FRAUD MANAGEMENT SYSTEM

UPT Teknologi Informasi dan Pangkalan Data
Institut Agama Islam Negeri Manado

Daftar Isi

BAB I : Pendahuluan *1*

1. Pendahuluan 1

BAB II : Pelaksanaan *5*

1. Definisi 5
2. Prinsip Dasar 6
3. Peran dan Tanggung Jawab 11
4. Prosedur Pencegahan 14
5. Prosedur Deteksi 17
6. Prosedur Penanganan 18
7. Pemantauan dan Evaluasi 20
8. Penegakan Kebijakan 21

BAB III : Penutup *23*

1. Kesimpulan 23

Lampiran 24

BAB I : Pendahuluan

1. Pendahuluan

a. Latar Belakang

Dalam era digital yang semakin maju, teknologi informasi telah menjadi tulang punggung utama dalam berbagai aktivitas di IAIN Manado, termasuk dalam bidang akademik, keuangan, administrasi, dan layanan digital lainnya. UPT TIPD, sebagai unit yang bertanggung jawab atas pengelolaan teknologi informasi dan pangkalan data, memegang peran strategis dalam memastikan keberlangsungan dan efisiensi operasional institusi. Namun, seiring dengan perkembangan teknologi ini, muncul pula tantangan yang signifikan, seperti ancaman terhadap keamanan data, kompleksitas infrastruktur IT, dan peningkatan frekuensi serangan siber. Data akademik, keuangan, dan personal mahasiswa maupun dosen menjadi target potensial bagi pelaku kejahatan siber, yang dapat mengakibatkan akses tidak sah, pencurian informasi, hingga manipulasi data. Di sisi lain, kesadaran pengguna terhadap risiko fraud masih menjadi tantangan, sehingga membuka celah terhadap potensi penyalahgunaan sistem.

Tanpa penerapan fraud management yang efektif, UPT TIPD menghadapi risiko kerugian besar, baik secara materiil maupun non-materiil. Insiden fraud dapat merusak reputasi institusi, mengganggu operasional sistem, serta menyebabkan pelanggaran terhadap regulasi yang berlaku. Gangguan terhadap layanan digital seperti sistem informasi akademik, portal keuangan, dan pembelajaran daring akan berdampak langsung pada kualitas pelayanan kepada mahasiswa dan dosen. Oleh karena itu, penerapan fraud management yang terstruktur dan komprehensif sangat diperlukan untuk melindungi integritas sistem, menjaga kepercayaan pengguna, dan mendukung visi IAIN Manado sebagai institusi pendidikan tinggi yang unggul dan religious.

b. Tujuan

Berikut adalah tujuan dari adanya Fraud Management System di IAIN Manado :

1) **Menjamin Keamanan Sistem Informasi**

   Melindungi seluruh sistem informasi akademik, keuangan, dan layanan digital di lingkungan IAIN Manado dari risiko penipuan atau penyalahgunaan data.

2) **Meningkatkan Kepercayaan Pengguna**

   Membangun kepercayaan dosen, mahasiswa, dan tenaga kependidikan terhadap keandalan serta integritas layanan teknologi informasi yang disediakan oleh UPT TIPD.

3) **Mencegah Kerugian Institusi**

   Meminimalkan potensi kerugian materiil maupun non-materiil akibat insiden fraud, seperti pencurian data, manipulasi sistem, atau akses ilegal.

4) **Memastikan Kepatuhan terhadap Regulasi**

   Mematuhi peraturan pemerintah dan standar keamanan informasi nasional maupun internasional, seperti Peraturan Menteri Komunikasi dan Informatika atau ISO 27001.

5) **Meningkatkan Efisiensi Operasional**

   Mengoptimalkan pengelolaan sumber daya teknologi informasi dengan menerapkan langkah-langkah pencegahan fraud yang terstruktur dan efisien.

6) **Mendukung Tata Kelola yang Transparan**

   Mendukung penerapan tata kelola yang akuntabel dan transparan dalam pengelolaan data dan layanan digital di IAIN Manado.

