LogicLink: Journal of Artificial Intelligence and Multimedia in Informatics
E-ISSN: 3062-9098 | P-ISSN: 3063-4504 | Vol. 3 No. 1, June 2026, pp. 59 – 67

Analisis Penguatan Tata Kelola Keamanan Informasi melalui Pengelolaan Kata Sandi

Nabil Surya Al Hakim[1], Abdul Majid*[2]
[1,2]Program Studi Sains Data, Universitas Islam Negeri K.H. Abdurrahman Wahid Pekalongan, Indonesia
*E-mail : abdul.majid@uingusdur.ac.id**
**Penulis Korespondensi*

Received 21 June 2026; Revised 6 July 2026; Accepted 7 July 2026

Abstrak - Pengelolaan kata sandi masih menjadi isu krusial dalam keamanan informasi digital karena perilaku pengguna dapat berkontribusi terhadap kebocoran kredensial, kompromi akun, dan akses tidak sah. Penelitian ini bertujuan menganalisis peran tata kelola data dalam memperkuat praktik pengelolaan kata sandi pada mahasiswa sebagai pengguna akun digital. Penelitian menggunakan pendekatan kuantitatif deskriptif dengan desain cross-sectional melalui kuesioner daring terhadap 50 responden yang dipilih menggunakan teknik purposive sampling. Data dianalisis menggunakan statistik deskriptif berupa frekuensi dan persentase. Hasil penelitian menunjukkan bahwa 46 responden (92%) pernah menggunakan kata sandi yang sama pada lebih dari satu akun, sedangkan hanya 4 responden (8%) yang tidak pernah menggunakan ulang kata sandi. Meskipun 33 responden (66%) sering atau selalu menggunakan kombinasi karakter yang kuat, indikator penggunaan password manager masih rendah karena 54% responden tidak pernah memanfaatkannya. Penerapan autentikasi dua faktor juga belum merata karena sebagian responden hanya menggunakannya pada beberapa akun atau belum menggunakannya sama sekali. Temuan ini menunjukkan bahwa praktik pengelolaan kata sandi belum sepenuhnya mencerminkan prinsip tata kelola data, khususnya kontrol akses, kerahasiaan, dan akuntabilitas. Oleh karena itu, diperlukan edukasi keamanan digital yang berkelanjutan, peningkatan literasi penggunaan password manager, penerapan autentikasi dua faktor, serta kebijakan akses institusional yang lebih jelas untuk memperkuat keamanan informasi digital.
Kata Kunci: Tata Kelola Data, Pengelolaan Kata Sandi, Keamanan Informasi, Kontrol Akses, Perilaku Pengguna.

Abstract - Password management remains a crucial issue in digital information security because user behavior can contribute to credential leakage, account compromise, and unauthorized access. This study aims to analyze the role of data governance in strengthening password management practices among university students as digital account users. The study employs a descriptive quantitative approach with a cross-sectional design using an online questionnaire administered to 50 respondents selected through purposive sampling. Data were analyzed using descriptive statistics in the form of frequencies and percentages. The results show that 46 respondents (92%) have used the same password for more than one account, while only 4 respondents (8%) have never reused a password. Although 33 respondents (66%) often or always use strong character combinations, the indicator of password manager use remains low, as 54% of respondents have never utilized one. The implementation of two-factor authentication is also uneven, as some respondents only apply it to a few accounts or do not use it at all. These findings indicate that password management practices do not yet fully reflect data governance principles, particularly in terms of access control, confidentiality, and

accountability. Therefore, continuous digital security education, enhanced literacy in the use of password managers, the implementation of two-factor authentication, and clearer institutional access policies are needed to strengthen digital information security.
Keywords: Data Governance, Password Management, Information Security, Access Control, User Behavior.

1. PENDAHULUAN

Perkembangan layanan digital telah meningkatkan ketergantungan pengguna terhadap akun daring dalam kegiatan pendidikan, pekerjaan, komunikasi, transaksi, dan layanan organisasi. Dalam konteks tersebut, perlindungan data dan keamanan akses menjadi kebutuhan penting karena akun digital sering kali menyimpan informasi pribadi maupun informasi organisasi. Salah satu mekanisme autentikasi yang masih banyak digunakan adalah kata sandi. Walaupun sederhana dan mudah diterapkan, kata sandi tetap berperan sebagai lapisan awal dalam membatasi akses terhadap sistem dan informasi digital (Stallings & Brown, 2018; Florêncio & Herley, 2007).

