



Tantangan Sistem Keamanan Rekod Elektronik di Era Disrupsi Digital

¹Aviazka Firdhaussi Azmir, ²Nina Mayesti

^{1,2}Fakultas Ilmu Pengetahuan Budaya, Universitas Indonesia

ABSTRACT

The development of technology and information in the digital disruption era impacts the human need for information. As a consequence of the information explosion, many businesses are investing in technology to manage the increasing number of documents or records in their organizations. However, easy access to electronic records and flexibility in converting, distributing, and duplicating documents pose challenges, especially in the record security system, which can be caused by internal or external errors. So it is necessary to know what are the challenges related to the electronic record security system faced by record managers and archivists in the era of digital disruption. This study uses a descriptive approach with a literature study method. It was found that the challenges of the electronic record security system in the era of digital disruption include maintaining record accessibility, security related to data transfer or record distribution, maintaining the authenticity or authenticity of records, security related to record preservation, security of storage locations, and security related to fraud or theft. By knowing the challenges, it is hoped that the record manager can seize the opportunities to set strategies for maintaining security, monitoring, and minimizing risks.

INTISARI

Perkembangan teknologi dan informasi di era disrupsi digital berimbas pada meningkatnya kebutuhan manusia akan informasi. Sebagai konsekuensi dari ledakan informasi, banyak bisnis yang berinvestasi pada teknologi untuk mengelola peningkatan jumlah dokumen atau rekod di organisasinya. Namun kemudahan mengakses rekod elektronik dan fleksibilitas dalam pengubahan, pendistribusian, hingga penggandaan dokumen, memiliki tantangan terutama pada sistem keamanan rekod yang dapat disebabkan oleh kesalahan internal maupun eksternal. Sehingga perlu untuk mengetahui apa saja tantangan terkait sistem keamanan rekod elektronik yang dihadapi oleh pengelola rekod maupun arsiparis di era disrupsi digital. Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur. Ditemukan bahwa tantangan sistem keamanan rekod elektronik di era disrupsi digital diantaranya adalah menjaga aksesibilitas rekod, keamanan terkait transfer data atau distribusi rekod, menjaga keaslian atau autentisitas rekod, keamanan terkait preservasi rekod, keamanan lokasi penyimpanan, dan keamanan terkait pencegahan terhadap fraud atau pencurian. Dengan mengetahui tantangan yang ada diharapkan pengelola rekod dapat menangkap peluang yang ada untuk mengatur strategi dalam menjaga keamanan, memberikan pengawasan dan meminimalisir risiko yang dapat terjadi.

Submitted: 08/08/2022
Received: 25/03/2023



*Correspondence:

Aviazka Firdhaussi Azmir
aviazka.firdhaussi@ui.ac.id

KEYWORDS:

digital disruption

electronic records

electronic records
management system

security systems

KATA KUNCI:

disrupsi digital

rekod elektronik

sistem manajemen
rekod elektronik

sistem keamanan

CITE THIS ARTICLE:

Azmir, A. F. & Mayesti, N. (2022). Tantangan Sistem Keamanan Rekod Elektronik Di Era Disrupsi Digital *Diplomatika: Jurnal Kearsipan Terapan*, 5(2), 111-119. <http://dx.doi.org/10.22146/diplomatika.76948>

PENDAHULUAN

Disrupsi digital memungkinkan munculnya model bisnis baru sebagai bentuk evolusi yang ditandai dengan berakhirnya siklus hidup pada model bisnis tertentu. Hal ini disebabkan oleh berkembangnya paradigma baru seperti *cloud*, *big data*, dan revolusi industri 4.0 (Linz et al., 2017). Mengadopsi teknologi digital baru menghasilkan perubahan substansial dalam proses bisnis, organisasi, domain bisnis, dan masyarakat sebagai pengaruh dari perubahan model bisnis dan lingkungan operasinya (Parviainen et al., 2017).

