



## Etika Profesi Pengembang Sistem Informasi dalam Pencegahan Insider Threat

Nova Adelia<sup>1</sup>, Joy Nashar Utamajaya<sup>2</sup>

Sistem Informasi, Stmik Borneo Internasional, Balikpapan, Indonesia

Email: [Novaadelia112018@gmail.com](mailto:Novaadelia112018@gmail.com)<sup>1</sup> [Joy.nashar@stmik-borneo.ac.id](mailto:Joy.nashar@stmik-borneo.ac.id)<sup>2</sup>

### ABSTRACT :

*Insider threat represents a security risk arising from individuals who have authorized access to organizational systems and information. In information system development, developers may interact with source code, databases, credentials, configurations, and deployment environments, making professional responsibility an important part of security protection. This study aims to synthesize the relationship between professional ethics of information system developers and insider threat prevention through a systematic literature review. Literature published primarily from 2021 to 2026 was examined from scholarly sources covering information security, software engineering, ethics, and secure software development. The synthesis indicates that privacy, confidentiality, security, responsibility, accountability, and professional judgment are ethical principles with direct implications for insider threat prevention. These principles can be operationalized through access control, least privilege, authentication, separation of duties, logging and audit trails, security monitoring, and secure software development practices. The study produces an integrative mapping that connects ethical principles, potential insider behaviors, security objectives, and preventive controls. The mapping positions professional ethics as a normative foundation that should be translated into concrete security practices throughout the software development life cycle.*

**Keywords:** *professional ethics, insider threat, information systems, software development, information security*

### ABSTRAK :

Insider threat merupakan risiko keamanan yang berasal dari individu yang memiliki akses resmi terhadap sistem dan informasi organisasi. Dalam pengembangan sistem informasi, pengembang dapat berinteraksi dengan source code, basis data, kredensial, konfigurasi, dan lingkungan deployment sehingga tanggung jawab profesional menjadi bagian penting dalam perlindungan keamanan. Penelitian ini bertujuan melakukan sintesis mengenai hubungan antara etika profesi pengembang sistem informasi dan pencegahan insider threat melalui systematic literature review. Literatur yang terutama diterbitkan pada periode 2021–2026 ditelaah dari sumber ilmiah yang mencakup keamanan informasi, software engineering, etika, dan secure software development. Hasil sintesis menunjukkan bahwa privacy, confidentiality, security, responsibility, accountability, dan professional judgment merupakan prinsip etika yang memiliki implikasi langsung terhadap pencegahan insider threat. Prinsip tersebut dapat dioperasionalkan melalui access control, least privilege, authentication, separation of duties, logging dan audit trail, security monitoring, serta praktik secure software development. Penelitian menghasilkan pemetaan integratif yang menghubungkan prinsip etika, potensi perilaku insider, sasaran keamanan, dan kontrol pencegahan. Pemetaan tersebut menempatkan etika profesi sebagai dasar normatif yang perlu diterjemahkan menjadi praktik keamanan konkret sepanjang software development life cycle.

**Kata Kunci:** etika profesi, insider threat, sistem informasi, pengembangan perangkat lunak, keamanan informasi

## PENDAHULUAN

Pengembangan sistem informasi menempatkan pengembang pada posisi yang tidak hanya berkaitan dengan fungsi perangkat lunak, tetapi juga dengan pengelolaan data, akses, konfigurasi, keamanan, dan keputusan teknis yang dapat memengaruhi pengguna maupun organisasi. Pengembang dapat berinteraksi dengan *source code*, basis data, API key, kredensial, konfigurasi keamanan, lingkungan pengujian, dan lingkungan produksi. Kondisi tersebut membuat kemampuan teknis dan hak akses yang dimiliki pengembang harus diimbangi dengan tanggung jawab profesional. *IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice* menempatkan *software engineering* sebagai profesi yang mencakup *analysis, specification, design, development, testing*, dan *maintenance* serta menetapkan kewajiban etis pada perilaku dan keputusan profesional (IEEE-CS/ACM Joint Task Force, 2001).

Kebutuhan tersebut semakin penting karena ancaman keamanan tidak selalu berasal dari pihak eksternal. *Insider threat* berkaitan dengan individu yang memiliki atau pernah memiliki akses resmi terhadap sumber daya organisasi. *Insider threat* dapat bersifat *malicious* maupun *accidental* dan dibentuk oleh interaksi faktor teknis serta faktor manusia (Pathirana et al., 2026). Inayat et al. (2024) juga menunjukkan bahwa *insider threat* dapat diklasifikasikan berdasarkan tipe *insider*, tingkat akses, sasaran keamanan, dan teknik serangan serta membutuhkan kombinasi pendekatan *prevention* dan *detection*. Persoalan *insider threat* tidak dapat direduksi menjadi tindakan pencurian data yang disengaja. Prabhu dan Dell (2025) melakukan *structured review* terhadap 123 artikel mengenai *insider cybersecurity behaviour* dan menunjukkan bahwa penelitian banyak berfokus pada perilaku yang disengaja, sedangkan *automatic* atau *unintentional behaviour* relatif kurang mendapat perhatian. Balagopal dan Mathew (2024) juga menunjukkan bahwa kepatuhan maupun pelanggaran *information security policy* dipengaruhi berbagai faktor individual dan organisasi. Dengan demikian, pengendalian *insider threat* perlu mempertimbangkan perilaku, kepatuhan, kondisi organisasi, serta kontrol teknis secara bersamaan.