Permasalahan muncul ketika kata sandi tidak dikelola secara aman. Kebiasaan menggunakan kata sandi yang sama pada beberapa akun, menggunakan informasi pribadi sebagai kata sandi, menyimpan kredensial secara sembarangan, serta tidak mengaktifkan autentikasi tambahan dapat meningkatkan risiko kompromi akun (Aiswarya et al., 2022; Rajah et al., 2020). Laporan keamanan data menunjukkan bahwa faktor manusia dan penyalahgunaan kredensial masih menjadi bagian penting dalam insiden keamanan digital (Verizon Business, 2025; Addae et al., 2019). Dengan demikian, pengelolaan kata sandi bukan hanya persoalan teknis, tetapi juga berkaitan dengan perilaku pengguna dan tata kelola keamanan informasi (Addae et al., 2019; Huwaidi & Destya, 2022).

Tata kelola data (data governance) didefinisikan sebagai kerangka kebijakan, prosedur, standar, dan mekanisme akuntabilitas yang mengatur pengelolaan data sepanjang siklus hidupnya, mulai dari pengumpulan, penyimpanan, pemrosesan, hingga penghapusan (Khatri & Brown, 2010; Weber et al., 2009; DAMA International, 2017). Prinsip-prinsip utama tata kelola data meliputi akuntabilitas, transparansi, integritas, kerahasiaan, dan kepatuhan (DAMA International, 2017; Weber et al., 2009).

Dalam perspektif tata kelola data, akses terhadap informasi perlu diatur, dikendalikan, dan diawasi agar prinsip kerahasiaan, integritas, dan ketersediaan data dapat terjaga (Stallings & Brown, 2018; ENISA, 2019). Kata sandi merupakan salah satu komponen kontrol akses yang menentukan siapa yang dapat masuk ke dalam sistem atau layanan digital tertentu. Pengelolaan kata sandi tidak dapat dipisahkan dari tata kelola data karena kata sandi berfungsi sebagai pelindung (gatekeeper) aset data dari akses tidak sah (Khatri & Brown, 2010; Bertino & Takahashi, 2011). Tata kelola data memengaruhi kontrol akses melalui penetapan kebijakan identitas dan autentikasi (identity and access management), standar kompleksitas kata sandi, kebijakan penggantian kata sandi, serta penerapan autentikasi multifaktor (National Institute of Standards and Technology, 2025; ENISA, 2019). Apabila pengelolaan kata sandi dilakukan secara lemah, maka kontrol akses juga menjadi lemah dan berpotensi membuka peluang akses tidak sah terhadap data. Penguatan kontrol akses juga sejalan dengan kebutuhan tata kelola keamanan informasi berbasis standar seperti ISO/IEC 27001 (Utomo et al., 2012).

Dalam teori keamanan informasi digital, dikenal tiga pilar utama yaitu CIA triad: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan) (Stallings & Brown, 2018). Kata sandi berperan penting dalam melindungi kerahasiaan data dengan memastikan hanya pengguna yang berwenang yang dapat mengakses informasi. Selain itu,

manajemen identitas dan akses (identity and access management/IAM) merupakan komponen fundamental dalam keamanan informasi yang mengatur siklus hidup identitas digital, termasuk autentikasi, otorisasi, dan audit akses (Bertino & Takahashi, 2011; ENISA, 2019).