Perkembangan teknologi dan informasi di era disrupsi digital ini juga berimbas pada meningkatnya kebutuhan manusia akan informasi. Informasi berperan penting dalam organisasi baik sebagai pengetahuan maupun membantu dalam proses pengambilan keputusan. Pemanfaatan teknologi dalam pengelolaan informasi memicu munculnya berbagai macam dokumen dan jenis media yang digunakan untuk memudahkan organisasi dalam menyimpan, mencari, dan menyebarkan informasi. Sebagai konsekuensi dari ledakan informasi saat ini, banyak bisnis yang berinvestasi pada teknologi untuk mengelola peningkatan jumlah dokumen atau rekod di organisasinya (Read et al., 2015).

Seiring dengan kemajuan teknologi, rekod elektronik yang digunakan saat ini merupakan konten yang dapat dibaca oleh mesin. Tantangan bagi pengelola rekod adalah memastikan bahwa semua rekod yang dimiliki dapat diakses dengan mudah ketika dibutuhkan. Namun kemudahan mengakses rekod elektronik dan fleksibilitas dalam pengubahan, pendistribusian, hingga penggandaan dokumen, menyebabkan ancaman terutama pada sistem keamanan rekod yaitu kesalahan (*failure*) pada perangkat yang digunakan maupun kesalahan yang disebabkan oleh sumber daya manusia. Ancaman keamanan rekod tidak hanya berasal dari kegiatan internal namun dapat juga dapat berasal dari pihak eksternal berupa tindakan kriminal seperti penipuan (*fraud*), peretasan (*hacking*), hingga pencurian data. Peningkatan penipuan dan pencurian data pada rekod elektronik menjadi suatu tantangan bagi pengelola rekod atau arsiparis untuk memastikan keselamatan dan keamanan rekod yang merupakan sumber daya berharga bagi organisasi.

Pengelolaan rekod elektronik dengan sistem keamanan yang tidak sesuai memungkinkan risiko hilangnya dokumen atau rekod hingga kebocoran informasi yang tentunya akan sangat merugikan organisasi. Sehingga sistem keamanan rekod elektronik yang tepat perlu diterapkan untuk mengelola dan memelihara rekod agar tetap autentik dan terhindar dari tindakan kejahatan dunia maya (*cybercrime*). Pada beberapa organisasi, pengelolaan rekod elektronik menghadapi beberapa isu terkait kurangnya kebijakan yang ditetapkan, serta kurangnya dukungan dari personil yang berkualitas dan berpengalaman.

Salah satu cara pengelolaan rekod elektronik dapat dilakukan dengan mengadopsi sistem manajemen rekod berbasis elektronik seperti *Electronic Records Management System (ERMS)* (Mukred et al., 2020). *International Council on Archives: Principles and Functional Requirements for Records* memberikan kriteria persyaratan terhadap penerapan ERMS, yaitu harus memastikan efektivitas proses pengelolaan rekod dengan tetap memelihara *authenticity*, *reliability*, *integrity*, dan *usability*.

Penelitian ini dilakukan untuk mengetahui apa saja tantangan terkait sistem keamanan rekod elektronik yang dihadapi di era disrupsi digital. Dengan mengetahui tantangan yang ada diharapkan pengelola rekod dapat menangkap peluang untuk mengatur strategi dalam menjaga keamanan rekod elektronik serta meminimalisir

risiko yang dapat terjadi.

TINJAUAN PUSTAKA

Rekod

Menurut ISO 15489-1:2016, rekod merupakan informasi yang diciptakan, dipelihara dan dikelola sebagai bukti dan aset organisasi atau perseorangan dalam melaksanakan kewajiban hukum atau dalam transaksi pekerjaan. Disebutkan pula bahwa rekod mendokumentasikan setiap kejadian atau transaksi atau membentuk himpunan yang telah dirancang untuk merekam proses, aktivitas atau fungsi kerja.

Dalam pedoman *International Council on Archives: Principles and Functional Requirements for Records* disebutkan bahwa rekod bukan hanya kumpulan data, tetapi merupakan konsekuensi atau produk dari suatu peristiwa terkait dengan kegiatan bisnis. Sebuah rekod harus berisi informasi hasil dari kegiatan atau operasional bisnis dalam bentuk tetap dan sah. Menurut ISO 15489-1:2016, suatu dokumen dapat dikatakan sebagai rekod jika karakteristik sebagai berikut:

1. Keautentikan (*Authenticity*)

Rekod yang autentik adalah rekod yang dapat dibuktikan sesuai dengan tujuan aslinya, telah diciptakan atau dikirimkan oleh pihak yang benar-benar menciptakan atau mengirimnya, dan diciptakan atau dikirimkan sesuai dengan tujuannya.

