BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi informasi dalam beberapa tahun terakhir telah berkembang secara signifikan, memungkinkan setiap individu untuk memperoleh dan mengakses informasi secara luas melalui berbagai platform digital. Di balik berbagai manfaat yang ditawarkan, perkembangan ini juga membawa tantangan, khususnya dalam hal keamanan informasi. Salah satu permasalahan yang muncul adalah masih rendahnya tingkat literasi pengguna dalam melindungi data pribadi ketika menggunakan teknologi informasi (Islami & Candiwan, 2016). Kondisi ini juga berdampak pada lingkungan perguruan tinggi, di mana kesadaran sivitas akademika terhadap pentingnya menjaga keamanan informasi masih tergolong rendah.

Universitas Pendidikan Ganesha (Undiksha) adalah sebuah perguruan tinggi negeri yang bertugas untuk melatih sumber daya manusia yang profesional, baik dalam bidang pendidikan maupun bidang lainnya. Untuk membantu menciptakan lulusan yang berkualitas, Undiksha memiliki sarana dan fasilitas yang cukup, terutama di bidang teknologi informasi (Universitas Pendidikan Ganesha, 2019). Berbagai sistem informasi telah dikembangkan agar dapat mendukung kegiatan civitas akademika dalam proses belajar mengajar. Dengan adanya sistem tersebut, Undiksha dapat menyediakan layanan informasi secara efisien melalui internet, baik dari dalam kampus maupun dari luar kampus. Tugas pengelolaan dan pemeliharaan sistem informasi tersebut dilaksanakan oleh Unit Pengelola dan Administrasi Teknologi Informasi dan Komunikasi (UPA TIK) Undiksha.

Universitas Pendidikan Ganesha (Undiksha) memiliki beberapa sistem informasi yang digunakan untuk mempermudah kegiatan akademik para civitas akademika, seperti mahasiswa dan dosen. Beberapa layanan yang bisa digunakan oleh mahasiswa antara lain Sistem Informasi Akademik (SIAK), E-learning Undiksha, Pangkalan Data Mahasiswa (PDM), Sistem Informasi Kuliah Kerja Nyata (KKN), Sistem Informasi Praktik Kerja Lapangan (PKL), Sistem Informasi Program Pengalaman Lapangan

(PPL), serta layanan sistem informasi lainnya. Semua layanan tersebut tergabung dalam satu sistem SSO Undiksha. Untuk mengakses sistem tersebut, pengguna perlu memakai akun masing-masing. Akun ini terdiri dari nama pengguna (username) dan kata sandi (password) yang diberikan secara individu.

Hal yang sama juga berlaku bagi dosen, di mana setelah berhasil login melalui SSO Undiksha, pengguna akan diarahkan ke layanan yang sesuai dengan status kepegawaiannya, baik sebagai PNS, CPNS, maupun dosen kontrak. Namun, dalam proses akses layanan tersebut, terdapat sejumlah risiko yang perlu diwaspadai. Misalnya, pada akun mahasiswa, data penting dalam SIAK dan PDM sangat rentan jika tidak dilindungi dengan baik. Demikian pula bagi dosen, jika informasi login seperti username dan password jatuh ke tangan pihak yang tidak berwenang, maka data sensitif dalam sistem berisiko disalahgunakan, yang pada akhirnya dapat merugikan pemilik akun.

Selain itu, dalam proses pembelajaran daring, sistem E-learning Undiksha menjadi salah satu fasilitas utama yang sangat diandalkan. Namun, penggunaan sistem ini juga mengandung sejumlah risiko yang perlu diperhatikan, khususnya terkait dengan aspek keamanan informasi. Salah satu risiko yang umum terjadi adalah ketika civitas akademika mengakses sistem E-learning dari tempat umum atau menggunakan fasilitas publik tanpa memperhatikan langkah-langkah keamanan. Tidak jarang pengguna lupa untuk melakukan *logout* dari akun mereka, sehingga informasi seperti username tersimpan secara otomatis di perangkat yang digunakan. Dalam beberapa kasus, sistem secara otomatis juga mengisi password, sehingga memudahkan pihak lain untuk mengakses akun tersebut tanpa izin. Situasi ini dapat memicu berbagai bentuk ancaman keamanan informasi, seperti kebocoran data, pencurian identitas, hingga akses ilegal oleh pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan perhatian dan kesadaran yang lebih terhadap praktik keamanan digital saat menggunakan layanan pembelajaran daring.