Penelitian sebelumnya telah membahas risiko penggunaan kata sandi lemah, kesadaran keamanan informasi, autentikasi dua faktor, dan perlindungan data pribadi (Rajah et al., 2020; Yamin et al., 2023; Huwaidi & Destya, 2022). Namun, pembahasan mengenai pengelolaan kata sandi sebagai bagian dari tata kelola data masih perlu diperkuat. Sebagian kajian masih memisahkan aspek perilaku pengguna dan aspek tata kelola data, padahal keduanya saling berkaitan dalam membangun keamanan informasi digital (Addae et al., 2019; Pearman et al., 2019). Oleh karena itu, penelitian ini menempatkan password management sebagai bagian dari data governance yang berhubungan dengan kontrol akses, akuntabilitas, dan budaya keamanan digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis praktik pengelolaan kata sandi pada mahasiswa pengguna akun digital serta menilai keterkaitannya dengan prinsip tata kelola data. Mahasiswa dipilih sebagai subjek penelitian karena memiliki intensitas penggunaan layanan digital yang tinggi dalam aktivitas akademik maupun nonakademik, serta mewakili generasi pengguna aktif yang rentan terhadap risiko keamanan digital (Nurjanah & Destya, 2022). Secara khusus, penelitian ini mengkaji penggunaan ulang kata sandi, kompleksitas kata sandi, frekuensi penggantian kata sandi, pengetahuan dan penggunaan password manager, penerapan autentikasi dua faktor, pengalaman kompromi akun, serta persepsi tanggung jawab pengguna terhadap keamanan akun digital.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan desain cross-sectional survey. Pendekatan kuantitatif deskriptif dipilih karena penelitian ini bertujuan menggambarkan praktik pengelolaan kata sandi, tingkat kesadaran keamanan informasi, penggunaan alat bantu keamanan, serta persepsi pengguna terhadap tata kelola data dalam perlindungan akun digital. Desain survei potong lintang digunakan karena data dikumpulkan pada satu periode tertentu, sehingga hasil penelitian menggambarkan kondisi dan perilaku responden pada saat pengisian kuesioner dilakukan.

2.2 Populasi dan Sampel

Populasi target dalam penelitian ini adalah mahasiswa Fakultas Sains dan Teknologi (Saintek) UIN K.H. Abdurrahman Wahid Pekalongan yang menggunakan akun digital secara aktif, mencakup layanan seperti email, media sosial, e-learning, penyimpanan awan, marketplace, dan berbagai layanan berbasis web lainnya. Mahasiswa Fakultas Saintek dipilih sebagai subjek penelitian karena memiliki intensitas penggunaan layanan digital yang tinggi dalam aktivitas akademik maupun nonakademik, sehingga berpotensi menghadapi berbagai risiko keamanan informasi.

Sampel penelitian terdiri atas 50 mahasiswa Fakultas Saintek UIN K.H. Abdurrahman Wahid Pekalongan yang ditentukan menggunakan teknik nonprobability purposive sampling. Pemilihan sampel didasarkan pada kriteria inklusi berikut: (1) berstatus mahasiswa aktif Fakultas Saintek, (2) menggunakan minimal satu akun digital dalam keseharian, (3) memahami penggunaan kata sandi sebagai mekanisme autentikasi, (4) bersedia berpartisipasi secara sukarela setelah mendapatkan penjelasan mengenai penelitian, dan (5) mengisi seluruh pertanyaan kuesioner secara lengkap.

2.3 Instrumen Penelitian

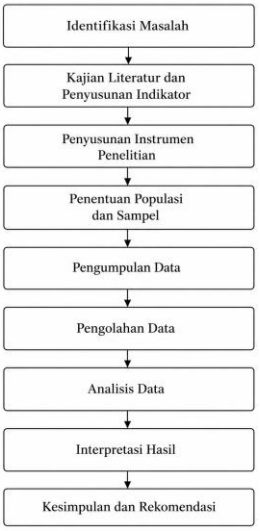
Instrumen penelitian yang digunakan berupa kuesioner daring (online). Kuesioner disusun berdasarkan indikator pengelolaan kata sandi dan tata kelola keamanan informasi. Indikator tersebut mencakup: penggunaan ulang kata sandi, bentuk dan kompleksitas kata sandi, frekuensi penggantian kata sandi, pengetahuan dan penggunaan password manager, penggunaan autentikasi dua faktor, pengalaman kompromi akun, serta persepsi responden mengenai tanggung jawab keamanan akun digital. Selain itu, kuesioner memuat butir-butir yang berkaitan dengan prinsip tata kelola data, khususnya kontrol akses, kerahasiaan informasi, akuntabilitas pengguna, dan budaya keamanan digital.

2.4 Prosedur Pengumpulan Data

Pengumpulan data dilakukan secara daring melalui formulir online yang disebarkan kepada responden menggunakan media sosial dan platform komunikasi mahasiswa. Sebelum mengisi kuesioner, responden diberikan penjelasan mengenai tujuan penelitian, sifat sukarela partisipasi, serta bahwa data yang dikumpulkan hanya digunakan untuk kepentingan akademik. Untuk menjaga keamanan dan privasi responden, kuesioner tidak meminta kata sandi asli, nama akun, nomor identitas, maupun informasi sensitif lainnya. Data yang dihimpun sebatas kebiasaan umum responden dalam mengelola kata sandi dan memanfaatkan fitur keamanan pada akun digital yang digunakan.

