RISOMA : Jurnal Riset Sosial Humaniora dan Pendidikan
Volume. 3 Nomor. 4 Juli 2025
e-ISSN : 3032-5218; p-ISSN : 3032-2960, Hal. 254-266
DOI: https://doi.org/10.62383/risoma.v3i4.868
Available online at: https://journal.appisi.or.id/index.php/risoma

Optimalisasi Keamanan Informasi melalui Sistem Pengelolaan Surat yang Aman di Lingkungan Kerja

Lili Raflika[1*], Khalisatun Husna[2], Muhammad Arby Fahrezi[3], Sari Andini[4], Saila Rahma Annisa[5], Tengku Darmansah[6]
[1-6] Universitas Islam Negeri Sumatera Utara,Medan,Indonesia

Alamat: Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara, 20371
*Korespondensi penulis: liliraflika568@gmail.com**

Abstract.*Mail management is a crucial element of organizational administration that plays a direct role in ensuring information security. This article discusses how poorly organized mail systems can create vulnerabilities for various threats to sensitive information, such as leakage, forgery, and document loss. Using a literature review method, the study identifies key risks and analyzes optimization strategies that can be implemented. The findings indicate that adopting digital systems, enhancing human resource (HR) capacity, and implementing access controls and audit trails are strategic steps to safeguard confidentiality, integrity, and availability of documents. The implications highlight the importance of integrating mail management with information security principles to establish an administrative governance system that is secure, efficient, and trustworthy.*

Keywords:*Access control; Audit trail; Digital systems; Information security; Mail management*

Abstrak. Pengelolaan surat merupakan elemen krusial dalam sistem administrasi organisasi yang berperan langsung dalam menjaga keamanan informasi. Artikel ini membahas bagaimana sistem pengelolaan surat yang tidak tertata dengan baik dapat menjadi celah bagi berbagai ancaman terhadap informasi penting, seperti kebocoran, pemalsuan, hingga hilangnya dokumen. Dengan menggunakan metode studi literatur, penelitian ini mengidentifikasi risiko-risiko utama serta menganalisis strategi optimalisasi yang dapat diterapkan. Hasil kajian menunjukkan bahwa penerapan sistem digital, peningkatan kapasitas sumber daya manusia (SDM), dan implementasi kontrol akses serta audit trail merupakan langkah strategis untuk menjaga kerahasiaan, integritas, dan ketersediaan dokumen. Implikasi dari kajian ini menekankan pentingnya integrasi pengelolaan surat dengan prinsip-prinsip keamanan informasi dalam membangun tata kelola administrasi yang aman, efisien, dan terpercaya.

Kata kunci: Audit trail; Keamanan informasi; Kontrol akses; Pengelolaan surat; Sistem digital.

1. LATAR BELAKANG

Di era digital yang semakin maju, keamanan informasi menjadi aspek krusial dalam menjaga keberlangsungan operasional suatu organisasi. Salah satu jalur utama penyampaian informasi di lingkungan kerja adalah melalui sistem persuratan, baik dalam bentuk fisik maupun digital. Surat sebagai media komunikasi formal tidak hanya memuat pesan administratif, tetapi sering kali juga mengandung informasi yang bersifat rahasia, strategis, dan berdampak langsung pada pengambilan keputusan organisasi.

Namun, dalam praktiknya, sistem pengelolaan surat di banyak instansi masih dilakukan secara konvensional dan belum memperhatikan prinsip-prinsip dasar keamanan informasi. Hal ini mengakibatkan tingginya risiko kebocoran data, pemalsuan dokumen, hingga kehilangan arsip penting. Kurangnya sistem kontrol akses, minimnya pelatihan sumber daya manusia

Received: Mei 17, 2025; Revised: Mei 31,2025; Accepted: Juni 01, 2025; Online Available: Juni 03, 2025;

dalam pengelolaan dokumen, serta belum adanya integrasi teknologi informasi menjadi penyebab utama lemahnya pengamanan terhadap informasi dalam surat.