Dari sisi pengembangan perangkat lunak, keamanan perlu diintegrasikan sepanjang *software development life cycle*. Nina et al. (2021) memetakan praktik *secure software development* pada *requirements, design, construction*, dan *testing*, sedangkan Khan et al. (2022) menunjukkan bahwa *security risk* dan *security practices* tersebar sepanjang siklus pengembangan. Rindell et al. (2021) melalui *practitioner survey* juga menunjukkan bahwa aktivitas keamanan yang dilakukan lebih awal dalam siklus pengembangan dinilai memiliki dampak yang tinggi. Temuan tersebut memperkuat kebutuhan untuk memasukkan tanggung jawab keamanan sejak tahap awal pengembangan, bukan hanya setelah sistem selesai. Etika memberikan lapisan normatif terhadap praktik keamanan tersebut. Alidoosti et al. (2025) melalui *systematic literature review* terhadap 623 artikel dan 85 *primary studies* memetakan *ethical values* dalam *software engineering* dan menekankan pentingnya *operationalization of ethical values* dalam *software design*. Gogoll et al. (2021) menjelaskan bahwa *codes of conduct* tidak dapat menggantikan *ethical deliberation* dalam pengembangan perangkat lunak sehingga persoalan etika perlu dipertimbangkan dalam proses pengambilan keputusan. Biable et al. (2023) mengembangkan *framework* etika pada *requirements engineering* untuk membantu mengurangi persoalan etis pada fase awal pengembangan.

Penelitian empiris juga memperlihatkan bahwa penerapan etika dan keamanan membutuhkan mekanisme yang dapat diterapkan dalam praktik. Halme et al. (2024) mengembangkan konsep *Ethical User Stories* sebagai cara untuk menerjemahkan pertimbangan etis ke dalam praktik *software engineering* dan memvalidasinya pada 689 *user stories*. Griffin et al. (2024) menunjukkan melalui wawancara dengan 40 *developers* bahwa *developer* memiliki *ethical agency* dalam pekerjaan mereka, tetapi penerapannya dipengaruhi oleh lingkungan organisasi dan pemahaman mengenai tanggung jawab etis. Weir et al. (2023) menemukan pada delapan organisasi bahwa *structured workshops* membantu 88 *developers* mengidentifikasi, mempromosikan, dan memprioritaskan masalah *security* dan *privacy*.

Pada konteks keamanan informasi, pengendalian perilaku internal juga berkaitan dengan kepatuhan kebijakan. Alraja et al. (2023) melakukan penelitian terhadap 348 *employees* dari tujuh negara dan menunjukkan bahwa faktor seperti *fear* dan *role values* berpengaruh terhadap *intention* untuk mematuhi *information security policies*, sedangkan *habit* tidak menunjukkan pengaruh signifikan. Jeong dan Zo (2021) menunjukkan bahwa pengendalian yang terlalu intrusif dapat menimbulkan persepsi *intrusion* terhadap *privacy* dan bahkan berdampak pada respons moral terhadap kebijakan keamanan. Karena itu, pengendalian *insider threat* perlu mempertimbangkan keseimbangan antara *security*, *privacy*, dan *autonomy*.

Literatur nasional juga menunjukkan bahwa hubungan antara etika profesi dan keamanan informasi mulai banyak dikaji. Anugrah et al. (2026) membahas pengaruh etika profesi terhadap keamanan informasi melalui *systematic literature study* dengan ilustrasi kebocoran data BSI. Nurmiati dan Aqeel (2026) mengkaji etika profesi TI sebagai instrumen pencegahan *cyber crime* di Indonesia menggunakan SLR. Bayhaqi et al. (2026) juga mengidentifikasi *professional accountability*, *data security and privacy*, *algorithmic transparency*, dan *public interest orientation* sebagai dimensi etika profesi dalam pengembangan dan pengelolaan sistem informasi. Literatur tersebut menunjukkan bahwa tema etika profesi dan keamanan telah berkembang, tetapi fokus penelitian masih berbeda-beda.

Berdasarkan kondisi tersebut, penelitian ini tidak mengklaim bahwa hubungan etika profesi dan *insider threat* belum pernah dibahas. Celah yang digunakan terletak pada kebutuhan untuk menyusun sintesis yang lebih terarah mengenai bagaimana prinsip etika profesi pengembang sistem informasi dapat dipetakan ke bentuk *insider threat* dan mekanisme pencegahannya dalam konteks pengembangan sistem. Penelitian ini bertujuan mengidentifikasi prinsip etika profesi yang relevan, mengidentifikasi bentuk dan faktor *insider threat*, menganalisis hubungan antara keduanya, serta memetakan mekanisme pencegahan yang dapat diintegrasikan sepanjang *software development life cycle*.

## METODE PENELITIAN

### 2.1. Desain Penelitian

Penelitian menggunakan *systematic literature review* untuk mengidentifikasi dan mensintesis bukti ilmiah mengenai etika profesi pengembang sistem informasi dan *insider threat*. Pelaporan proses kajian mengacu pada PRISMA 2020 yang menyediakan kerangka untuk pelaporan transparan mengenai identifikasi, screening, eligibility, dan inclusion pada *systematic review*. Pendekatan sintesis yang digunakan bersifat tematik, yaitu mengelompokkan temuan literatur berdasarkan prinsip etika, bentuk *insider threat*, faktor yang memengaruhi, serta mekanisme pencegahan.