2. Keandalan (*Reliability*)

Rekod dapat dipercaya sebagai bukti akurat transaksi, kegiatan, atau fakta dan dapat diandalkan untuk transaksi atau kegiatan berikutnya. Arsip sebaiknya diciptakan pada saat terjadinya peristiwa baik oleh perseorangan, organisasi, maupun oleh sistem yang secara rutin digunakan untuk melaksanakan transaksi.

3. Integritas (*Integrity*)

Rekod harus dilindungi dari tindakan pengubahan yang tidak sah. Kebijakan dan prosedur untuk mengelola rekod sebaiknya menetapkan keterangan tambahan yang sah setelah rekod diciptakan, meliputi kondisi dan siapa yang diberi kewenangan untuk menciptakannya. Keterangan tambahan atau penghapusan terhadap rekod sebaiknya dinyatakan secara eksplisit dan dapat ditelusur.

4. Ketergunaan (*Usability*)

Rekod dapat ditemukan, diambil, disimpan, dan diinterpretasikan secara tepat waktu.

Rekod Elektronik

Rekod elektronik merupakan rekod yang disimpan pada media elektronik sehingga mudah diakses dan dapat dilakukan revisi atau perubahan dengan mudah. Rekod elektronik adalah seluruh informasi dalam bentuk yang dapat dibaca oleh mesin. Rekod elektronik meliputi dokumen numerik, grafik, audio, video, dan informasi tekstual yang direkam atau dikonversi kedalam bentuk analog atau digital seperti *spreadsheet* elektronik, *word processing files*, *database*, surat elektronik, pesan instan, hasil pindai, foto digital, dan file multimedia (Aramide et al., 2020)

The National Archives of Austria mendefinisikan rekod elektronik kedalam empat kategori (Katu, 2016):

1. Dokumen yang dibuat menggunakan aplikasi perkantoran, seperti dokumen teks, *spreadsheet*, dan presentasi.
2. Rekod berbasis web atau *online*, seperti intranet, ektranet, dan rekod transaksi online.
3. Rekod yang dihasilkan oleh sistem informasi bisnis seperti *database*, sistem data geospasial, sistem sumber daya manusia, sistem keuangan, sistem alur kerja dan sistem manajemen konten.
4. Sistem komunikasi digital seperti email, layanan pesan singkat, layanan pesan multimedia, dan *fax* elektronik.

Sistem rekod elektronik adalah sistem data terkomputerisasi yang dibentuk melalui pengumpulan, pengolahan, dan penyebarluasan data yang memenuhi persyaratan fungsional. Perancangan sistem pengelolaan rekod elektronik harus berdasarkan prinsip pengelolaan arsip yang baik. Sistem rekod elektronik berbeda dengan sistem pengelolaan rekod fisik. Sehingga diperlukan sistem manajemen rekod yang terdiri atas elemen teknis seperti perangkat lunak yang dirancang khusus untuk mengelola rekod untuk keperluan operasional pekerjaan, dan elemen non teknis seperti kebijakan, prosedur, sumber daya manusia dan stakeholder lainnya, serta tanggung jawab yang dibebankan.

Sistem Manajemen Rekod Elektronik

Integrasi manajemen rekod pada organisasi yang sebagian besar menghasilkan rekod dalam bentuk elektronik dapat diwujudkan melalui implementasi *Electronic Record Management System* (ERMS). ERMS mengacu pada sistem atau rangkaian aplikasi yang dirancang untuk melacak dan menyimpan rekod digital serta metadata (Mukred et al., 2016). ERMS merupakan sistem yang memungkinkan organisasi untuk menetapkan lingkup manajemen rekod mencakup serangkaian kegiatan yang berkaitan dengan penyimpanan, keamanan, akses, dan pemusnahan. Lingkup manajemen rekod tersebut tercermin dalam serangkaian tindakan yang dilakukan dalam proses pengelolaan rekod secara digital.

