terjadi dapat merujuk ke aspek dasar *Confidentiality* karena suatu sistem harus menjamin bahwa mereka yang memiliki hak akses saja yang boleh melakukan akses kedalam sistem.

Adapun risiko yang perlu menjadi perhatian bagi mahasiswa dan dosen adalah mengenai layanan yang ada pada aplikasi E-Ganesha seperti halnya pada mahasiswa terdapat Pangkalan Data Mahasiswa (PDM) serta Sistem Informasi

Akademik (SIAK) yang dimana terdapat Informasi pribadi dan data keluarga yang berisikan Nomor Induk Keluarga hal ini jika di akses oleh pihak yang tidak bertanggung jawab dapat memicu penyalahgunaan terhadap data pribadi yang dapat merugikan pemilik akun. Sehingga perlu dilakukannya pengukuran terhadap pengguna baik mahasiswa atau pun dosen guna mengetahui bagaimana tingkat keamanan informasi yang ada di Universitas Pendidikan Ganesha.

Salah satu hal yang harus di waspadai adalah keamanan, terdapat banyak kasus yang terjadi berkaitan dengan keamanan Informasi seperti pencurian data, akses secara *illegal*, kebocoran informasi, serta *vandalisme*. Berdasarkan publikasi *International Telecommunication Union* (ITU) tahun 2021 menyebutkan bahwa Global Cyber Security Index Indonesia pada tahun 2020 indonesia berada pada peringkat 24 dari 194 negara. Pada tingkat regional indonesia menepati peringkat 6 di asia pasifik dan peringkat 3 di ASEAN setelah Singapura dan Malaysia berdasarkan keterangan pers BSSN (Badan Siber dan Sandi Negara). Hal ini menunjukkan bahwa kurangnya kesadaran masyarakat terhadap keamanan (CNN Indonesia, 2021). BSSN juga mempublish pada website resminya pada 30 Maret 2022 mengenai laporan tahunan hasil monitoring keamanan siber tahun 2021 yang menyatakan bahwa terdapat 1.6 miliar anomaly trafik yang masuk ke Indonesia dengan trafik tertinggi di bulan desember tahun 2021 adapun mayoritas dari trafik tersebut merupakan aktivitas malware serta runsomware, selain itu BSSN juga mempublish top 10 vulnerabilities yang diantaranya adalah: *Cross-Site Scripting (XSS), Clickjacking, Possible Brutrforce, Insecure Direct Object Reference (IDOR), SQL Injection, Unencrypted Comunnication, Cleartect Submission Password, Weak Password, Sensitive Data Exposure, Dan Directory Listing* (BSSN, 2022).

Adapun aspek keamanan Informasi yakni *Confidentiality, Integrity* dan *Availability. Confidentiality* merupakakan hanya mereka yang memiliki hak akses informasi tertentu, *Integrity* adalah memastikan bahwa Informasi tersebut akurat, utuh serta belum dimodifikasi oleh pihak yang tidak memiliki kepentingan, serta *Availability* adalah meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu Informasi. Perlu kesadaran yang tinggi bagi para mahasiswa dalam memanfaatkan suatu teknologi Informasi tersebut. Menurut Lenhart jejaring sosial

merupakan *sosial network* yang dimana penggunanya dapat membuat serta melakukan pengubahan terhadap sebuah profile dan jaringan personalnya sendiri yang dapat menghubungkan dengan pengguna lainnya (Lenhart & Madden, 2007).

Kurangnya kesadaran terhadap keamanan data milik pribadi di internet dapat memicu kejahatan yang semakin gencar di dunia maya, berdasarkan survei yang dilakukan oleh Avast terhadap 700 orang di Indonesia terdapat (35%) lebih orang di Indonesia tidak pernah mengganti kata sandi padahal sudah diperingati mengenai adanya pembobolan data atau peretasan, sedangkan sisanya (66.3%) pengguna hanya merubah kata sandi mereka pada website yang diretas akan tetapi tindakan pengubahan kata sandi terhadap akun lain tidak dilakukan (selular.id, 2017).