Literatur utama dibatasi terutama pada publikasi 2021–2026 agar pembahasan mencerminkan perkembangan terbaru. Sumber sebelum periode tersebut hanya digunakan sebagai landasan normatif apabila memiliki kedudukan fundamental, terutama *Software Engineering Code of Ethics and Professional Practice IEEE-CS/ACM* yang secara khusus mendokumentasikan kewajiban etis dan profesional *software engineer*. *Review* dan *survey* digunakan untuk memetakan *state of the art*, sedangkan penelitian empiris digunakan untuk memperkuat temuan yang berkaitan dengan praktik developer, keamanan pengembangan, dan perilaku kepatuhan.

### 2.2. Strategi Penelusuran dan Seleksi Literatur

Penelusuran diarahkan pada IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Wiley Online Library, Taylor & Francis, Google Scholar, dan sumber indeks akademik nasional. Kata kunci disusun dalam tiga kelompok konsep, yaitu *ethics*, *software development*, dan *insider threat*. Kombinasi yang digunakan meliputi ("professional ethics" OR "software engineering ethics" OR "professional responsibility" OR "code of ethics") AND ("software developer" OR "software engineer" OR "software development" OR "information systems development") AND ("insider threat" OR "insider attack" OR "malicious insider" OR "insider risk"). Pencarian tambahan

dilakukan dengan menggabungkan dua domain ketika penggunaan tiga kelompok kata kunci sekaligus menghasilkan literatur yang terlalu sempit.

Kriteria inklusi mencakup artikel ilmiah yang diterbitkan terutama pada 2021–2026, memiliki identitas bibliografis yang dapat diverifikasi, relevan dengan sekurang-kurangnya satu pertanyaan penelitian, dan membahas etika profesi, insider threat, security behaviour, secure software development, atau mekanisme pengendalian yang berkaitan. Kriteria eksklusi meliputi artikel duplikat, sumber populer atau non-ilmiah, artikel yang hanya membahas serangan eksternal tanpa keterkaitan dengan insider threat, dan artikel yang tidak menyediakan informasi bibliografis yang dapat diverifikasi. Artikel yang menggunakan responden tetap dapat menjadi sumber sekunder dalam SLR; penelitian ini sendiri tidak melakukan pengumpulan data primer.

Sebagai korpus inti terverifikasi, penelitian memprioritaskan artikel yang mempunyai halaman penerbit atau repositori akademik yang menyediakan metadata dan DOI yang dapat ditelusuri. Hasil pencarian kemudian dikodekan berdasarkan fokus, metode, temuan utama, prinsip etika, bentuk insider threat, faktor risiko, dan mekanisme pencegahan. Angka tahapan PRISMA tidak dibuat berdasarkan perkiraan; jumlah hasil pencarian final perlu mengikuti ekspor dan screening aktual dari setiap database pada tahap replikasi penelitian.

### 2.3. Ekstraksi dan Sintesis Data

Data dari setiap artikel diekstraksi ke dalam kategori penulis, tahun, jenis penelitian, konteks, fokus, prinsip etika, jenis insider threat, faktor penyebab, mekanisme pencegahan, dan temuan utama. Review seperti Inayat et al., Pathirana et al., Prabhu dan Dell, serta Alidoosti et al. digunakan untuk membangun kategori awal, kemudian penelitian empiris seperti Jeong dan Zo, Alraja et al., Weir et al., Halme et al., dan Rezaei Nasab et al. digunakan untuk menguji keterkaitan kategori tersebut dengan praktik nyata.

Sintesis tematik dilakukan dalam dua tahap. Tahap pertama mengelompokkan konsep yang berulang pada literatur insider threat dan etika software engineering. Tahap kedua memetakan setiap prinsip etika terhadap potensi pelanggaran, sasaran keamanan, dan kontrol pencegahan. Mekanisme pencegahan dikategorikan ke dalam access governance, identity and authentication, activity traceability, development security, dan behavioral or organizational support. Pendekatan ini digunakan untuk menghasilkan pemetaan integratif yang menjadi hasil utama penelitian.

**Tabel 1. Kelompok literatur dan kontribusinya**

| Kelompok                    | Sumber utama                                                                                                                             | Fokus                                                       | Kontribusi                                   |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------|
| Insider threat              | Inayat et al. (2024); Pathirana et al. (2026); Prabhu & Dell (2025); Balagopal & Mathew (2024)                                           | Mitigation, detection, behaviour, compliance, human factors | Bentuk, faktor, dan kontrol insider threat   |
| Etika software engineering  | Alidoosti et al. (2025); Gogoll et al. (2021); Biabla et al. (2023); Halme et al. (2024); Griffin et al. (2024); Cociancig et al. (2025) | Ethical values, responsibility, ethical deliberation        | Prinsip etika dan cara mengoperasionalkannya |
| Secure software development | Nina et al. (2021); Khan et al. (2022); Rindell et al. (2021); Weir et al. (2023)                                                        | Security practices dan SDLC                                 | Penerapan keamanan pada proses pengembangan  |
| Konteks Indonesia           | Nurmiati & Aqeel (2026); Anugrah et al. (2026); Bayhaqi et al. (2026)                                                                    | Etika profesi dan keamanan TI                               | Perbandingan dan konteks nasional            |

## HASIL DAN PEMBAHASAN

### 3.1. Karakteristik Literatur yang Ditelaah

Literatur yang ditelaah dapat dikelompokkan menjadi tiga domain utama. Domain pertama adalah insider threat, yang mencakup mitigation, detection, human factors, security behaviour, policy compliance, dan opportunity reduction. Domain kedua adalah ethics in software engineering, yang mencakup ethical values, professional responsibility, ethical deliberation, dan developer ethical agency. Domain ketiga adalah secure software development, yang membahas penerapan security pada requirements, design, implementation, testing, dan pengelolaan akses. Pengelompokan tersebut menunjukkan bahwa penelitian tentang insider threat dan etika software engineering berkembang luas, tetapi tidak selalu menggunakan kerangka konseptual yang sama.