Penelitian ini bertujuan untuk mengeksplorasi keterkaitan antara sistem pengelolaan surat dan keamanan informasi, serta merumuskan strategi optimalisasi yang dapat diterapkan oleh organisasi. Dengan pendekatan studi literatur, artikel ini berusaha memberikan pemahaman menyeluruh mengenai risiko, tantangan, serta solusi dalam menciptakan sistem persuratan yang tidak hanya efisien, tetapi juga aman dan terpercaya sesuai prinsip kerahasiaan *(confidentiality),* integritas *(integrity),* dan ketersediaan *(availability).*

2. KAJIAN TEORITIS

Keamanan Informasi

Keamanan Informasi adalah upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung memastikan kelangsungan bisnis, mengurangi risiko yang muncul, dan memungkinkan Anda mengoptimalkan laba atas investasi. Tujuannya untuk menjaga agar informasi sensitif tetap bersembunyi dari orang yang tidak berhak, memastikan bahwa hanya individu yang berhak saja yang dapat mengakses informasi tersebut. (Pardosi et al., 2024)

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjami kelangsungan bisnis, meminimalisir resiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Dimensi atau indikator Keamanan Informasi adalah keamanan informasi ditujukan untuk mencapai tiga tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas. Keamanan informasi terdiri dari perlindungan terhadap aspek *Confidentiality, Integrity dan Availability*. (Saputra et al., 2023)

Keamanan informasi adalah aspek utama pada upaya menjaga aset informasi pada suatu organisasi. Menurut Basyarahil, tipe keamanan informasi bisa dikelompokkan dalam sejumlah komponen berikut ini: (Nurul et al., 2022)

a. *Physical security:* keamanan yang berfokus pada strategi dalam mengamankan tenaga kerja maupun anggota organisasi, aset fisik, serta lokasi kerja dari sejumlah marabahaya yaitu resiko kebakaran, akses tanpa otorisasi, serta bencana alam.
b. *Personal security:* keamanan yang overlap dari physical security untuk memberikan perlindungan terhadap individu pada sebuah perusahaan pada sebuah organisasi.
c. Operational security: keamanan yang berfokus pada strategi dalam mengamankan kekuatan perusahaan agar tidak ada hambatan saat bekerja.

d. *Communications security:* keamanan dengan tujuan melindungi media komunikasi, teknologi komunikasi dan isinya, serta kecakapan dalam menggunakan alat tersebut agar meraih tujuan suatu perusahaan
e. *Network security:* keamanan yang berfokus terhadap perlindungan alat jaringan serta organisasi, jaringan serta isinya, dan kecakapan dalam memakai jaringan itu untuk memenuhi fungsi komunikasi data organisasi itu.

Pengelolaan Surat

Surat merupakan salah satu sarana atau media yang digunakan oleh organisasi didalam melakukan komunikasi secara tertulis. Pengelolaan surat merupakan salah satu kegiatan organisasi yang dapat membantu kelancaran bidang administrasi (Azis et al., 2021). Surat juga dapat diartikan sebagai suatu sarana komunikasi yang digunakan untuk menyampaikan informasi tertulis oleh suatu pihak kepada pihak lain atas nama perseorangan dan dapat atas nama jabatan dalam suatu organisasi.

Dalam suatu organisasi atau perusahaan surat menurut prosedur pengurusannya dibagi menjadi dua yaitu surat masuk dan surat keluar. Surat masuk adalah semua jenis surat yang diterima dari instansi lain maupun perorangan, baik yang diterima melalui pos maupun yang diterima melalui kurir dengan mempergunkan buku pengiriman atau ekspedisi. Sedangkan surat keluar adalah surat yang sudah lengkap (bertanggal,bernomor,berstempel,dan telah ditandatangani oleh pejaat yang berwenang) yang dibuat oleh suatu instansi, kantor atau lembaga untuk diajukan atau dikirim kepada instansi, kantor atau lembaga lain (Hidayat & Jumiatin, 2016).

Prosedur pengelolaan surat masuk yang meliputi, pengelompokkan surat, membuka surat, pemeriksaan surat, pencatatan surat dan pendistribusian surat. Sedangkan untuk pengelolaan surat keluar meliputi, pembuatan konsep, persetujuan konsep, pengetikan surat, pemberian nomor, penyusunan surat, pengiriman surat (Sya'bany, 2015).