Keamanan Informasi dan privasi sangat penting guna mencegah terjadinya kejahatan akademik melalui jejaring online, intimidasi online terhadap gender, penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab, potensi pencemaran nama baik, hak kendali atas data pribadi, selain melakukan penetrasi test perlu dikalukan upaya pencegahan secara pribadi yang dilakukan oleh user guna melindungi data-data penting yang ada pada aplikasi mengingat pada masa sekarang aktivitas digital sangat meningkat (Kominfo.go.id, 2019)

Penelitian yang akan digunakan menggunakan pendekatan *Multiple Criteria Decision Analysis* (MCDA). Metode ini digunakan sebagai pengambilan keputusan atas dasar beberapa alternatif yang memiliki kriteria. Pendekatan MCDA dibedakan menjadi tiga kategori *1. Value measurement models*, 2. Model perengkingan, dan *3. Goal programing*. Pada penelitian ini menggunakan ketiga kategori diantaranya *value measurement models* yang artinya menggunakan pendekatan nilai, pendekatan ini didasari atas perhitungan nilai total dari masing-masing alternatif pada penelitian ini yang dimaksud adalah dimensi yang merupakan jumlah nilai total kriteria area kesadaran keamanan informasi (Amin, 2014)

Untuk mendapatkan data dalam penelitian ini menggunakan survei kuesioner dengan teknik pengambilan sampel secara acak berdasarkan area yang menyasar kepada mahasiswa dan dosen dilingkungan Universitas Pendidikan

Ganesha dimana dosen dan mahasiswa merupakan pengguna sistem informasi dalam aktivitas perkuliahan sehingga resikonya lebih tinggi. Setelah mendapatkan data selanjutnya melakukan pengukuran kesadaran dengan berpedoman pada konsep-konsep yang sudah dikemukakan oleh para ahli serta penelitian terdahulu yang relevan. Sebelum melakukan pengambilan data penulis akan melakukan uji instrument terlebih dahulu. Uji instrument merupakan penelitian yang menggunakan kuesioner sebagai skala pengukuran variable dari sebuah penelitian.

Berdasarkan latar belakang yang telah di uraikan maka diperlukan sebuah penelitian untuk mengetahui tingkat kesadaran keamanan Informasi dikalangan mahasiswa dan dosen di Universitas Pendidikan Ganesha maka penulis berinisiatif untuk melakukan penelitian dengan judul **"Pengukuran Kesadaran Keamanan Informasi Dan Privasi Menggunakan Metode *Multiple Criteria Decision Analysis* (MCDA) Di Universitas Pendidikan Ganesha"**

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang sudah dipaparkan adapun rumusan masalah yang diajukan dalam penelitian ini yaitu:

1. Bagaimana hasil pengukuran tingkat kesadaran keamanan informasi dan privasi menggunakan metode *Multiple Criteria Decision Analysis.*
2. Bagaimana rekomendasi dari hasil pengukuran tingkat kesadaran keamanan informasi dan privasi menggunakan metode *Multiple Criteria Decision Analysis.*

1.3 BATASAN MASALAH

Dalam penelitian ini penulis melakukan pembatasan masalah supaya pelaksanaan serta hasil yang nantinya diperoleh sesuai dengan tujuan pelaksanaan sebagaimana mestinya, Adapun Batasan masalah yang ditetapkan adalah sebagai berikut:

1. Responden yang digunakan dalam penelitian ini merupakan dosen dan mahasiswa di Universitas Pendidikan Ganesha dengan jumlah dosen sebanyak 56 orang serta mahasiswa berjumlah 144 orang

2. Pengukuran keamanan informasi dan privasi yaitu mengukur kesadaran keamanan secara umum
3. Pengukuran keamanan informasi dan privasi berfokus pada scope pengguna yakni dosen dan mahasiswa

1.4 TUJUAN PENELITIAN

Berdasarkan rumusan masalah diatas, adapun tujuan penelitian ini yaitu:

1. Untuk mengetahui hasil pengukuran tingkat kesadaran keamanan informasi dan privasi menggunakan metode *Multiple Criteria Decision Analysis*
2. Mengetahui rekomendasi yang akan disarankan berdasarkan hasil pengukuran tingkat kesadaran keamanan informasi dan privasi menggunakan metode *Multiple Criteria Decision Analysis.*

1.5 MANFAAT PENELITIAN

1. Bagi Peneliti

   Penelitian ini diharapkan dapat menjadi sarana dalam menerapkan kesadaran keamanan informasi penulis yang telah diterima dalam perkuliahan serta dapat menambah wawasan bagi penulis
2. Bagi Universitas Pendidikan Ganesha

   Hasil penelitian ini dapat digunakan oleh Universitas Pendidikan Ganesha kususnya bagi UPT TIK sebagai referensi pendukung keputusan serta penelitian ini dapat memberikan informasi untuk mengetahui tingkat kesadaran keamanan informasi mahasiswa dan dosen yang ada dilingkungan Universitas Pendidikan Ganesha