Pada domain insider threat, Inayat et al. memberikan landasan paling langsung karena fokusnya adalah systematic review terhadap metode mitigasi insider threat dan pemetaan jenis serangan terhadap strategi prevention dan detection Pathirana et al. memperluas perspektif dengan human factors dan menganalisis 121 studi dari 2014 hingga Oktober 2025. Prabhu dan Dell meninjau 123 artikel mengenai insider cybersecurity behaviour Balagopal dan Mathew memetakan faktor compliance dan violation terhadap information security policy Bersama-sama, penelitian tersebut menunjukkan bahwa insider threat merupakan persoalan lintas teknologi dan perilaku.

Pada domain etika, Alidoosti et al. menyaring 623 artikel menjadi 85 primary studies dan menghasilkan value model untuk mengkategorikan ethical values serta hubungan antarnilai. Gogoll et al. menekankan keterbatasan codes of conduct sebagai sumber orientasi etis yang berdiri sendiri dan mengusulkan ethical deliberation dalam tim pengembang. Biabie et al. mengembangkan framework etika pada requirements engineering untuk meminimalkan persoalan etis pada tahap tersebut. Griffin et al. kemudian memperlihatkan bahwa developer mempunyai ethical agency dan dapat membuat keputusan etis dalam pekerjaan, walaupun agency tersebut dipengaruhi konteks pekerjaan.

Pada domain pengembangan aman, Nina et al. dan Khan et al. memperlihatkan bahwa security harus ditempatkan sepanjang SDLC. Rezaei Nasab et al. mengidentifikasi 28 security practices khusus untuk microservices dan memvalidasinya dengan practitioner survey. Weir et al. menunjukkan bahwa intervensi yang berpusat pada developer dapat membantu tim memprioritaskan security dan privacy. Halme et al. menunjukkan bahwa prinsip etika dapat diterjemahkan ke praktik melalui Ethical User Stories. Hasil ini memperkuat bahwa etika dan keamanan tidak seharusnya hanya menjadi dokumen tambahan, tetapi perlu diterjemahkan menjadi aktivitas pengembangan.

### 3.2. Prinsip Etika Profesi yang Relevan

Sintesis literatur menunjukkan enam prinsip yang paling konsisten dan relevan dengan insider threat, yaitu privacy, confidentiality, security, responsibility, accountability, dan professional judgment. Keenam prinsip tersebut disarikan dari kode etik software engineering dan literatur etika software development, kemudian dihubungkan dengan risiko yang dibahas pada literatur insider threat.

Privacy berkaitan dengan pembatasan penggunaan dan akses terhadap informasi pribadi. Dalam pekerjaan pengembangan, akses terhadap data dapat muncul ketika developer melakukan debugging, testing, migration, atau maintenance. Karena itu, akses teknis terhadap data tidak dapat diperlakukan sebagai izin etis untuk melihat seluruh informasi. Prinsip ini diperkuat oleh temuan Jeong dan Zo bahwa kontrol keamanan yang terlalu intrusif dapat memunculkan privacy intrusion dan memengaruhi respons terhadap kebijakan.

Confidentiality berkaitan dengan kewajiban melindungi informasi agar hanya dapat digunakan oleh pihak yang berwenang. Pada pengembangan, informasi sensitif dapat meliputi source code, credentials, API keys, database records, konfigurasi, dan dokumen internal. IEEE-CS/ACM Code of Ethics mengharuskan software engineer mempertimbangkan dampak pekerjaan dan menggunakan professional judgment secara bertanggung jawab.

Security berkaitan dengan tanggung jawab untuk mengurangi risiko yang dapat ditimbulkan oleh software maupun proses pengembangannya. Rindell et al. menunjukkan bahwa praktik security paling awal dalam lifecycle cenderung dipersepsikan lebih berdampak. Weir et al. juga menunjukkan bahwa developer engagement dapat membantu mengidentifikasi dan memprioritaskan persoalan security serta privacy. Responsibility dan accountability berhubungan dengan siapa yang bertanggung jawab terhadap keputusan dan aktivitas selama pengembangan. Gogoll et al. menunjukkan bahwa ethical deliberation diperlukan karena kode etik tidak selalu menyediakan jawaban spesifik untuk setiap kondisi. Accountability selanjutnya membutuhkan kemampuan menelusuri aktivitas melalui logging, audit trail, dan pembagian kewenangan.

Professional judgment menjadi penting ketika developer memiliki kemampuan teknis yang lebih besar daripada hak akses yang sebenarnya dibutuhkan. Prinsip ini menegaskan bahwa kemampuan untuk melakukan suatu tindakan berbeda dengan kewenangan untuk melakukannya. Separation of Duty memperkuat pemisahan tersebut dengan membagi fungsi kritis kepada beberapa pengguna agar satu individu tidak mengendalikan seluruh proses.