Hubungan antara Pengelolaan Surat dan Keamanan Informasi

Sistem pengelolaan surat memegang peranan penting sebagai garis pertahanan awal dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi yang terkandung dalam dokumen resmi. Selain itu, sistem pengelolaan surat yang baik juga berkontribusi terhadap terciptanya tata kelola organisasi yang transparan dan akuntabel. Setiap proses pengiriman dan penerimaan surat terdokumentasi dengan jelas, sehingga memudahkan proses audit dan

pengawasan (Muchtar et al., 2022). Ini mendukung prinsip *good governance* dan meningkatkan kepercayaan publik terhadap institusi yang bersangkutan.

Keterkaitan sistem pengelolaan surat dengan keamanan informasi adalah hubungan erat antara cara suatu organisasi mengelola surat-menyurat (baik secara fisik maupun digital) dengan upaya menjaga kerahasiaan, integritas, dan ketersediaan informasi yang terkandung dalam surat tersebut.

Sistem pengelolaan surat yang baik berfungsi sebagai mekanisme perlindungan awal terhadap informasi penting (Darmansah, Siregar, et al., 2024). Jika sistem ini tidak dikelola dengan aman, maka risiko kebocoran data, penyalahgunaan informasi, dan hilangnya dokumen penting akan meningkat. Sebaliknya, pengelolaan surat yang terintegrasi dengan prinsip-prinsip keamanan informasi akan membantu organisasi.

Dengan demikian, keterkaitan antara sistem pengelolaan surat dan keamanan informasi tidak dapat dipisahkan. Keduanya saling menunjang dalam mewujudkan sistem administrasi yang efisien, aman, dan terpercaya.

3. METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah studi literatur. Studi literatur merupakan pendekatan yang mengkaji berbagai sumber informasi yang relevan, seperti artikel jurnal, buku, laporan, dan dokumen lainnya, untuk mendapatkan pemahaman yang komprehensif mengenai topik yang sedang diteliti. Dalam konteks penelitian ini, yaitu " Optimalisasi Keamanan Informasi melalui Sistem Pengelolaan Surat yang Aman di Lingkungan Kerja", kami mengidentifikasi dan menganalisis berbagai sumber yang relevan dengan topik tersebut.

Proses ini melibatkan pencarian sistematis dalam basis data ilmiah, penelaahan abstrak, dan seleksi sumber yang sesuai berdasarkan kriteria relevansi dan kualitas. Selanjutnya, kami menyusun temuan dari berbagai sumber tersebut untuk menghasilkan analisis yang komprehensif dan terpadu mengenai isu-isu utama, tren, dan praktik terkait. Studi literatur ini bertujuan untuk memberikan wawasan yang lebih dalam mengenai topik yang diteliti.

4. HASIL DAN PEMBAHASAN

a. Ancaman terhadap Keamanan Informasi dari Pengelolaan Surat yang Buruk

Pengelolaan surat yang tidak sistematis dan tidak memperhatikan aspek keamanan dapat menjadi celah serius terhadap kebocoran informasi. Dalam banyak kasus, surat dinas, nota dinas, maupun dokumen internal yang seharusnya bersifat rahasia menjadi rentan diakses,

dimodifikasi, bahkan disalahgunakan oleh pihak yang tidak berwenang. Berikut ini beberapa bentuk ancaman yang muncul akibat pengelolaan surat yang buruk: (Rozi et al., 2024)

- **Kebocoran Informasi Sensitif**

  Surat yang berisi informasi penting, seperti data kepegawaian, anggaran, atau strategi kebijakan dapat tersebar ke pihak luar jika tidak dikelola secara aman. Penyimpanan surat di tempat terbuka, tidak adanya kontrol akses, serta kebiasaan mendistribusikan dokumen tanpa pencatatan adalah penyebab umum terjadinya kebocoran.

- **Pemalsuan dan Manipulasi Surat**

  Tanpa adanya sistem verifikasi dan pencatatan yang baik, surat resmi dapat dengan mudah dipalsukan atau dimodifikasi isinya. Hal ini bisa dimanfaatkan oleh oknum untuk melakukan tindakan penipuan, penyalahgunaan wewenang, atau manipulasi informasi dalam proses birokrasi.

- **Kehilangan Dokumen**

  Surat yang tidak tercatat atau disimpan tanpa sistem pengarsipan yang jelas sangat rentan hilang. Kehilangan dokumen penting dapat mengganggu proses administrasi, memperlambat pengambilan keputusan, dan menyebabkan konflik antarlembaga atau unit kerja.