Pengelolaan rekod bertujuan untuk menyediakan bukti dari peristiwa atau kegiatan bisnis dalam suatu organisasi ketika dibutuhkan. Tujuan ini dapat dicapai melalui penangkapan informasi kontekstual (metadata) terkait dengan rekod yang diciptakan, mengintegrasikan rekod ke dalam aktivitas bisnis, serta menerapkan kontrol keamanan untuk memastikan bahwa rekod memenuhi persyaratan autentisitas dan integritas. Agar ERMS berfungsi dengan baik dalam organisasi, manajer arsip, dan profesional teknologi informasi (TI) harus bekerja sama untuk mengintegrasikan rekod elektronik dengan aplikasi yang digunakan. Manajemen arsip elektronik yang baik membawa beberapa keuntungan diantaranya:

1. Mengurangi volume data dan menghilangkan kekacauan pada tempat penyimpanan data. Data dapat diarsipkan secara aman diluar lokasi penyimpanan organisasi, sehingga memungkinkan organisasi untuk mengurangi kebutuhan ruang penyimpanan mereka.
2. Pengambilan informasi yang cepat.
3. Kepatuhan hukum dan mitigasi risiko litigasi. Manajemen rekod elektronik yang efektif akan melindungi organisasi dari litigasi dan investigasi hukum. Dalam hal ini sistem manajemen rekod elektronik harus berperan sebagai sistem yang menjamin keamanan rekod organisasi agar dapat terhindar dari ancaman bahaya dan kerugian.

Keamanan Rekod Elektronik

Keamanan rekod dapat didefinisikan sebagai tingkat perlindungan terhadap rekod dari ancaman bahaya, kerugian, dan tindakan kriminal (Aramide et al., 2020). Keamanan rekod perlu dikelola agar rekod dapat terlindungi dan terhindar dari kerusakan maupun akses tidak sah. Metode keamanan sepenuhnya bergantung pada metode penyimpanan yang diadopsi oleh organisasi. Kerahasiaan rekod elektronik yang tersimpan dapat dijaga dengan memberikan kata sandi ke dokumen atau file sehingga menyulitkan pengguna lain yang tidak mengetahui kata sandi untuk mengakses file.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur yang merupakan kegiatan pengumpulan data pustaka, membaca, merangkum, dan mencatat hal-hal penting dari buku dan literatur lainnya, kemudian mengolah bahan penelitian tersebut sebagai objek utama penelitian (Zed, 2014). Selain itu, studi literatur berkaitan dengan kajian teoritis melalui referensi-referensi terkait dengan nilai, budaya, dan norma yang berkembang pada situasi sosial yang diteliti. Penelitian kepustakaan ini tidak terlepas dari literatur-literatur ilmiah. (Sugiyono, 2018)

Data dalam penelitian ini diambil melalui kajian literatur berupa buku, artikel dalam jurnal, standar internasional, peraturan perundang-undangan, dan sumber-sumber tertulis lainnya yang sejalan dengan tujuan penelitian. Artikel-artikel dalam maupun luar negeri yang membahas tentang sistem keamanan rekod elektronik dihimpun, kemudian dianalisis untuk lebih memahami tantangan mengenai sistem keamanan rekod yang akan dihadapi dalam era disrupsi digital, serta melakukan pencarian penelitian terdahulu mengenai sistem keamanan rekod elektronik.

HASIL DAN PEMBAHASAN

Tantangan Sistem Keamanan Rekod Elektronik

Penggabungan layanan bisnis berbasis digital untuk memenuhi kebutuhan informasi yang semakin berkembang mengarah pada dinamika yang lebih kompleks terkait dengan penyebaran data dan risiko keamanan data. Secara umum, keamanan data mencakup keamanan sistem, perlindungan data pribadi, optimalisasi layanan, kemampuan untuk melakukan perbaikan dan mitigasi secara cepat jika terjadi kesalahan (Repetto et al., 2021)

Dalam konteks manajemen rekod elektronik, sifatnya yang rawan dimanipulasi atau rawan terjadi kesalahan dalam bentuk perubahan atau penghapusan secara sengaja maupun tidak disengaja, mengindikasikan bahwa perlindungan rekod elektronik belum dilakukan secara tepat. Sehingga suatu organisasi perlu memberikan perhatian khusus untuk memastikan keamanan rekod yang dimiliki untuk mencegah kehilangan data, korupsi data, akses data yang tidak sah, memastikan integritas data, serta keandalan dan kerahasiaan rekod elektronik.