7) **Mengidentifikasi dan Menangani Risiko Fraud secara Cepat**

   Mengembangkan kemampuan deteksi dini untuk mengidentifikasi aktivitas mencurigakan serta merespons secara efektif guna mencegah dampak negatif yang lebih besar.

8) **Memberikan Edukasi tentang Fraud Management**

   Meningkatkan kesadaran seluruh staf dan pengguna layanan digital di IAIN Manado mengenai pentingnya tindakan pencegahan terhadap fraud.

c. Lingkup

Kebijakan ini berlaku untuk seluruh perangkat keras, perangkat lunak, data, dan sistem yang dikelola oleh UPT TIPD.

1) **Keamanan Data dan Informasi**

   Melindungi data akademik, keuangan, personal, dan administratif dari akses tidak sah, manipulasi, atau pencurian. Mengamankan sistem informasi akademik (SIA), Learning Management System (LMS), dan basis data lainnya dengan mekanisme keamanan seperti enkripsi dan autentikasi multi-faktor.

2) **Infrastruktur Teknologi Informasi**

   Mengawasi dan memitigasi risiko pada perangkat keras (server, komputer, perangkat jaringan) dan perangkat lunak yang digunakan di UPT TIPD. Mencegah kerentanan sistem dari serangan malware, ransomware, atau hacking.

3) **Pengelolaan Akses Sistem**

   Memberikan hak akses berdasarkan prinsip least privilege (akses minimum yang diperlukan). Mengelola autentikasi pengguna untuk sistem informasi dan layanan online yang dikelola UPT TIPD, seperti portal mahasiswa dan dosen.

4) **Aktivitas Operasional IT**

   Mengawasi aktivitas rutin seperti pengelolaan server, pemeliharaan perangkat lunak, dan pembaruan sistem untuk mencegah potensi fraud. Memantau log sistem untuk mendeteksi aktivitas mencurigakan atau anomali.

5) **Layanan Digital untuk Pengguna**

   Melindungi portal layanan mahasiswa, dosen, dan tenaga kependidikan dari potensi fraud seperti manipulasi data akademik atau penyalahgunaan fitur pembayaran online. Menyediakan mekanisme pelaporan yang aman bagi pengguna untuk melaporkan aktivitas mencurigakan.

6) **Kesadaran dan Edukasi Keamanan**

   Memberikan pelatihan dan sosialisasi kepada staf, dosen, dan mahasiswa tentang bahaya fraud dan cara mencegahnya, seperti mengenali phishing atau

social engineering. Menyusun panduan dan kebijakan terkait keamanan informasi yang mudah dipahami oleh pengguna.

7) **Kepatuhan terhadap Regulasi**

   Memastikan bahwa seluruh aktivitas teknologi informasi di UPT TIPD mematuhi regulasi nasional dan standar internasional, seperti UU ITE, ISO 27001, atau standar lainnya yang relevan. Mendokumentasikan semua proses dan kebijakan terkait untuk memenuhi persyaratan audit.

8) **Penanganan Insiden dan Pemulihan**

   Membentuk tim tanggap insiden untuk menangani kasus fraud IT dengan cepat dan efektif. Menyusun rencana pemulihan (disaster recovery plan) untuk mengembalikan sistem ke kondisi normal setelah insiden fraud.

Sehingga lingkup dari Fraud Management IT oleh UPT TIPD adalah 8 poin utama diatas dan merupakan tugas pokok institusi yang dilaksanakan.