Tahapan penelitian dilakukan secara sistematis sejak identifikasi masalah hingga penyusunan kesimpulan dan rekomendasi. Alur penelitian diawali dengan identifikasi permasalahan terkait lemahnya praktik pengelolaan kata sandi dalam konteks keamanan informasi digital. Selanjutnya, peneliti melakukan kajian literatur dan merumuskan indikator penelitian berdasarkan konsep tata kelola data, kontrol akses, keamanan informasi, dan perilaku pengguna.

Tahap berikutnya adalah penyusunan instrumen penelitian dalam bentuk kuesioner daring yang mengacu pada indikator tersebut. Setelah instrumen selesai disusun, peneliti menetapkan populasi dan sampel sesuai kriteria yang telah ditentukan. Data kemudian dikumpulkan melalui penyebaran kuesioner, diperiksa kelengkapannya, dan diolah menggunakan statistik deskriptif. Hasil analisis selanjutnya diinterpretasikan berdasarkan prinsip keamanan informasi dan tata kelola data, kemudian dirangkum dalam bentuk kesimpulan serta rekomendasi yang mendukung penguatan praktik pengelolaan kata sandi. Alur tahapan penelitian disajikan pada Gambar 1.



Gambar 1. Alur metode penelitian

2.5 Teknik Analisis Data

Data yang terkumpul diperiksa kelengkapannya sebelum dianalisis. Jawaban yang tidak lengkap tidak dimasukkan ke dalam proses analisis. Data dianalisis menggunakan statistik deskriptif berupa frekuensi dan persentase. Teknik analisis ini digunakan untuk mengetahui distribusi jawaban responden pada setiap indikator penelitian. Hasil analisis disajikan dalam bentuk tabel, diagram, dan narasi interpretatif agar pola perilaku responden dapat dijelaskan secara jelas.

Rumus persentase yang digunakan dalam penelitian ini adalah:

$$P = \left(\frac{f}{N}\right) \times 100\%$$

Keterangan:

P adalah persentase jawaban responden

f adalah frekuensi jawaban pada kategori tertentu, dan

N adalah jumlah seluruh responden.

Interpretasi hasil dilakukan dengan mengaitkan temuan penelitian dengan prinsip keamanan informasi dan tata kelola data. Praktik penggunaan ulang kata sandi, penggunaan kata sandi yang lemah, rendahnya pemanfaatan password manager, dan belum optimalnya autentikasi dua faktor dianalisis sebagai faktor yang dapat memengaruhi efektivitas kontrol akses dan perlindungan data digital. Sebaliknya, penggunaan kata sandi yang kuat, penggunaan password manager, dan penerapan autentikasi dua faktor dipahami sebagai bentuk praktik keamanan yang mendukung tata kelola akses digital.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Penelitian

Hasil penelitian menunjukkan bahwa praktik pengelolaan kata sandi pada responden masih memiliki beberapa kelemahan. Aspek yang dianalisis meliputi penggunaan ulang kata sandi, bentuk kata sandi, frekuensi penggantian kata sandi, pengetahuan password manager, penerapan autentikasi dua faktor, pengalaman diretas, serta persepsi mengenai pihak yang bertanggung jawab terhadap keamanan akun digital. Ringkasan hasil penelitian ditampilkan pada Tabel 1.

Temuan paling menonjol adalah tingginya penggunaan ulang kata sandi. Sebanyak 46 responden atau 92,0% pernah menggunakan kata sandi yang sama pada lebih dari satu akun. Praktik ini menunjukkan adanya konsentrasi risiko. Jika satu akun mengalami kebocoran kredensial, akun lain yang menggunakan kata sandi sama berpotensi ikut terdampak. Dari sudut pandang tata kelola data, kondisi ini menunjukkan bahwa kontrol akses belum dikelola secara optimal pada tingkat pengguna.

Dari sisi bentuk kata sandi, 33 responden atau 66,0% sudah sering atau selalu menggunakan kombinasi karakter kuat. Hal ini menunjukkan adanya kesadaran awal mengenai pentingnya kompleksitas kata sandi. Namun, masih terdapat 8 responden atau 16,0% yang menggunakan pola lemah atau mudah ditebak. Temuan ini memperlihatkan bahwa sebagian pengguna masih membutuhkan edukasi mengenai karakteristik kata sandi yang aman dan risiko penggunaan informasi pribadi sebagai kata sandi.