Tentunya untuk mengatur strategi terkait dengan manajemen sistem keamanan data, seorang pengelola rekod perlu mengetahui seperti apa risiko dan tantangan yang akan dihadapi ketika sebuah organisasi menerapkan manajemen rekod berbasis elektronik. Berikut ini adalah beberapa tantangan pada sistem keamanan rekod elektronik yang akan dihadapi di era disrupsi digital (Majore et al., 2014):

1. Tantangan Akses Jangka Panjang

Pengelola rekod atau arsiparis dalam suatu organisasi harus memastikan aksesibilitas rekod terutama dengan memanfaatkan teknologi berupa perangkat keras dan perangkat lunak yang terus berkembang.

2. Keusangan Media

Media yang berisi rekod elektronik dapat menjadi tidak terbaca karena kurangnya perangkat keras yang memadai untuk mengakses media.

3. Keusangan Format

Rekod elektronik menjadi tidak dapat diakses karena perangkat lunak asli yang digunakan untuk membuat rekod digital tidak lagi tersedia sehingga perlu dilakukan update secara berkala.

4. Hilangnya Integritas

Rekod elektronik dapat dengan mudah dimanipulasi dan diubah karena sifat digitalnya yang mudah diakses dan fleksibel untuk dilakukan perubahan, pendistribusian, hingga penggandaan.

5. Hilangnya Bukti Keberadaan Rekod

Rekod elektronik harus memiliki bukti yang dapat digunakan untuk membuktikan keberadaan rekod elektronik pada suatu periode tertentu dan harus berasal dari sumber yang terpercaya.

Meskipun rekod elektronik membawa manfaat yang sangat berguna bagi organisasi terutama dalam hal aksesibilitas informasi, namun banyak tantangan yang masih perlu dihadapi. Teknologi digital berkembang dengan sangat pesat sehingga perangkat lunak dan perangkat keras yang digunakan untuk mengelola rekod elektronik cenderung memiliki umur yang lebih singkat. Dalam arti, perangkat lunak maupun perangkat keras yang sudah muncul dalam versi terbaru harus di upgrade atau dilakukan penggantian jika sudah tidak kompatibel untuk digunakan.

Selain itu tantangan autentikasi rekod juga menjadi tantangan mengingat kemudahan akses rekod elektronik memungkinkan terjadinya manipulasi dokumen baik berupa perubahan dan penghapusan. Rekod merupakan bukti aktivitas bisnis yang harus dikelola dengan aman untuk mencegah adanya modifikasi yang tidak sah. Keamanan rekod elektronik berkaitan erat dengan metadata. Memelihara metadata termasuk spesifikasi teknis yang diperlukan untuk memastikan pelestarian rekod elektronik dan keberlanjutan aksesibilitasnya dari waktu ke waktu.

Strategi Sistem Keamanan Rekod Elektronik

Menurut Peraturan Pemerintah Republik Indonesia Nomor 28 Tahun 2012 tentang Pelaksanaan UU Nomor 43 Tahun 2009 tentang Kearsipan, disebutkan bahwa “pemeliharaan arsip adalah kegiatan menjaga keutuhan, keamanan, dan keselamatan arsip baik fisik maupun informasinya”. Menjaga rekod dari kerusakan yang disengaja maupun tidak disengaja atau menjaga kerahasiaannya dikenal sebagai perlindungan rekod. Keamanan rekod mengacu pada perlindungan rekod dari bahaya fisik dan ancaman yang dapat terjadi kapan saja. Sehingga pengelola rekod perlu memikirkan bagaimana strategi terbaik yang dapat diimplementasikan pada sistem keamanan rekod elektronik di organisasinya.