BAB II : Pelaksanaan

1. Definisi

a. Fraud

Fraud merupakan tindakan yang disengaja oleh individu atau kelompok untuk memperoleh keuntungan secara tidak sah atau menghindari kerugian dengan cara menipu, memanipulasi, atau menyalahgunakan kepercayaan dalam berbagai konteks, baik keuangan maupun non-keuangan. Albrecht et al. (2015) mendefinisikan fraud sebagai perilaku ilegal yang melibatkan penyalahgunaan sistem atau hubungan kepercayaan untuk mencapai tujuan tertentu yang melanggar hukum. Menurut Singleton dan Singleton (2010), fraud juga mencakup tindakan penipuan atau penyembunyian fakta untuk menipu pihak lain demi mendapatkan keuntungan pribadi. Hal ini menunjukkan bahwa fraud bukan hanya berkaitan dengan tindakan kriminal, tetapi juga mencakup pelanggaran etika yang dapat merugikan individu maupun organisasi..

b. Fraud IT

Fraud dalam teknologi informasi (IT) adalah tindakan penipuan yang dilakukan dengan memanfaatkan sistem, perangkat lunak, data, atau infrastruktur IT untuk memperoleh keuntungan ilegal atau menyebabkan kerugian pada pihak lain. Menurut Rainer et al. (2016), fraud dalam IT mencakup aktivitas seperti pencurian data, manipulasi sistem, penyalahgunaan akses, dan tindakan lain yang bertujuan untuk merugikan atau mengambil keuntungan dari kelemahan sistem informasi. Hall (2018) menambahkan bahwa fraud dalam IT sering kali melibatkan penyalahgunaan teknologi canggih untuk menghindari deteksi, seperti penggunaan malware, ransomware, atau rekayasa sosial (social engineering).

Fraud dalam IT terus berkembang seiring dengan kemajuan teknologi dan meningkatnya ketergantungan organisasi pada sistem digital. Beberapa bentuk umum fraud IT meliputi:

- **Phishing**

  Penipuan yang bertujuan untuk mencuri informasi sensitif, seperti kredensial login atau data kartu kredit, melalui email atau situs web palsu.
- **Identity Theft**

  Penyalahgunaan identitas seseorang untuk mengakses sistem atau informasi tertentu.
- **Unauthorized Access**

  Akses ilegal ke sistem atau data tanpa otorisasi yang sah.
- **Data Manipulation**

  Pengubahan atau pemalsuan data dalam sistem untuk keuntungan tertentu.
- **Insider Fraud**

  Penipuan yang dilakukan oleh individu dari dalam organisasi, seperti karyawan atau mitra bisnis, yang memiliki akses ke sistem IT.

Fraud dalam IT memiliki dampak serius, baik secara materiil maupun non-materiil. Dampak finansial mencakup kerugian akibat pencurian data atau kerusakan sistem, sementara dampak non-materiil dapat berupa hilangnya kepercayaan pelanggan atau reputasi organisasi. Oleh karena itu, strategi mitigasi fraud dalam IT sangat penting, termasuk penerapan teknologi keamanan seperti enkripsi data, firewall, dan sistem deteksi intrusi, serta edukasi pengguna untuk meningkatkan kesadaran terhadap ancaman fraud.

2. Prinsip Dasar

a. Pencegahan

Pencegahan fraud dalam manajemen TI di IAIN Manado, khususnya oleh UPT TIPD, didasarkan pada beberapa prinsip utama yang bertujuan untuk melindungi integritas sistem informasi dan data institusi.

1) Keamanan Berlapis (defense in depth)

   Yang mencakup penggunaan berbagai teknologi keamanan seperti firewall, enkripsi data, dan sistem deteksi intrusi untuk mencegah ancaman baik dari luar maupun dalam.

2) Hak akses minimum (least privilege)

   Diterapkan dengan memberikan hak akses kepada pengguna hanya sesuai dengan kebutuhan pekerjaannya, guna mengurangi risiko penyalahgunaan akses.

3) Log Audit

   Transparansi dan akuntabilitas juga menjadi prinsip penting, dengan mencatat setiap aktivitas dalam sistem IT secara jelas melalui log audit, serta menyediakan saluran pelaporan insiden yang mudah diakses dan transparan. Untuk mendeteksi dan mencegah fraud secara dini, deteksi dan pencegahan dini dilakukan dengan menggunakan alat analitik dan algoritma pendeteksi anomali yang memantau aktivitas sistem secara real-time.