**Tabel 2. Pemetaan prinsip etika dan risiko insider threat**

| Prinsip etika         | Potensi pelanggaran                       | Bentuk risiko             | Mekanisme pencegahan                     |
|-----------------------|-------------------------------------------|---------------------------|------------------------------------------|
| Privacy               | Mengakses data di luar kebutuhan tugas    | Unauthorized access       | Access control, data minimization        |
| Confidentiality       | Mengungkapkan informasi rahasia           | Data leakage              | Least privilege, encryption, restriction |
| Security              | Menggunakan privilege secara berlebihan   | Privilege abuse           | IAM, authentication, monitoring          |
| Responsibility        | Mengabaikan prosedur keamanan             | Negligence                | Secure SDLC, security review             |
| Accountability        | Aktivitas tidak dapat ditelusuri          | Unauthorized modification | Logging, audit trail                     |
| Professional judgment | Menggunakan akses karena kemampuan teknis | Misuse of privilege       | RBAC, approval, separation of duties     |

### 3.3. Bentuk dan Faktor Insider Threat

Bentuk insider threat yang muncul dalam literatur dapat dikelompokkan berdasarkan niat dan cara penggunaan hak akses. Malicious insider menggunakan akses secara sengaja untuk memperoleh keuntungan, merusak sistem, membocorkan data, atau melakukan tindakan lain yang merugikan organisasi. Unintentional insider muncul ketika individu melakukan kesalahan, lalai, atau tidak memahami dampak keamanan dari tindakannya. Pathirana et al. secara eksplisit memasukkan kedua kategori tersebut dalam taxonomy human factors untuk insider threat.

Penyalahgunaan hak istimewa merupakan risiko yang sangat relevan bagi pengembang. Developer dapat mempunyai akses ke source code, repository, database, CI/CD pipeline, container registry, cloud environment, dan server. Apabila privilege tersebut tidak dibatasi berdasarkan kebutuhan tugas, ruang untuk penyalahgunaan akan meningkat. Inayat et al. memasukkan privilege

escalation, credential attacks, data loss, exfiltration, sabotage, dan bentuk serangan lain dalam klasifikasi insider threat..

Faktor perilaku juga perlu diperhatikan. Balagopal dan Mathew mengelompokkan penelitian policy violation ke dalam faktor seperti moral disengagement, neutralization, deterrence, stress, dan monitoring. Alraja et al. menunjukkan bahwa fear dan role values berpengaruh terhadap intention to comply, sedangkan habit tidak menunjukkan pengaruh signifikan. . Temuan tersebut menunjukkan bahwa kontrol teknis harus berjalan bersama kebijakan dan kondisi yang mendukung perilaku aman.

Cybersecurity culture menjadi faktor pendukung lain. Georgiadou et al. mengembangkan framework yang mengaitkan insider threat categories dengan security domains serta faktor human, behavioral, dan personal . Temuan tersebut menempatkan aspek manusia dan budaya keamanan sebagai bagian yang perlu diperhatikan dalam pencegahan insider threat.

### **3.4. Mekanisme Pencegahan Insider Threat**

Mekanisme pencegahan yang konsisten pada literatur dapat dikelompokkan menjadi access control, identity and authentication, separation of duties, logging and monitoring, serta secure development practices. Inayat et al. menunjukkan bahwa prevention dan detection perlu dipadukan sesuai tipe ancaman dan sasaran keamanan. Groll et al. menempatkan Separation of Duty sebagai prinsip fundamental untuk membagi tugas kritis di antara beberapa pengguna sehingga mengurangi peluang fraud atau penyalahgunaan.

Least privilege menjadi mekanisme penting karena membatasi akses hanya pada sumber daya yang diperlukan untuk menjalankan fungsi. Pada konteks developer, penerapan prinsip ini berarti akses ke production database, deployment credential, atau administrative interface tidak otomatis diberikan hanya karena seseorang berada dalam tim pengembangan. Pembatasan privilege dapat mengurangi dampak ketika akun internal disalahgunakan maupun ketika kredensial jatuh ke pihak lain. Access control perlu didukung identity and authentication yang tepat. Role-based access control dapat menghubungkan hak akses dengan tanggung jawab pekerjaan, sedangkan authentication dan pengelolaan akun membantu memastikan bahwa aktivitas dilakukan oleh identitas yang tepat. Groll et al. menunjukkan bahwa kontrol separation of duty berkaitan dengan pengurangan konflik kepentingan dan pemisahan fungsi kritis. Dalam praktik pengembangan, pemisahan antara developer, reviewer, tester, dan deployer dapat mengurangi konsentrasi hak istimewa pada satu individu.

Logging dan audit trail berfungsi memperkuat accountability. Aktivitas seperti perubahan source code, pemberian privilege, perubahan konfigurasi, akses ke data sensitif, dan deployment sebaiknya dapat ditelusuri. Mekanisme tersebut tidak selalu mencegah tindakan pertama, tetapi meningkatkan kemampuan organisasi untuk mendeteksi, menelusuri, dan merespons perilaku yang menyimpang. Al-Mhiqani et al. menunjukkan bahwa detection merupakan bagian penting dari pengelolaan insider threat, termasuk pada lingkungan cyber-physical systems.