Frekuensi penggantian kata sandi menunjukkan variasi perilaku. Sebanyak 25 responden atau 50,0% mengganti kata sandi lebih dari enam bulan sekali, sedangkan 7 responden atau 14,0% tidak pernah mengganti kata sandi. Penggantian kata sandi memang tidak selalu harus dilakukan secara berkala tanpa alasan, tetapi pengguna perlu mengganti kata sandi ketika terdapat indikasi kebocoran, aktivitas mencurigakan, atau penggunaan kata sandi yang lemah.

Tabel 1. Ringkasan hasil penelitian pengelolaan kata sandi

No.	Indikator	Hasil
1	Penggunaan ulang kata sandi	46 responden (92,0%) pernah menggunakan kata sandi yang sama pada lebih dari satu akun; 4 responden (8,0%) tidak pernah menggunakan ulang kata sandi.
2	Bentuk kata sandi	33 responden (66,0%) sering atau selalu menggunakan kombinasi karakter kuat; 9 responden (18,0%) berada pada kategori cukup; 8 responden (16,0%) masih menggunakan pola lemah atau mudah ditebak.
3	Frekuensi penggantian kata sandi	25 responden (50,0%) mengganti kata sandi lebih dari enam bulan sekali; 7 responden (14,0%) mengganti 3-6 bulan sekali; 7 responden (14,0%) mengganti saat ada masalah; 7 responden (14,0%) tidak pernah mengganti; 4 responden (8,0%) mengganti kurang dari tiga bulan sekali.
4	Pengetahuan password manager	25 responden (50,0%) mengetahui password manager; 9 responden (18,0%) hanya pernah mendengar; 16 responden (32,0%) tidak mengetahui password manager.
5	Penggunaan password manager	5 responden (10,0%) menggunakan secara rutin; 8 responden (16,0%) kadang-kadang; 10 responden (20,0%) pernah mencoba; 27 responden (54,0%) tidak pernah menggunakan.
6	Penggunaan autentikasi dua faktor	6 responden (12,0%) menggunakan pada semua akun penting; 24 responden (48,0%) menggunakan pada beberapa akun; 4 responden (8,0%) pernah tetapi tidak aktif; 13 responden (26,0%) tidak pernah menggunakan; 3 responden (6,0%) tidak tahu.
7	Pengalaman diretas	9 responden (18,0%) pernah mengalami peretasan; 35 responden (70,0%) tidak pernah; 6 responden (12,0%) tidak yakin.
8	Pihak yang dianggap bertanggung jawab	36 responden (72,0%) menilai diri sendiri paling bertanggung jawab; 5 responden (10,0%) menunjuk kampus atau organisasi; 4 responden (8,0%) penyedia layanan; 4 responden (8,0%) pemerintah atau regulasi; 1 responden (2,0%) tidak tahu.

Pengetahuan dan penggunaan password manager masih belum optimal. Meskipun 25 responden atau 50,0% mengetahui password manager, sebanyak 27 responden atau 54,0% tidak pernah menggunakan alat tersebut. Hal ini menunjukkan adanya kesenjangan antara pengetahuan dan praktik. Pengguna mungkin mengetahui istilah password manager, tetapi belum memahami manfaat, cara penggunaan, atau tingkat keamanannya. Penggunaan autentikasi dua faktor juga belum merata. Sebanyak 30 responden atau 60,0% menggunakan autentikasi dua faktor pada semua atau beberapa akun penting, tetapi masih terdapat responden yang tidak pernah menggunakannya atau tidak mengetahui fitur tersebut. Padahal, autentikasi dua faktor dapat menjadi lapisan keamanan tambahan ketika kata sandi diketahui pihak lain.

Hasil penelitian menunjukkan bahwa pengelolaan kata sandi oleh responden belum sepenuhnya mencerminkan praktik keamanan informasi yang baik. Tingginya penggunaan ulang kata sandi menjadi indikator bahwa faktor kemudahan masih lebih dominan dibandingkan pertimbangan risiko keamanan. Dalam konteks banyaknya akun digital yang digunakan mahasiswa, pengguna cenderung memilih kata sandi yang mudah diingat dan dapat dipakai pada beberapa layanan sekaligus. Namun, kebiasaan tersebut meningkatkan risiko credential stuffing, yaitu penyalahgunaan kredensial yang bocor dari satu layanan untuk mencoba masuk ke layanan lain (Rajah et al., 2020; Aiswarya et al., 2022; Florêncio & Herley, 2007). Temuan ini sejalan dengan kajian Aiswarya et al. (2022) dan Rajah et al. (2020) yang menunjukkan bahwa perilaku penggunaan ulang kata sandi berkaitan dengan risiko kebocoran data pribadi.