- **Akses Tidak Sah *(Unauthorized Access)***

  Tanpa sistem klasifikasi kerahasiaan atau pembatasan hak akses, surat penting dapat dengan mudah diakses oleh pegawai yang tidak memiliki kewenangan. Hal ini tidak hanya menyalahi prinsip tata kelola informasi, tetapi juga dapat membahayakan kepentingan lembaga jika informasi digunakan secara tidak semestinya.

- **Tidak Terdeteksinya Jejak Distribusi Surat**

  Pengelolaan surat secara manual sering kali tidak mencatat secara rinci alur distribusi dokumen. Akibatnya, bila terjadi kebocoran atau penyalahgunaan, sangat sulit untuk melakukan pelacakan siapa yang terakhir mengakses atau memegang surat tersebut. Hal ini membuat proses audit dan pertanggungjawaban menjadi lemah.

  Salah satu sumber risiko adalah pengelolaan dokumen dan surat yang tidak memadai**,** baik secara fisik maupun digital. Dokumen tersebut sering kali menjadi vektor pembawa informasi sensitif**,** sehingga jika tidak dikelola dengan aman,

dapat mengancam tiga pilar utama keamanan informasi, yaitu:(Harahap et al., 2023)

- **Kerahasiaan *(*Confidentiality*)***

  Konsep kerahasiaan mengacu pada upaya membatasi akses informasi hanya kepada pihak yang berwenang. Dalam konteks pengelolaan surat, ancaman terhadap kerahasiaan muncul ketika:

  - Surat tidak diklasifikasikan berdasarkan tingkat keamanan,
  - Tidak ada pembatasan akses pada surat yang bersifat rahasia,
  - Penyimpanan surat dilakukan di tempat terbuka atau mudah diakses oleh publik.

  Teori akses terkendali (access control theory) menjelaskan bahwa tanpa kontrol hak akses yang jelas, informasi dalam surat dapat dilihat, disalin, atau disebarluaskan oleh pihak yang tidak berkepentingan.

- **Integritas *(Integrity)***

  Integritas berkaitan dengan keaslian dan ketepatan informasi. Ancaman terhadap integritas dapat muncul jika surat:

  - Dimodifikasi secara tidak sah,
  - Dipalsukan oleh pihak yang tidak berwenang,
  - Tidak melalui prosedur validasi yang jelas saat diterima atau dikirim.

  Menurut teori sistem kontrol internal dalam manajemen dokumen, absennya proses otentikasi (seperti tanda tangan digital atau cap resmi) dapat menyebabkan surat mudah dimanipulasi, sehingga isinya tidak lagi mencerminkan kondisi sebenarnya.

- **Ketersediaan *(Availability)***

  Ketersediaan berarti informasi harus dapat diakses tepat waktu oleh pihak yang berwenang saat dibutuhkan. Pengelolaan surat yang buruk, seperti sistem pengarsipan manual yang tidak sistematis, tidak adanya backup digital, atau kehilangan dokumen—dapat menghambat akses yang sah. Teori manajemen arsip menekankan pentingnya sistem klasifikasi dan pengarsipan agar informasi tetap tersedia ketika dibutuhkan, serta dapat dilacak dengan mudah

b. Strategi Optimalisasi Sistem Pengelolaan Surat

Optimalisasi sistem pengelolaan surat bertujuan untuk memastikan bahwa setiap dokumen yang beredar dalam lingkungan kerja dapat dikendalikan secara aman, efisien, dan

sesuai dengan prinsip keamanan informasi (Dako et al., 2024). Upaya ini perlu menyasar pada integrasi teknologi, peningkatan kompetensi sumber daya manusia (SDM), serta penerapan kebijakan pengendalian akses dan pelacakan dokumen. Berikut adalah strategi yang dapat diterapkan:

- **Penerapan Sistem Digital**

  Dalam era transformasi digital, kebutuhan untuk mengelola informasi secara efisien dan aman menjadi semakin mendesak. Salah satu aspek penting dari manajemen informasi adalah pengelolaan surat, yang dalam konteks organisasi baik pemerintah maupun swasta masih sering dilakukan secara manual.

  Pendekatan tradisional tersebut memiliki berbagai kelemahan, mulai dari rawan kehilangan dokumen, keterbatasan dalam pelacakan distribusi surat, hingga tingginya risiko kebocoran informasi. Oleh karena itu, penerapan sistem digital menjadi strategi yang sangat relevan dan strategis untuk menjawab tantangan tersebut.