4) Edukasi dan Kesadaran Pengguna

   Bagian tak terpisahkan dalam pencegahan fraud, dengan memberikan pelatihan rutin kepada staf, dosen, dan mahasiswa mengenai ancaman siber, seperti phishing dan malware. Kepatuhan terhadap standar dan regulasi juga dijaga dengan mengikuti standar internasional seperti ISO 27001 dan mematuhi regulasi nasional seperti UU ITE, serta menyusun kebijakan internal yang sesuai.

5) Evaluasi dan Perbaikan Berkelanjutan

   Dilakukan melalui audit rutin untuk mengidentifikasi kerentanan dan memperbarui sistem keamanan guna menghadapi ancaman baru. Pengendalian proaktif juga diterapkan dengan memantau dan menganalisis potensi risiko fraud secara terus-menerus, serta mengantisipasi dan mengatasi ancaman sebelum terjadi melalui kebijakan dan prosedur yang jelas, seperti pembaruan perangkat lunak dan sistem secara berkala.

6) Kolaborasi dan Pengawasan Terintegrasi

   UPT TIPD dan unit kerja lainnya serta keterlibatan pihak ketiga seperti konsultan IT atau auditor eksternal, memastikan sistem pengawasan yang efektif dan objektif dalam mengelola potensi risiko fraud.

Dengan prinsip-prinsip ini, IAIN Manado berkomitmen untuk menciptakan lingkungan TI yang aman, transparan, dan bebas dari fraud, serta siap untuk menangani potensi risiko secara proaktif sebelum merugikan institusi.

b. Deteksi

Untuk mendeteksi dini dan mengidentifikasi tindakan fraud secara cepat melalui sistem pemantauan, penting untuk menerapkan beberapa pendekatan teknis. Salah satunya adalah dengan menggunakan

1) Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS), yang memantau dan menganalisis trafik jaringan untuk mendeteksi serta mencegah akses tidak sah. Selain itu, User Behavior Analytics (UBA) dapat digunakan untuk memantau aktivitas pengguna dan mendeteksi pola perilaku yang mencurigakan, seperti akses tidak sah atau aktivitas yang tidak sesuai dengan pola normal. Deteksi anomali juga dapat dilakukan dengan memanfaatkan algoritma machine learning untuk mengidentifikasi pola yang tidak biasa dalam data, serta menganalisis log sistem untuk mendeteksi tindakan yang mencurigakan, seperti transaksi yang tidak biasa atau perubahan data yang tidak sah. Sistem ini juga dapat dilengkapi dengan automated alerts yang memberi peringatan secara real-time ketika terdeteksi aktivitas mencurigakan, seperti login berulang dari lokasi atau perangkat yang tidak dikenal.
2) Penting untuk memastikan bahwa setiap aksi yang dilakukan dalam sistem tercatat dengan jelas dalam audit trail atau log aktivitas. Dengan demikian, setiap penyalahgunaan atau manipulasi data dapat dideteksi lebih cepat. Sistem keamanan berlapis yang menggabungkan firewall, enkripsi data, dan autentikasi ganda juga dapat memperkuat perlindungan terhadap fraud. Semua pendekatan ini perlu didukung oleh tim yang terlatih untuk memantau dan merespons dengan cepat terhadap potensi ancaman, serta memiliki prosedur standar yang jelas dalam menangani kasus fraud. Dengan cara ini, tindakan fraud dapat dideteksi dan ditanggulangi secara efektif dan cepat.

c. Respon

Dalam fraud management di IAIN Manado, tahap respon sangat penting untuk menanggapi setiap potensi atau kejadian fraud yang terdeteksi. Proses respon ini bertujuan untuk mengidentifikasi, menangani, dan memitigasi dampak dari fraud secara efisien. Berikut adalah tahapan respon dalam fraud management yang dapat diterapkan di IAIN Manado:

1) **Penerimaan dan Penilaian Insiden**

   Langkah pertama adalah penerimaan laporan atau deteksi fraud dari sistem pemantauan atau pelaporan internal. Begitu sebuah insiden dicurigai atau teridentifikasi, tim keamanan TI harus melakukan penilaian awal untuk menentukan tingkat keparahan dan potensi dampaknya. Penilaian ini melibatkan pengecekan terhadap bukti yang ada, seperti log sistem, riwayat akses, atau aktivitas yang mencurigakan.