Menurut ISO 15489-1 tahun 2016, keamanan rekod merupakan upaya pengendalian akses, pemantauan, pemvalidasian dan pemusnahan yang dilakukan

untuk mencegah akses, pengubahan, penyembunyian, atau perusakan rekod secara tidak sah. Terdapat beberapa tindakan yang dapat digunakan untuk melindungi rekod, yaitu (Aramide et al., 2020):

1. Mengelola Akses Rekod

Tingkat keamanan yang diperlukan untuk rekod akan bervariasi bergantung pada nilai atau jenis rekod. Beberapa rekod mungkin memiliki tingkat sensitivitas yang sangat rendah, membutuhkan sangat sedikit atau tidak memerlukan pengamanan. Namun sebagian rekod yang lain mungkin memiliki tingkat sensitivitas yang tinggi, sehingga membutuhkan keamanan yang tinggi pula. Aksesibilitas rekod harus bergantung pada tingkat sensitivitasnya. Tingkat sensitivitas rekod akan menentukan pihak-pihak mana saja yang dapat mengakses rekod tersebut.

2. Transfer Rekod

Jika data atau informasi perlu dikirim kepada pihak ketiga atau pihak lainnya baik di dalam maupun di luar organisasi, maka keamanan diperlukan untuk melakukan tindakan perlindungan dan pencegahan. Hal ini meliputi menentukan format dan pengemasan yang tepat, serta mengirimkan ke alamat yang tepat.

3. Keaslian atau autentisitas Rekod

Hal ini berlaku untuk rekod cetak maupun rekod elektronik. Terdapat beberapa kesulitan dalam menjaga integritas elektronik rekod, misalnya rekod yang disimpan di email atau data yang terkandung dalam *database*, keduanya dapat diubah dengan mudah. Tindakan yang harus diambil harus mencakup:

- a. Mengontrol akses rekod atau data,
- b. Mengetahui siapa yang bertanggung jawab atas akses ke rekod atau data,
- c. Mencegah perubahan yang tidak disengaja atau dapat membahayakan rekod,
- d. Memeriksa keakuratan informasi atau rekod secara berkala.

4. preservasi Rekod

Organisasi harus mempertimbangkan format atau media yang tepat untuk menyimpan rekod, dan memilih yang memiliki tingkat keamanan tinggi. Sehingga dapat mencegah hilang rekod. Melakukan pencadangan dokumen diperlukan jika dokumen dirasa sangat penting dalam bisnis.

5. Lokasi Penyimpanan

Rekod harus disimpan dengan aman, baik secara elektronik dan fisik. Dokumen sensitif tidak boleh ditinggalkan di meja atau ketika layar komputer tidak terjaga. Organisasi harus mempertimbangkan metode terbaik untuk melakukan penyusutan arsip pada akhir masa pakainya.

6. Mencegah *Fraud* dan Pencurian Data

Merupakan suatu tindakan preventif yang harus dilakukan organisasi untuk menghindari tindakan kriminal pada dunia maya yang dikenal dengan *cybercrime* seperti *fraud*, *hacking*, dan pencurian data.

Organisasi menghadapi berbagai macam ancaman keamanan yang datang dari berbagai sudut pandang yang berbeda seperti pencurian dan penyalahgunaan informasi baik oleh pihak internal maupun pihak eksternal, ancaman bencana seperti kebakaran, banjir, dan bencana alam lainnya, atau ancaman virus yang dapat menyerang sistem perangkat lunak. Ancaman peretasan (*hacking*) dan pencurian data

yang saat ini semakin meningkat juga menjadi tantangan untuk menggunakan strategi sistem manajemen rekod elektronik. Menurut National Archives of Australia (2011), beberapa praktik yang dapat digunakan sebagai protokol untuk menjaga keamanan dokumen elektronik meliputi kegiatan :

1. Membatasi akses dokumen digital kepada personel yang berwenang untuk melindungi integritas dokumen dan mencegah perubahan secara tidak sah.
2. Membangun sistem keamanan jaringan seperti *firewall*, untuk melindungi akses eksternal yang tidak sah (misalnya peretas).
3. Menginstall *filter gateway* perangkat lunak, untuk memastikan bahwa filter diperbarui berkala untuk melindungi spam dan kode berbahaya seperti virus.
4. Menetapkan prosedur sistem *backup* dan pemulihan bencana yang sesuai untuk melindungi dokumen digital.
5. Mengembangkan dan menerapkan jejak audit untuk mendeteksi siapa yang mengakses sistem, apakah prosedur keamanan yang ditentukan telah diikuti dan untuk memastikan tidak ada tindakan tidak sah atau *fraud* yang terjadi.