Penggunaan perangkat umum seperti komputer dan perangkat mobile di lingkungan perguruan tinggi tidak hanya memberikan kemudahan dan efisiensi dalam menunjang aktivitas akademik, namun juga membawa potensi risiko terhadap

keamanan informasi yang perlu diwaspadai. Pemanfaatan perangkat bersama oleh mahasiswa, dosen, maupun tenaga kependidikan dapat meningkatkan kerentanan sistem, terutama jika tidak disertai dengan pemahaman yang memadai mengenai praktik keamanan informasi. Kondisi ini dapat membuka celah terhadap berbagai bentuk ancaman siber, yang pada akhirnya mengancam integritas, kerahasiaan, dan ketersediaan data institusi.

Pengukuran tingkat kesadaran keamanan informasi di lingkungan perguruan tinggi merupakan langkah krusial untuk mengidentifikasi berbagai permasalahan yang sering muncul, khususnya dalam penggunaan perangkat secara bersama-sama. Dalam penelitian ini, pengukuran kesadaran keamanan informasi dilakukan dengan mengacu pada tiga instrumen utama, yaitu *Risky Behavior Scale* (RBS), *Conservative Behavior Scale* (CBS), dan *Exposure Offense Scale* (EOS), yang masing-masing digunakan untuk menilai aspek perilaku, sikap, dan potensi pelanggaran terhadap keamanan informasi.

RBS merupakan instrumen penilaian berbasis skala Likert yang dirancang untuk mengukur perilaku berisiko di dunia digital, seperti pertemuan langsung dengan orang asing dari internet, mengakses konten eksplisit, penyalahgunaan media daring, serta tindakan menonaktifkan fitur keamanan seperti program penyaring konten (Khan, 2023). Sementara itu, CBS digunakan untuk menilai tingkat kehati-hatian pengguna dalam memanfaatkan sistem informasi (Candiwan, 2022). Sedangkan EOS digunakan untuk mengukur sejauh mana pengguna terpapar risiko keamanan digital sebagai akibat dari perilaku mereka sendiri (Candiwan, 2022).

Dalam pengukuran tingkat keamanan informasi, terdapat beberapa permasalahan penggunaan perangkat umum yang sering terjadi, meliputi 1). Penggunaan kata sandi yang lemah dapat memberikan celah bagi penyerang untuk melakukan upaya pencarian kata sandi atau serangan kekerasan kata sandi. 2). Berbagi informasi pribadi secara tidak aman, seperti seperti nomor mahasiswa atau kredensial login, tanpa mempertimbangkan risiko keamanan yang dapat meningkatkan risiko pencurian identitas atau akses tidak sah ke akun pribadi. 3). Mengunduh materi berpotensi berisiko, seperti mengunduh materi atau file dari internet yang berpotensi berisiko

terdapat perangkat lunak crack atau file yang terinfeksi malware. Hal tersebut, dapat membuka pintu bagi serangan malware atau virus yang dapat merugikan perangkat dan data pengguna. 4). Tidak memperbarui perangkat lunak secara teratur dapat membuat perangkat menjadi target potensial bagi serangan siber.

Penelitian ini bertujuan melihat tingkat kepedulian masyarakat akademika, seperti mahasiswa dan dosen, terhadap keamanan informasi. Untuk mengevaluasi hal ini, penelitian menggunakan tiga alat pengukuran, yaitu Risky Behavior Scale (RBS), Conservative Behavior Scale (CBS), dan Exposure Offense Scale (EOS). Penelitian fokus pada penerapan prinsip-prinsip keamanan informasi dalam penggunaan sistem E-Learning Undiksha di Universitas Pendidikan Ganesha. Tujuan utama penelitian ini adalah meningkatkan pemahaman dan kesadaran pengguna tentang pentingnya melindungi data dalam pengelolaan sistem informasi akademik. Hasil penelitian berharap dapat memberikan saran strategis, seperti menyelenggarakan pelatihan keamanan informasi secara rutin bagi mahasiswa dan dosen, serta menyebarkan materi pembelajaran melalui media yang mudah diakses, sehingga dapat membantu meningkatkan kesadaran tentang keamanan informasi di institusi pendidikan tinggi.