2) **Isolasi dan Pengendalian Dampak**

   Setelah penilaian, tahap selanjutnya adalah mengisolasi insiden fraud untuk mencegah penyebaran lebih lanjut dan mengurangi dampaknya. Ini mungkin melibatkan penghentian akses pengguna yang terlibat, pemutusan koneksi ke jaringan atau sistem yang terkompromi, serta memperketat pengamanan untuk mencegah kejadian serupa di masa mendatang. Pengendalian dampak bertujuan untuk menjaga integritas data dan sistem agar tetap aman.

3) **Investigasi dan Pengumpulan Bukti**

   Setelah insiden terisolasi, tahap berikutnya adalah penyelidikan lebih lanjut untuk mengumpulkan bukti-bukti yang diperlukan untuk menilai secara mendalam siapa yang terlibat, bagaimana kejadian tersebut terjadi, dan sejauh mana kerugian yang ditimbulkan. Pada tahap ini, audit log, rekaman aktivitas, serta jejak digital lainnya akan dianalisis secara mendalam untuk memastikan pemahaman yang jelas mengenai insiden fraud.

4) **Pengambilan Tindakan Korektif dan Pencegahan**

   Setelah penyelidikan selesai dan bukti ditemukan, tim harus mengambil langkah-langkah korektif untuk memperbaiki kelemahan sistem yang memungkinkan fraud terjadi. Ini bisa termasuk memperbarui kebijakan keamanan, memperbaiki kerentanannya, atau memperkenalkan prosedur pengamanan tambahan, seperti perubahan akses atau penggunaan sistem otentikasi yang lebih ketat. Selain itu, langkah-langkah pencegahan perlu

diterapkan untuk mencegah kejadian serupa terjadi di masa depan, seperti memperbarui prosedur keamanan atau menambah lapisan kontrol.

5) **Komunikasi dan Pelaporan**

Selanjutnya, penting untuk memastikan komunikasi yang jelas dan transparan baik kepada pihak internal (seperti pimpinan fakultas atau unit kerja lain) maupun eksternal (misalnya pihak berwenang atau auditor eksternal). Pelaporan yang transparan akan membantu dalam memahami penyebab fraud dan memitigasi risiko di masa depan. Laporan ini harus mencakup detail mengenai insiden, kerugian yang ditimbulkan, serta langkah-langkah yang telah diambil untuk menanganinya.

6) **Pemulihan dan Pemantauan Lanjutan**

Setelah langkah-langkah korektif diterapkan, tahap terakhir adalah pemulihan sistem dan data yang terdampak, serta pemantauan lanjutan untuk memastikan bahwa sistem kembali berfungsi dengan baik dan bebas dari ancaman. Pemulihan ini mencakup pengembalian data yang hilang atau rusak, serta memastikan bahwa operasi kembali berjalan normal. Setelah pemulihan, perlu dilakukan pemantauan lebih lanjut untuk memastikan bahwa fraud tidak terulang kembali dan sistem tetap aman.

7) **Evaluasi dan Pembelajaran**

Setelah insiden fraud ditangani, evaluasi keseluruhan terhadap proses respon perlu dilakukan untuk mengidentifikasi apa yang berjalan dengan baik dan apa yang bisa diperbaiki di masa depan. Pembelajaran dari insiden ini dapat digunakan untuk memperbaiki kebijakan, prosedur, dan sistem untuk memastikan bahwa institusi dapat merespons fraud dengan lebih cepat dan lebih efektif pada kejadian berikutnya.

Dengan mengikuti tahapan respon ini, IAIN Manado melalui UPT TIPD dapat merespons insiden fraud dengan cepat dan efisien, memitigasi dampaknya, serta memperkuat pertahanan terhadap potensi fraud di masa depan.