Temuan ini memperlihatkan pentingnya memandang kata sandi sebagai bagian dari tata kelola data. Dalam tata kelola data, kontrol akses tidak hanya ditentukan oleh sistem, tetapi juga oleh kepatuhan pengguna terhadap praktik keamanan (Khatri & Brown, 2010; Weber et al., 2009). Penggunaan kata sandi yang sama pada banyak akun menunjukkan bahwa kontrol akses pada tingkat individu masih lemah. Oleh karena itu, kebijakan keamanan informasi tidak cukup hanya memberikan anjuran umum, tetapi perlu disertai standar pengelolaan kredensial, edukasi praktis, dan dukungan teknologi seperti password manager (DAMA International, 2017; ENISA, 2019).

Kesenjangan antara pengetahuan dan praktik terlihat pada penggunaan password manager. Sebagian responden mengetahui password manager, tetapi tidak menggunakannya.

Hal ini menunjukkan bahwa literasi keamanan digital perlu diarahkan pada kemampuan praktis, bukan hanya pemahaman konseptual (Pearman et al., 2019). Edukasi tentang password manager sebaiknya mencakup cara memilih aplikasi yang aman, cara menyimpan master password, cara membuat kata sandi unik, dan risiko menyimpan kata sandi di catatan biasa atau pesan pribadi. Hal ini sejalan dengan Pearman et al. (2019) yang menemukan bahwa adopsi password manager dipengaruhi oleh pemahaman pengguna dan kenyamanan penggunaan.

Penerapan autentikasi dua faktor yang belum merata juga menjadi perhatian penting. Autentikasi dua faktor dapat memperkuat keamanan akun karena akses tidak hanya bergantung pada kata sandi (National Institute of Standards and Technology, 2025; ENISA, 2019). Pedoman NIST menekankan pentingnya pengelolaan autentikator dan perlindungan kredensial dalam keamanan identitas digital (National Institute of Standards and Technology, 2025). Dari perspektif tata kelola data, penggunaan autentikasi tambahan dapat dipahami sebagai bagian dari kontrol akses berlapis. Institusi pendidikan sebaiknya mendorong aktivasi autentikasi dua faktor pada akun yang menyimpan data penting, seperti email kampus, sistem akademik, penyimpanan cloud, dan platform pembelajaran daring.

Mayoritas responden menilai bahwa diri sendiri merupakan pihak paling bertanggung jawab terhadap keamanan akun digital. Temuan ini positif karena menunjukkan adanya kesadaran akuntabilitas individu. Namun, tanggung jawab keamanan tidak seharusnya hanya dibebankan kepada pengguna. Institusi, penyedia layanan, dan pembuat kebijakan juga memiliki peran dalam menyediakan sistem yang aman, kebijakan akses yang jelas, dan edukasi keamanan yang berkelanjutan (Addae et al., 2019; ENISA, 2019). Dengan demikian, tata kelola kata sandi perlu dibangun melalui kerja sama antara individu, institusi, dan sistem teknologi.

4. KESIMPULAN

Berdasarkan hasil survei terhadap 50 responden, penelitian ini menegaskan bahwa pengelolaan kata sandi masih menjadi aspek krusial sekaligus tantangan utama dalam menjaga keamanan informasi digital di kalangan mahasiswa. Mayoritas responden masih menggunakan kata sandi yang sama pada lebih dari satu akun, sehingga meningkatkan risiko berantai ketika terjadi kebocoran kredensial pada salah satu layanan. Meskipun sebagian mahasiswa telah menerapkan kombinasi karakter yang kuat, praktik keamanan pendukung seperti penggunaan password manager dan autentikasi dua faktor belum diadopsi secara luas, sehingga menunjukkan adanya kesenjangan antara tingkat kesadaran keamanan digital dan perilaku aman dalam penggunaan akun sehari-hari.