Selain itu, bekerja sama dengan para ahli di bidang keamanan informasi serta rutin melakukan evaluasi merupakan bagian penting dalam upaya memperkuat sistem keamanan informasi di lingkungan universitas. Dengan beberapa rekomendasi yang diharapkan dapat disusun, penelitian ini bertujuan untuk menciptakan ekosistem digital yang lebih aman dan mampu mengurangi risiko serangan siber di Universitas Pendidikan Ganesha. Berdasarkan latar belakang tersebut, peneliti memutuskan untuk melakukan penelitian dengan judul **"Pengukuran Tingkat Kesadaran Keamanan Informasi di Universitas Pendidikan Ganesha Menggunakan Model *Risky Behavior Scale* (RBS), *Conservative Behavior Scale* (CBS), dan *Exposure Offense Scale* (EOS)".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan sebelumnya, adapun rumusan masalah yang diperoleh sebagai berikut:

1. Bagaimana hasil dari pengukuran tingkat kesadaran keamanan informasi di Universitas Pendidikan Ganesha menggunakan model *Risky Behavior Scale* (RBS), *Conservative Behavior Scale* (CBS), dan *Exposure Offense Scale* (EOS)?
2. Bagaimana rekomendasi dari hasil pengukuran tingkat kesadaran keamanan informasi di Universitas Pendidikan Ganesha menggunakan model *Risky Behavior Scale* (RBS), *Conservative Behavior Scale* (CBS), dan *Exposure Offense Scale* (EOS)?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan diatas, adapun tujuan dari penelitian ini diantaranya:

1. Untuk mengetahui hasil pengukuran tingkat kesadaran keamanan informasi di Universitas Pendidikan Ganesha menggunakan model *Risky Behavior Scale* (RBS), *Conservative Behavior Scale* (CBS), dan *Exposure Offense Scale* (EOS)
2. Memberikan rekomendasi dari hasil pengukuran tingkat kesadaran keamanan informasi di Universitas Pendidikan Ganesha menggunakan model *Risky Behavior Scale* (RBS), *Conservative Behavior Scale* (CBS), dan *Exposure Offense Scale* (EOS)

1.4 Ruang Lingkup Penelitian

Pada penelitian ini penulis memberikan ruang lingkup penelitian agar dalam pelaksanaan dan hasil yang diperoleh nantinya sesuai dengan tujuan penelitian sebagaimana mestinya, adapun ruang lingkup penelitian yang ditetapkan adalah sebagai berikut:

1. Responden yang digunakan dalam penelitian ini mencangkup mahasiswa dan dosen dilingkungan Universitas Pendidikan Ganesha dengan jumlah mahasiswa sebanyak 120 orang, dan dosen sebanyak 48 orang
2. Penelitian ini dilakukan untuk mengukur tingkat kesadaran keamanan informasi mahasiswa dan dosen dilingkungan Universitas Pendidikan Ganesha

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Bagi Peneliti

   Penelitian ini diharapkan bisa menjadi sarana untuk menerapkan ilmu yang telah dipelajari selama kuliah, terutama dalam memahami lebih dalam mengenai konsep dan cara menerapkan keamanan informasi. Selain itu, kegiatan penelitian ini juga bisa membantu peneliti dalam meningkatkan kemampuan merancang metode, mengumpulkan dan menganalisis data, menafsirkan hasil, serta memberikan rekomendasi berdasarkan temuan yang diperoleh.

2. Bagi Universitas Pendidikan Ganesha

   Hasil dari penelitian ini dapat dijadikan rekomendasi oleh Universitas Pendidikan Ganesha khususnya bagi UPA TIK sebagai acuan referensi dalam merancang program pelatihan untuk meningkatkan pengetahuan akan kesadaran keamanan informasi terhadap pengguna mahasiswa dan dosen dilingkungan Universitas Pendidikan Ganesha.