3. Peran dan Tanggung Jawab

Fraud management di IAIN Manado, khususnya oleh UPT TIPD, melibatkan berbagai pihak dengan peran dan tanggung jawab yang jelas untuk memastikan pencegahan, deteksi, dan respons yang efektif terhadap tindakan fraud. Berikut adalah peran dan tanggung jawab masing-masing pihak yang terlibat dalam fraud management:

a. UPT Teknologi Informasi dan Pangkalan Data (TIPD)

UPT TIPD bertanggung jawab untuk merancang, mengimplementasikan, dan memelihara infrastruktur IT yang aman serta memantau sistem untuk mendeteksi potensi ancaman fraud.

Tanggung Jawab:

- Mengelola dan mengoperasikan sistem pemantauan, termasuk Intrusion Detection System (IDS), sistem audit log, dan perangkat lunak pemantauan lainnya.
- Menyusun dan memperbarui kebijakan keamanan IT untuk mencegah fraud.
- Melakukan penilaian risiko secara berkala untuk mengidentifikasi potensi celah yang dapat dimanfaatkan untuk tindakan fraud.
- Mengimplementasikan pengendalian teknis untuk mencegah akses tidak sah, termasuk otentikasi dua faktor dan enkripsi data.

b. Tim Manajemen Puncak dan Pimpinan Unit Kerja

Manajemen puncak, termasuk rektor dan pimpinan fakultas atau unit lainnya, berperan dalam memberikan dukungan strategis dan memastikan implementasi kebijakan fraud management yang efektif di seluruh organisasi.

Tanggung Jawab:

- Menetapkan visi dan kebijakan fraud management di tingkat institusi.
- Menyediakan sumber daya yang diperlukan, baik dari segi anggaran, teknologi, maupun personel, untuk mendukung upaya pencegahan fraud.
- Memastikan keberlanjutan dan efektivitas dari program fraud management melalui audit internal dan eksternal.

- Mengambil keputusan yang diperlukan setelah laporan terkait insiden fraud diterima dari tim IT.

c. Tim Keamanan Informasi dan Audit Internal

Tim Keamanan Informasi dan Audit Internal bertanggung jawab untuk melakukan evaluasi dan audit secara berkala terhadap kebijakan, prosedur, dan praktik yang ada di IAIN Manado guna memastikan bahwa fraud dapat dideteksi lebih dini dan ditanggulangi dengan tepat.

Tanggung Jawab:

- Melakukan audit berkala terhadap sistem dan kebijakan fraud management untuk memastikan kebijakan yang ada dijalankan dengan benar.
- Melakukan penyelidikan terhadap insiden fraud yang dilaporkan dan memberikan rekomendasi untuk tindak lanjut.
- Membantu dalam perencanaan dan pelaksanaan pelatihan kesadaran fraud bagi staf dan pengguna.

d. Pengguna (Staf, Dosen, dan Mahasiswa)

Setiap pengguna sistem informasi di IAIN Manado, termasuk staf, dosen, dan mahasiswa, memiliki peran penting dalam mencegah fraud melalui kepatuhan terhadap kebijakan dan prosedur yang ada.

Tanggung Jawab:

- Mengikuti pelatihan dan meningkatkan kesadaran mengenai ancaman fraud, seperti phishing, malware, dan social engineering.
- Menggunakan sistem informasi sesuai dengan hak akses yang diberikan dan melaporkan aktivitas yang mencurigakan.
- Menjaga kerahasiaan data pribadi dan data institusi, serta tidak melakukan tindakan yang dapat membahayakan integritas sistem.

e. Tim Respons dan Penanganan Insiden

Tim ini terdiri dari anggota yang terlatih dalam menangani insiden fraud yang terdeteksi, baik secara teknis maupun administratif.