Dalam perspektif tata kelola data, kata sandi tidak hanya berfungsi sebagai mekanisme autentikasi teknis, tetapi juga sebagai bagian integral dari kontrol akses yang berkontribusi terhadap terjaganya kerahasiaan, integritas, dan perlindungan informasi digital. Pengelolaan kata sandi yang lemah membuka peluang terjadinya akses tidak sah, penyalahgunaan akun, dan kebocoran data, sehingga perlu diposisikan sebagai isu tata kelola keamanan informasi yang menuntut keterlibatan simultan dari pengguna, institusi, dan pembuat kebijakan. Penelitian ini memiliki keterbatasan pada penggunaan teknik purposive sampling dan pengumpulan data melalui kuesioner daring, sehingga temuan tidak dapat digeneralisasi secara luas dan sangat bergantung pada kejujuran serta pemahaman responden. Namun demikian, hasil yang diperoleh tetap memberikan gambaran awal yang bernilai mengenai praktik pengelolaan kata sandi pada mahasiswa dan dapat dijadikan landasan untuk merumuskan intervensi peningkatan literasi keamanan digital dan penguatan tata kelola akses.

Oleh karena itu, penelitian ini memberikan kontribusi praktis berupa penekanan pentingnya peningkatan literasi keamanan digital secara berkelanjutan, penguatan pemahaman dan pemanfaatan password manager, perluasan penerapan autentikasi dua faktor pada akun-

akun kritis, serta penyusunan kebijakan pengelolaan akses yang lebih sistematis di lingkungan pendidikan. Dengan langkah-langkah tersebut, pengelolaan kata sandi dapat diarahkan bukan sekadar sebagai kebiasaan individu, tetapi sebagai bagian dari budaya keamanan digital yang mendukung perlindungan data secara lebih efektif.

DAFTAR PUSTAKA

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction, 29(3*), 701–750. https://doi.org/10.1007/s11257-019-09236-5

Aiswarya, R., Jayasree, R., & Vijayanand, B. (2022). Behavioral attributes in password reuse: Analysis of password practices in work and personal spaces. In *Proceedings of the 13th Indian Conference on Human-Computer Interaction (India HCI 2022)* (pp. 1–19). ACM. https://doi.org/10.1145/3570211.3570212

Bertino, E., & Takahashi, K. (2011). *Identity management: Concepts, technologies, and systems*. Artech House.

Bonneau, J., Preibusch, S., & Anderson, R. (2012). A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *Financial Cryptography and Data Security* (pp. 25–40). Springer. https://doi.org/10.1007/978-3-642-32946-3_3

DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications.

ENISA. (2017). *Technical guidelines for the implementation of minimum security measures for digital service providers*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW 2007)* (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661

Huwaidi, M. Z., & Destya, S. (2022). Mencegah serangan rekayasa sosial dengan human firewall. *JUSTIN: Jurnal Sistem dan Teknologi Informasi, 10*(1), 107–112. https://doi.org/10.26418/justin.v10i1.44280

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

National Institute of Standards and Technology. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST SP 800-63B-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4

Nurjanah, D., & Destya, S. (2022). Pengukuran tingkat kesadaran keamanan informasi mahasiswa pada pembelajaran online. *JUSTIN: Jurnal Sistem dan Teknologi Informasi, 10*(1), 81–85. https://doi.org/10.26418/justin.v10i1.44362

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people don't use password managers effectively. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 319–338).

Rajah, P. R. S., Dastane, O., Bakon, K. A., & Johari, Z. (2020). The effect of bad password habits on personal data breach. *International Journal of Emerging Trends in Engineering Research, 8*(10), 6950–6960. https://doi.org/10.30534/ijeter/2020/538102020

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Utomo, M., Ali, A. H. N., & Affandi, I. (2012). Pembuatan tata kelola keamanan informasi kontrol akses berbasis ISO/IEC 27001:2005 pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS, 1*(1), 288–293.

Verizon Business. (2025). *Data Breach Investigations Report*. Verizon Business.

Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all—A contingency approach to data governance. *ACM Journal of Data and Information Quality, 1*(1), 1–27. https://doi.org/10.1145/1515693.1515696

Yamin, M., Malethi, T. T., Monica, J., & Natali, S. (2023). Evaluasi risiko pada penggunaan password yang lemah: Analisis kasus penggunaan password umum. *Jurnal Ilmiah Multidisiplin Ilmu Komputer, 1*(1), 41–48. https://doi.org/10.61674/jimik.v1i1.112