Monitoring perlu diterapkan secara proporsional. Jeong dan Zo menunjukkan bahwa hard opportunity-reducing techniques dapat dirasakan terlalu intrusif oleh pekerja dan berhubungan dengan privacy-security trade-off [8]. Karena itu, monitoring perlu memiliki tujuan yang jelas, batas akses, mekanisme audit, dan perlindungan terhadap data monitoring. Prinsip ini membuat ethical responsibility tetap menjadi bagian dari desain kontrol keamanan.

### **3.5. Integrasi Etika ke dalam Software Development Life Cycle**

Integrasi etika dan pencegahan insider threat dapat dilakukan sepanjang SDLC. Pada requirements, kebutuhan akses dan data sensitif sebaiknya ditentukan sejak awal. Bioble et al. menunjukkan bahwa requirements engineering dapat memunculkan berbagai persoalan etis dan membutuhkan framework untuk menguranginya. Halme et al. menunjukkan bahwa Ethical User Stories dapat digunakan untuk menerjemahkan prinsip etika menjadi bagian dari requirements dan fitur.

Pada design, prinsip least privilege dan separation of duties dapat diterjemahkan menjadi arsitektur role dan access control. Sistem dapat memisahkan role developer, tester, reviewer, administrator, dan deployer sehingga fungsi kritis tidak terkonsentrasi pada satu pihak. Groll et al.

menunjukkan bahwa SoD dirancang untuk membagi tugas kritis agar peluang fraud berkurang. Pada construction, developer perlu menerapkan secure coding, code review, pengelolaan secret, dan pembatasan akses terhadap data produksi. Rezaei Nasab et al. menunjukkan adanya 28 security practices yang relevan pada microservices systems, termasuk praktik yang berkaitan dengan konfigurasi dan pengelolaan keamanan. Rindell et al. juga menunjukkan bahwa security activities pada fase awal dan implementation menjadi bagian penting dalam praktik agile software development.

Pada testing, penggunaan data produksi perlu dikendalikan agar tidak membuka akses yang tidak diperlukan. Prinsip privacy dan confidentiality dapat diterjemahkan ke penggunaan data yang dimasking, synthetic data, atau environment terisolasi sesuai kebutuhan. Nina et al. serta Khan et al. menunjukkan bahwa testing dan quality assurance merupakan bagian dari secure software development, bukan aktivitas yang berdiri sendiri setelah coding. Pada deployment dan maintenance, hak akses perlu disesuaikan dengan kebutuhan aktual, termasuk pencabutan akses ketika peran berubah atau hubungan kerja berakhir. Logging, audit trail, monitoring, dan review privilege perlu diterapkan secara berkelanjutan. Weir et al. menunjukkan bahwa keterlibatan developer dapat membantu tim mengidentifikasi dan memprioritaskan persoalan security dan privacy.

### 3.6. Perbandingan dengan Penelitian Terdahulu

Penelitian ini berada pada titik temu beberapa kelompok literatur. Inayat et al. berfokus pada mitigasi insider threat, Pathirana et al. pada human factors, dan Prabhu dan Dell pada insider cybersecurity behavior. Di sisi lain, Alidoosti et al., Gogoll et al., Biabie et al., Marebane dan Hans, serta Griffin et al. membahas ethical values, professional responsibility, dan ethical agency dalam software development. Literatur secure software development kemudian memberikan mekanisme teknis yang dapat digunakan untuk mengoperasionalkan kewajiban tersebut.

Penelitian nasional juga perlu diposisikan secara hati-hati. Nurmiati dan Aqeel membahas etika profesi TI sebagai instrumen menghadapi cyber crime di Indonesia, sedangkan Anugrah et al. menelaah etika profesi dan keamanan informasi pada konteks kebocoran data BSI. Bayhaqi et al. memetakan dimensi etika profesi dalam pengembangan dan pengelolaan sistem informasi. Penelitian ini berbeda dalam fokus sintesis karena menjadikan prinsip etika pengembang sebagai titik awal untuk memetakan bentuk insider threat, sasaran keamanan, dan mekanisme pencegahan secara bersama-sama.

Penelitian empirical tentang ethical concerns juga menunjukkan bahwa etika dapat muncul dalam berbagai tahap software lifecycle. Tjikhoeeri et al. menganalisis lima juta app-store reviews dan menemukan bahwa pengguna melaporkan berbagai ethical concerns seperti identity theft dan safety. Cociancig et al. menunjukkan bagaimana prinsip etika muncul dalam collaborative ideation processes dan menekankan pentingnya praktik yang lebih konkret dalam pengembangan AI. Temuan tersebut mendukung kebutuhan untuk mengubah prinsip etika dari pernyataan abstrak menjadi praktik yang dapat ditelusuri dalam proses pengembangan.

### 3.7. Sintesis Integratif

Sintesis menunjukkan bahwa etika profesi dapat diposisikan sebagai lapisan normatif, sedangkan kontrol keamanan merupakan lapisan operasional. Privacy dan confidentiality memberi alasan mengapa akses harus dibatasi; security dan responsibility memberi alasan mengapa keamanan harus diperhatikan sejak proses development; accountability memberi dasar untuk logging dan auditability; sedangkan professional judgment memberi batas bahwa kemampuan teknis tidak sama dengan kewenangan teknis.