  Sistem digital dalam pengelolaan surat mencakup penggunaan perangkat lunak dan teknologi informasi untuk mencatat, menyimpan, mendistribusikan, dan mengarsipkan dokumen secara elektronik. Penerapan sistem ini dapat dilakukan melalui platform seperti e-office**,** e-archive**,** atau aplikasi khusus manajemen dokumen yang dilengkapi dengan fitur keamanan seperti tanda tangan elektronik**,** enkripsi data**,** dan verifikasi identitas pengguna**.** Sistem ini tidak hanya mempermudah proses administrasi, tetapi juga memberikan jaminan keamanan informasi karena setiap dokumen tercatat secara otomatis dan aktivitas pengguna terdokumentasi dengan baik.

- **Peningkatan Kapasitas SDM**

  Keberhasilan pengelolaan surat yang aman dan efisien tidak hanya bergantung pada kecanggihan teknologi, tetapi juga sangat ditentukan oleh kualitas sumber daya manusia (SDM) yang mengoperasikannya. SDM memegang peran sentral sebagai pengelola, pengakses, sekaligus penjaga dokumen organisasi. Ketidaktahuan, kelalaian, atau kurangnya kepedulian terhadap prosedur keamanan dapat membuka celah bagi terjadinya kebocoran informasi, manipulasi data, atau bahkan pencurian identitas organisasi. Oleh karena itu, peningkatan kapasitas SDM menjadi strategi utama yang tidak boleh diabaikan dalam upaya optimalisasi sistem pengelolaan surat.

Peningkatan kapasitas ini dapat dilakukan melalui pelatihan teknis yang terstruktur, pembinaan etika kerja, serta sosialisasi kebijakan keamanan informasi (Darmansah, Wahyudi, et al., 2024). SDM perlu dibekali dengan keterampilan dalam menggunakan sistem digital pengelolaan surat, memahami klasifikasi dokumen, dan menerapkan prinsip-prinsip keamanan seperti kerahasiaan, integritas, serta ketersediaan informasi. Selain itu, penting juga untuk menanamkan budaya disiplin dan tanggung jawab terhadap dokumen yang dikelola.

Dengan kapasitas SDM yang meningkat, organisasi akan lebih siap menghadapi tantangan keamanan informasi yang terus berkembang. Pegawai yang sadar akan pentingnya menjaga kerahasiaan surat tidak hanya akan patuh terhadap prosedur, tetapi juga akan mampu mengidentifikasi dan mencegah potensi ancaman sejak dini. Hal ini akan menciptakan lingkungan kerja yang lebih tertib, aman, dan profesional. Maka, investasi pada pengembangan kompetensi dan sikap pegawai bukan hanya berdampak pada peningkatan efisiensi kerja, tetapi juga merupakan bentuk perlindungan jangka panjang terhadap aset informasi organisasi.

- **Penerapan Kontrol Akses dan Audit Trail**

  Dalam sistem pengelolaan surat yang aman, kontrol akses memegang peran penting untuk memastikan bahwa hanya pihak yang berwenang yang dapat melihat, mengubah, atau mendistribusikan dokumen tertentu. Prinsip ini bertujuan untuk menjaga kerahasiaan dan integritas informasi, terutama terhadap surat-surat yang bersifat rahasia atau terbatas. Kontrol akses dapat diimplementasikan melalui sistem login personal, pembagian hak akses berdasarkan jabatan atau fungsi kerja, serta penerapan kebijakan penggunaan dokumen yang ketat. Dengan demikian, setiap pegawai hanya dapat mengakses surat sesuai dengan kewenangan yang diberikan, sehingga risiko penyalahgunaan informasi dapat diminimalkan.