KESIMPULAN

Disrupsi digital telah membawa perubahan terhadap model bisnis yang ditandai dengan berkembangnya teknologi baru. Perkembangan teknologi ini juga membawa perubahan terhadap sistem manajemen rekod elektronik yang dalam pelaksanaannya melibatkan elemen teknis seperti perangkat lunak dan perangkat keras, serta elemen non teknis seperti kebijakan, prosedur, dan sumber daya manusia. Manajemen rekod elektronik meliputi serangkaian kegiatan yang berkaitan dengan penyimpanan, keamanan, akses, dan pemusnahan yang bertujuan untuk menjaga keautentikan, keandalan, integritas, dan kegunaan rekod.

Berdasarkan tujuan tersebut, terdapat beberapa tantangan yang harus dihadapi oleh pengelola rekod dalam mengelola rekod elektronik diantaranya adalah menjaga aksesibilitas rekod, keamanan terkait transfer data atau distribusi rekod, menjaga keaslian atau autentisitas rekod, keamanan terkait preservasi rekod, keamanan lokasi penyimpanan, dan keamanan terkait pencegahan terhadap *fraud* atau pencurian. Sehingga saat ini lembaga maupun organisasi pengelola rekod juga perlu mengatur strategi terkait keamanan dari segi teknologi informasi (TI) seperti pembatasan akses, pembangunan sistem keamanan, perlindungan sistem dari virus, prosedur sistem *backup*, dan menerapkan jejak audit untuk menghindari terjadinya tindakan *fraud* ataupun penyalahgunaan dokumen.

DAFTAR PUSTAKA

- Aramide, O. K., PhD., Ajibola, R. E., Olatunji, O. S., & Oduroye, P. (2020). Improving records management and security for successful business performance: The role of new media. *The Role of New Media. Library Philosophy and Practice*, 1-19,1A-1B.
- Katuu, S. (2016). Managing digital records in a global environment: A review of the landscape of international standards and good practice guidelines. *The Electronic Library*., 34(5), 869–894.
- Linz, C., Müller-Stewens, G., & Zimmermann, A. (2017). Radical business model

transformation: Gaining the competitive edge in a disruptive world. *Kogan Page Limited, Croydon, UK*.

- Majore, S. A., Yoo, H., & Shon, T. (2014). Secure and reliable electronic record management system using digital forensic technologies. *Journal of Supercomputing*, 70(1), 149–165.
- Mukred, M., & Yusof, Z. M. (2016). Electronic records management system adoption readiness framework for higher professional education institutions in Yemen. *International Journal on Advanced Science, Engineering and Information Technology*, 6(6), 804–811.
- Mukred, M., & Yusof, Z. M. (2020). The performance of educational institutions through the electronic records management systems: factors influencing electronic records management system adoption. *IGI Global*, 1578–1598.
- National Archives of Australia. (2011). *Implementing an EDRMS - Key considerations*.
- Parviainen, P., Tihinen, M., Kaariainen, J., Teppola, S. (2017). Tackling the digitalization challenge: how to benefit from digitalization in practice. *Int. J. Inf. Syst. Proj. Manag*, 5(1), 63–77.
- Read, Judith, & Ginn, M. L. (2015). Records management. *Boston: Cengage Learning*, 10th ed.
- Repetto, M., Carrega, A., & Rapuzzi, R. (2021). An architecture to manage security operations for digital service chains. *Future Generation Computer Systems*, 115, 251–266.
- Sugiyono. (2018). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.
- Zed, M. (2014). *Metode Penelitian Kepustakaan*. Jakarta: Yayasan Pustaka Obor Indonesia.