Hubungan tersebut menghasilkan rantai konseptual: prinsip etika membentuk batas perilaku yang diharapkan, batas tersebut menentukan risiko perilaku internal yang perlu dikendalikan, risiko menentukan sasaran keamanan yang harus dilindungi, dan sasaran keamanan menentukan kontrol pencegahan yang sesuai. Misalnya, pelanggaran confidentiality dapat muncul melalui data leakage; risiko tersebut menuntut least privilege, access restriction, dan monitoring. Demikian juga, pelanggaran accountability dapat meningkatkan kesulitan penelusuran aktivitas sehingga logging dan audit trail menjadi mekanisme pendukung. Kerangka tersebut juga memperlihatkan bahwa kontrol

teknis tidak dapat berdiri sendiri. Jeong dan Zo menunjukkan bahwa kontrol yang terlalu invasif dapat garuhi faktor psikologis dan nilai peran. Dengan demikian, pencegahan insider threat yang berkelanjutan memerlukan kombinasi governance, technical controls, dan ethical decision-making.

**Tabel 3. Sintesis integratif etika, risiko, dan kontrol**

| Prinsip etika         | Risiko utama                     | Sasaran keamanan                         | Kontrol yang relevan              |
|-----------------------|----------------------------------|------------------------------------------|-----------------------------------|
| Privacy               | Akses data tanpa kebutuhan       | Privacy, confidentiality                 | Access control, data minimization |
| Confidentiality       | Kebocoran informasi              | Confidentiality                          | Least privilege, encryption       |
| Security              | Privilege abuse                  | Confidentiality, integrity, availability | IAM, authentication, monitoring   |
| Responsibility        | Kelalaian atau insecure practice | Integrity, availability                  | Secure SDLC, security review      |
| Accountability        | Aktivitas tidak dapat ditelusuri | Integrity                                | Logging, audit trail              |
| Professional judgment | Penyalahgunaan kewenangan        | All CIA objectives                       | RBAC, approval, SoD               |

## KESIMPULAN

Penelitian ini menunjukkan bahwa etika profesi pengembang sistem informasi mempunyai hubungan yang erat dengan pencegahan insider threat. Prinsip privacy, confidentiality, security, responsibility, accountability, dan professional judgment dapat digunakan sebagai dasar untuk menentukan perilaku yang diharapkan dari pengembang ketika berhadapan dengan data, source code, privilege, dan lingkungan sistem. Literatur menunjukkan bahwa insider threat dapat muncul melalui tindakan malicious maupun unintentional dan dipengaruhi oleh human factors, security behaviour, policy compliance, budaya keamanan, serta penyalahgunaan akses. Hasil sintesis menunjukkan bahwa prinsip etika dapat diterjemahkan menjadi mekanisme operasional berupa access control, least privilege, authentication, separation of duties, logging dan audit trail, monitoring, serta secure software development practices. Pemetaan integratif yang dihasilkan menempatkan etika sebagai dasar normatif dan kontrol keamanan sebagai mekanisme operasional yang saling melengkapi. Kerangka tersebut dapat digunakan sebagai dasar konseptual untuk mengintegrasikan tanggung jawab profesional dengan pengendalian keamanan sejak requirements hingga maintenance. Penelitian selanjutnya dapat memvalidasi pemetaan ini melalui studi kasus organisasi atau pengembangan instrumen evaluasi tanpa mengubah prinsip dasar sintesis yang dihasilkan dari literatur.

## SUMBER RUJUKAN

U. Inayat, M. Farzan, S. Mahmood, M. F. Zia, S. Hussain, and F. Pallonetto, "Insider threat mitigation: Systematic literature review," *Ain Shams Engineering Journal*, vol. 15, no. 12, Art. no. 103068, 2024. doi: 10.1016/j.asej.2024.103068