  Audit trail melengkapi sistem kontrol akses dengan menyediakan rekam jejak digital atas semua aktivitas terhadap dokumen. Setiap tindakan seperti pembukaan, pengeditan, pengunduhan, atau penghapusan surat akan tercatat secara otomatis dalam sistem. Fitur ini memungkinkan organisasi untuk melacak siapa yang melakukan apa, kapan, dan terhadap dokumen mana. Jika terjadi pelanggaran atau kebocoran informasi, audit trail dapat digunakan sebagai alat forensik untuk mengidentifikasi sumber masalah dengan cepat dan akurat. Penerapan audit trail

juga meningkatkan akuntabilitas pegawai karena setiap aktivitasnya terdokumentasi dengan jelas.

c. Dampak terhadap Keamanan Informasi

Implementasi sistem pengelolaan surat yang aman di lingkungan kerja memiliki pengaruh signifikan terhadap upaya perlindungan keamanan informasi. Dalam era digital saat ini, di mana informasi menjadi salah satu aset paling berharga dalam organisasi, kebutuhan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi menjadi semakin mendesak. Surat dinas, memo internal, dokumen kontrak, serta korespondensi elektronik lainnya mengandung berbagai data sensitif yang, jika tidak dikelola dengan aman, dapat menjadi celah bagi kebocoran informasi, pencurian data, hingga penyalahgunaan dokumen penting.

Sistem pengelolaan surat yang dirancang dengan pendekatan keamanan informasi memungkinkan penerapan berbagai kontrol seperti otentikasi pengguna, enkripsi data, pelacakan aktivitas, dan pengelompokan hak akses. Dengan begitu, hanya pihak yang berwenang yang dapat mengakses surat atau dokumen tertentu. Ini berdampak langsung pada peningkatan kontrol internal serta pencegahan terhadap akses tidak sah. Selain itu, sistem semacam ini mampu menciptakan jejak audit (audit trail) yang memungkinkan setiap aktivitas terhadap surat terekam dan dapat ditelusuri jika terjadi insiden keamanan. Hal ini memperkuat prinsip akuntabilitas dan transparansi dalam pengelolaan dokumen organisasi (Imany et al., 2019). Adapun dampak terhadap keamanan informasi sebagai berikut:

- **Efektivitas pengamanan data**

  Penerapan sistem pengelolaan surat yang aman membawa dampak besar terhadap efektivitas pengamanan data dalam organisasi. Dalam lingkungan kerja modern, surat-surat yang masuk dan keluar tidak hanya sekadar dokumen administratif, tetapi sering kali memuat informasi penting, strategis, bahkan rahasia. Oleh karena itu, pengamanan data menjadi prioritas. Dengan menggunakan sistem digital yang dilengkapi dengan fitur keamanan canggih seperti enkripsi, autentikasi multi-faktor (MFA), dan pengendalian akses berbasis peran, organisasi dapat meningkatkan efektivitas perlindungan terhadap data dari pihak-pihak yang tidak berwenang. Sistem ini memungkinkan hanya pengguna dengan hak akses tertentu yang dapat membuka, memodifikasi, atau mendistribusikan surat, sehingga risiko kebocoran informasi secara signifikan dapat dikurangi.

Efektivitas pengamanan data juga tercermin dari kemampuan sistem dalam mencatat setiap aktivitas yang terjadi terhadap dokumen melalui fitur audit trail. Setiap perubahan, akses, dan pengiriman surat terekam secara otomatis, memungkinkan proses forensik digital dilakukan dengan cepat apabila terjadi insiden keamanan. Selain itu, sistem yang terotomatisasi mampu mendeteksi anomali atau pola akses tidak wajar yang bisa menjadi indikasi adanya percobaan pelanggaran keamanan. Penerapan sistem pengelolaan surat yang efektif membuat organisasi mampu bertindak lebih proaktif dalam mengidentifikasi potensi ancaman, daripada sekadar reaktif ketika insiden terjadi. Hal ini memperkuat kemampuan respons insiden keamanan dan memperkecil dampak kerusakan data yang mungkin terjadi (Matin et al., 2017).

- **Peningkatan kerahasiaan informasi**

  Penerapan sistem pengelolaan surat yang aman secara langsung berdampak pada peningkatan kerahasiaan informasi yang beredar di lingkungan kerja. Dalam sistem tradisional, pengelolaan surat yang dilakukan secara manual sering kali menimbulkan risiko kebocoran informasi, terutama ketika surat bersifat rahasia dan berpindah tangan tanpa kontrol yang ketat. Dengan beralih ke sistem digital yang menggunakan teknologi keamanan seperti enkripsi dan autentikasi ganda, organisasi dapat memastikan bahwa hanya pihak yang memiliki otorisasi yang dapat mengakses atau membaca surat tertentu.

  Enkripsi berperan sebagai teknologi inti yang menjaga data agar tidak dapat dibaca oleh pihak yang tidak berwenang. Dalam surat dinas atau komunikasi internal organisasi, enkripsi *end-to-end* sangat penting untuk menghindari penyadapan informasi ketika surat ditransmisikan melalui jaringan. Selain itu, sistem digital biasanya memungkinkan pengelompokan surat berdasarkan tingkat klasifikasi informasi (misalnya: publik, internal, rahasia), yang membantu dalam pengaturan hak akses secara sistematis dan terstruktur.

  Peningkatan kerahasiaan ini juga berdampak pada kepercayaan internal dan eksternal terhadap organisasi. Pihak internal, seperti manajemen dan staf, akan merasa lebih aman dalam bertukar dokumen penting tanpa khawatir akan kebocoran informasi. Pihak eksternal, termasuk mitra kerja dan pelanggan, juga akan lebih percaya pada sistem komunikasi organisasi yang terjamin keamanannya (Darmansah et al., 2025). Dengan demikian, kerahasiaan informasi yang dijaga

melalui sistem pengelolaan surat yang aman berkontribusi langsung terhadap citra dan kredibilitas organisasi secara keseluruhan.

- **Menjaga integritas informasi**

  Selain kerahasiaan, integritas informasi merupakan aspek penting yang dijaga oleh sistem pengelolaan surat yang aman. Integritas informasi mengacu pada jaminan bahwa data atau dokumen tidak mengalami perubahan tanpa izin dari pihak berwenang selama proses pengolahan, pengiriman, maupun penyimpanan. Dalam sistem manual, dokumen dapat dengan mudah dimanipulasi, disalahgunakan, atau bahkan hilang tanpa jejak. Namun dengan sistem digital, setiap tindakan terhadap dokumen terekam secara otomatis dalam sistem (*audit trail*), sehingga segala perubahan dapat ditelusuri kembali.

  Sistem pengelolaan surat yang aman juga dilengkapi dengan fitur validasi dan verifikasi dokumen digital, seperti tanda tangan digital dan cap waktu (*timestamp*). Fitur-fitur ini memastikan bahwa isi surat yang dikirim adalah versi yang asli dan belum diubah sejak dikirim. Penggunaan checksum atau hash pada dokumen juga bisa diterapkan untuk mendeteksi jika ada perubahan sekecil apa pun terhadap isi dokumen. Dalam banyak sistem manajemen dokumen modern, ketika sebuah surat diubah, sistem akan membuat versi baru (*versioning*) sambil tetap menyimpan versi lama untuk pelacakan.

  Dengan terjaganya integritas informasi, risiko terhadap manipulasi data dapat diminimalkan. Hal ini sangat penting dalam lingkungan kerja yang berkaitan dengan kebijakan strategis, keuangan, atau hukum, di mana sedikit perubahan informasi dapat berakibat fatal. Keandalan dokumen menjadi salah satu kunci pengambilan keputusan yang akurat. Oleh karena itu, menjaga integritas informasi melalui sistem pengelolaan surat yang aman bukan hanya mendukung keamanan, tetapi juga menjamin ketepatan operasional organisasi (Putra et al., 2019).

KESIMPULAN

Pengelolaan surat yang aman merupakan elemen krusial dalam menjaga keamanan informasi di lingkungan kerja, terutama di era digital yang penuh tantangan terhadap kerahasiaan, integritas, dan ketersediaan data. Sistem pengelolaan surat yang lemah dapat menjadi titik rawan terjadinya kebocoran informasi, pemalsuan dokumen, hingga hilangnya arsip penting. Hal tersebut berdampak langsung pada efektivitas operasional dan kredibilitas institusi.

Optimalisasi sistem pengelolaan surat dapat dicapai melalui tiga strategi utama: penerapan sistem digital**,** peningkatan kapasitas sumber daya manusia (SDM)**,** serta implementasi kontrol akses dan audit trail**.** Secara keseluruhan, sistem pengelolaan surat yang terintegrasi dengan prinsip-prinsip keamanan informasi tidak hanya meningkatkan perlindungan terhadap data, tetapi juga memperkuat tata kelola administrasi organisasi. Dengan demikian, organisasi dapat menciptakan lingkungan kerja yang lebih aman, profesional, dan terpercaya dalam menghadapi dinamika informasi modern.