- N. Pathirana, R. Roberts, H. Kalutarage, and C. D. McDermott, "Integrating human factors into insider threat detection – A systematic review," *ACM Computing Surveys*, vol. 58, no. 10, Art. no. 260, pp. 1–37, 2026. doi: 10.1145/3798089
- S. Prabhu and P. Dell, "A structured review of insider cybersecurity behaviour studies," *Information Security Journal: A Global Perspective*, vol. 34, no. 6, pp. 655–682, 2025. doi: 10.1080/19393555.2025.2543458
- N. Balagopal and S. K. Mathew, "Exploring the factors influencing information security policy compliance and violations: A systematic literature review," *Computers & Security*, vol. 147, Art. no. 104062, 2024. doi: 10.1016/j.cose.2024.104062
- M. N. Al-Mhiqani, T. Alsoubi, T. Al-Shehari, K. H. Abdulkareem, R. Ahmad, and M. A. Mohammed, "Insider threat detection in cyber-physical systems: A systematic literature review," *Computers & Electrical Engineering*, vol. 119, Art. no. 109489, 2024. doi: 10.1016/j.compeleceng.2024.109489
- F. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," *IEEE Access*, vol. 12, pp. 30907–30927, 2024. doi: 10.1109/ACCESS.2024.3369906
- A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting insider threat via a cyber-security culture framework," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 706–716, 2022. doi: 10.1080/08874417.2021.1903367
- M. Jeong and H. Zo, "Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques," *Telematics and Informatics*, vol. 63, Art. no. 101670, 2021. doi: 10.1016/j.tele.2021.101670
- R. Alidoosti, P. Lago, M. Razavian, and A. Tang, "Exploring ethical values in software systems: A systematic literature review," *Journal of Systems and Software*, vol. 226, Art. no. 112430, 2025. doi: 10.1016/j.jss.2025.112430
- J. Gogoll, N. Zuber, S. Kacianka, T. Greger, A. Pretschner, and J. Nida-Rümelin, "Ethics in the software development process: From codes of conduct to ethical deliberation," *Philosophy & Technology*, vol. 34, pp. 1085–1108, 2021. doi: 10.1007/s13347-021-00451-w
- S. E. Biabale, N. M. Garcia, and D. Midekso, "Proposed ethical framework for software requirements engineering," *IET Software*, vol. 17, no. 4, pp. 526–537, 2023. doi: 10.1049/sfw2.12136
- H. Nina, J. A. Pow-Sang, and M. Villavicencio, "Systematic mapping of the literature on secure software development," *IEEE Access*, vol. 9, pp. 36852–36867, 2021. doi: 10.1109/ACCESS.2021.3062388
- R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic literature review on security risks and its practices in secure software development," *IEEE Access*, vol. 10, pp. 5456–5481, 2022. doi: 10.1109/ACCESS.2022.3140181
- S. Groll, L. Fuchs, and G. Pernul, "Separation of duty in information security," *ACM Computing Surveys*, vol. 57, no. 7, Art. no. 180, pp. 1–35, 2025. doi: 10.1145/3715959
- Z. Zulkifli, N. H. binti Abd Rahim, T. Alam, F. H. Yusoff, and M. M. Rahman, "Uncovering ethical values in information systems development methodologies: A systematic literature review," *Malaysian Journal of Computing*, vol. 11, no. 1, pp. 2421–2436, 2026. doi: 10.24191/mjoc.v011i1.9810
- M. N. Alraja, U. J. Butt, and M. Abbod, "Information security policies compliance in a global setting: An employee's perspective," *Computers & Security*, vol. 129, Art. no. 103208, 2023. doi: 10.1016/j.cose.2023.103208
- A. Rezaei Nasab, M. Shahin, S. A. Hoseyni Raviz, P. Liang, A. Mashmool, and V. Lenarduzzi, "An empirical study of security practices for microservices systems," *Journal of Systems and Software*, vol. 198, Art. no. 111563, 2023. doi: 10.1016/j.jss.2022.111563
- C. Weir, I. Becker, and L. Blair, "Incorporating software security: Using developer workshops to engage product managers," *Empirical Software Engineering*, vol. 28, Art. no. 21, 2023. doi: 10.1007/s10664-022-10252-0

- E. Halme, M. Jantunen, V. Vakkuri, K. K. Kemell, and P. Abrahamsson, "Making ethics practical: User stories as a way of implementing ethical consideration in Software Engineering," *Information and Software Technology*, vol. 167, Art. no. 107379, 2024. doi: 10.1016/j.infsof.2023.107379
- T. A. Griffin, B. P. Green, and J. V. M. Welie, "The ethical agency of AI developers," *AI and Ethics*, vol. 4, pp. 179–188, 2024. doi: 10.1007/s43681-022-00256-3
- N. Tjikhoei, L. Olson, and E. Guzmán, "The best ends by the best means: Ethical concerns in app reviews," *Empirical Software Engineering*, vol. 29, Art. no. 138, 2024. doi: 10.1007/s10664-024-10463-7
- S. M. Marebane and R. T. Hans, "A comparative study on the ethical responsibilities of key role players in software development," *Software*, vol. 2, no. 4, pp. 504–516, 2023. doi: 10.3390/software2040023
- C. Cociancig, H. Heuer, and A. Breiter, "AI ethics unwrapped: An empirical investigation of ethical principles in collaborative ideation processes," *AI Ethics*, vol. 5, pp. 3159–3172, 2025. doi: 10.1007/s43681-024-00638-9
- E. Nurmiati and M. F. Aqeel, "Tinjauan etika profesi IT dalam menghadapi ancaman cyber crime di Indonesia," *Jurnal Sistem Informasi dan Ilmu Komputer*, vol. 4, no. 2, pp. 13–22, 2026. doi: 10.59581/jusiik-widyakarya.v4i2.6168
- S. Anugrah, M. Z. Himawan, N. R. Qalby, and E. Nurmiati, "Pengaruh etika profesi terhadap keamanan informasi dalam konteks kebocoran data BSI (Bank Syariah Indonesia): Studi literatur sistematis," *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, vol. 11, no. 2,
- A. Bayhaqi, A. S. Rohyan, and L. Swastina, "Etika profesi dalam pengembangan dan pengelolaan sistem informasi di era transformasi digital," *Majalah Ilmiah METHODDA*, vol. 16, no. 2, pp. 204–210, 2026. doi: 10.46880/methoda.Vol16No2.pp204-210
- K. Rindell, J. Ruohonen, J. Holvitie, S. Hyrynsalmi, and V. Leppänen, "Security in agile software development: A practitioner survey," *Information and Software Technology*, vol. 131, Art. no. 106488, 2021. doi: 10.1016/j.infsof.2020.106488
- IEEE-CS/ACM Joint Task Force on Software Engineering Ethics and Professional Practices, "Software engineering code of ethics and professional practice," *Science and Engineering Ethics*, vol. 7, no. 2, pp. 231–238, 2001. doi: 10.1007/s11948-001-0044-4
- M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, Art. no. n71, 2021. doi: 10.1136/bmj.n71