DAFTAR REFERENSI

Azis, M., Sawiji, H., & Indrawati, C. D. S. (2021). Mekanisme pengurusan surat masuk dan surat keluar di instansi pemerintah. Jurnal Informasi dan Komunikasi Administrasi Perkantoran, 5(4), 36–44. https://doi.org/10.25130/sc.24.1.6

Dako, R. D. R., Abdussamad, S., Nasibu, I. Z., & Tolago, A. I. (2024). Optimalisasi penggunaan aplikasi pengelolaan surat untuk meningkatkan efisiensi kerja aparat di Desa Tunggulo. EMPIRIS: Jurnal Pengabdian pada Masyarakat (EJPPM), 2(2), 78–85. https://doi.org/10.37915/EJPPM.v2i2

Darmansah, T., Pasaribu, G. A., Juliana, D., Pulungan, S. N., & Pangolangan, C. A. (2025). Optimalisasi sistem informasi administrasi digital untuk meningkatkan efisiensi layanan dan keamanan informasi digital. Socius: Jurnal Pendidikan Ilmu-Ilmu Sosial, 2(11), 108–112. https://doi.org/10.5281/zenodo.15535360

Darmansah, T., Siregar, N. K., & Marpaung, W. T. (2024). Peran penting manajemen persuratan dalam menunjang kinerja organisasi. Madani: Jurnal Ilmiah Multidisipline, 2(6), 316–321. https://doi.org/10.5281/zenodo.11619549

Darmansah, T., Wahyudi, I., Lubis, N. M., Jannah, R., & Amanda, T. (2024). Peran manajemen persuratan dalam menjaga keamanan informasi persuratan. Jurnal Pendidikan Sosial dan Konseling, 2(1), 152–159. https://jurnal.ittc.web.id/index.php/jpdsk

Harahap, A. H., Andani, C. D., Christie, A., & Fauzi, A. (2023). Pentingnya peranan CIA Triad dalam keamanan informasi dan data untuk pemangku kepentingan atau stakeholder. Jurnal Manajemen dan Pemasaran Digital, 1(2), 73–83. https://doi.org/10.38035/jmpd.v1.i2

Hidayat, S., & Jumiatin, U. (2016). Prosedur pengelolaan surat untuk memperlancar proses penyampaian informasi pada Kantor Kecamatan Pamulang. Jurnal Sekretaris, 3(1), 83–115.

Imany, Y. D., Putra, W. H. N., & Herlambang, A. D. (2019). Evaluasi tata kelola keamanan informasi menggunakan COBIT 5 pada domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(6), 5926–5935.

Matin, I. M. M., Arini, A., & Wardhani, L. K. (2017). Analisis keamanan informasi data center menggunakan COBIT 5. Jurnal Teknik Informatika, 10(2), 119–128.

Muchtar, Heriyandi, & Hasyim, S. Bin. (2022). Implementasi sistem informasi manajemen surat dan pengarsipan di Sekretariat Daerah Kabupaten Garut. Jurnal Pembangunan dan Kebijakan Politik, 13(1), 44–61. http://www.journal.uniga.ac.id

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi keamanan sistem informasi: Keamanan informasi, teknologi informasi dan network (Literature review SIM). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). Sistem keamanan informasi. PT. Mafy Media Literasi Indonesia.

Putra, G. P., Santoso, N., & Junemaro, E. M. A. (2019). Rancang bangun sistem informasi manajemen persuratan Dinas Pendidikan Banyuwangi. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(5), 4276–4282.

Rozi, F., Ibrahim, A. M., & Pujiastuti, E. (2024). Analisis ancaman keamanan dalam penggunaan teknologi cloud computing. Just IT: Jurnal Sistem Informasi, Teknologi Informatika dan Komputer, 14(3), 209–219. https://jurnal.umj.ac.id/index.php/just-it/index

Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan keamanan informasi dan persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. Jurnal Teknologi dan Komunikasi Pemerintahan, 5(2), 159–187. https://doi.org/10.33701/jtkp.v5i2.3735

Sya'bany, M. (2015). Strategi pengamanan surat rahasia berbasis sumber daya persuratan. Jurnal Kajian Informasi dan Perpustakaan, 23(2), 253–270. https://doi.org/10.24198/jkip.v3i2.10001