Tanggung Jawab:

- Menanggapi insiden fraud secara cepat dan tepat, termasuk isolasi sistem yang terlibat dan pengumpulan bukti.
- Melakukan investigasi mendalam untuk memahami akar penyebab fraud.
- Bekerja sama dengan tim IT untuk mengimplementasikan langkah-langkah pengendalian yang diperlukan dan memperbaiki kerentanannya.
- Menyusun laporan insiden fraud dan mengkomunikasikan temuan kepada manajemen puncak untuk pengambilan keputusan lebih lanjut.

f. Pihak Eksternal (Konsultan Keamanan dan Auditor)

Pihak eksternal, seperti konsultan keamanan TI dan auditor, memainkan peran dalam memberikan penilaian objektif terhadap kebijakan dan prosedur fraud management yang diterapkan di IAIN Manado.

Tanggung Jawab:

- Melakukan audit independen terhadap kebijakan, prosedur, dan infrastruktur TI untuk memastikan bahwa sistem telah mengimplementasikan kontrol yang memadai untuk mencegah fraud.
- Memberikan saran dan rekomendasi untuk memperbaiki kelemahan dalam sistem dan prosedur yang ada.
- Membantu tim internal dalam mengembangkan rencana respons dan pemulihan setelah insiden fraud.

g. Tim Hukum dan Kepatuhan

Tim hukum dan kepatuhan bertanggung jawab untuk memastikan bahwa tindakan fraud ditanggapi sesuai dengan hukum yang berlaku dan bahwa IAIN Manado mematuhi semua regulasi yang relevan.

Tanggung Jawab:

- Menyusun kebijakan dan prosedur yang sesuai dengan peraturan perundang-undangan, seperti UU ITE, yang mengatur tentang tindak pidana di dunia maya.

- Menyusun prosedur hukum untuk menangani kasus fraud, termasuk pengumpulan bukti yang sah dan melaporkan insiden fraud ke pihak berwenang jika diperlukan.
- Memberikan nasihat hukum kepada manajemen terkait langkah-langkah yang diambil selama proses respons fraud.

Dengan melibatkan berbagai pihak dan menetapkan peran serta tanggung jawab yang jelas, IAIN Manado dapat mengelola fraud secara lebih efektif dan responsif, sehingga melindungi integritas dan keamanan sistem informasi yang digunakan di seluruh lingkungan kampus.

4. Prosedur Pencegahan

Pencegahan fraud dalam manajemen TI di IAIN Manado adalah langkah penting untuk memastikan integritas, keamanan, dan keandalan sistem informasi di lingkungan kampus. Prosedur ini bertujuan untuk mencegah terjadinya tindak fraud sebelum dapat merugikan institusi. Berikut adalah prosedur pencegahan fraud yang dapat diterapkan:

a. Penyusunan Kebijakan Keamanan TI

Langkah pertama dalam pencegahan fraud adalah penyusunan kebijakan keamanan TI yang jelas dan terperinci. Kebijakan ini harus mencakup:

- Hak akses minimum: Menentukan hak akses pengguna berdasarkan kebutuhan kerja mereka untuk mencegah akses yang tidak sah ke sistem dan data.
- Keamanan data: Mengatur pengamanan data pribadi dan institusional yang ada di sistem.
- Keamanan transaksi: Menetapkan prosedur pengamanan untuk transaksi finansial atau administratif yang dilakukan melalui sistem TI.
- Pemantauan aktivitas pengguna: Menyusun kebijakan untuk memantau dan mencatat aktivitas pengguna dalam sistem secara berkala untuk mendeteksi potensi penyalahgunaan.

b. Penggunaan Sistem Keamanan Berlapis (Defense in Depth)

Sistem keamanan TI harus dirancang dengan prinsip pertahanan berlapis untuk melindungi sistem dari ancaman fraud. Langkah-langkah yang harus diambil meliputi:

- Firewall dan Intrusion Detection System (IDS): Menggunakan firewall untuk membatasi akses ke jaringan internal dan sistem IDS untuk mendeteksi adanya aktivitas mencurigakan.
- Autentikasi Multi-Faktor: Implementasi autentikasi dua faktor (2FA) untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem penting.
- Enkripsi Data: Semua data sensitif harus dienkripsi baik saat disimpan maupun saat dikirim melalui jaringan untuk mencegah pencurian data.

c. Penetapan Prosedur Pengelolaan Akses Pengguna

Untuk mencegah fraud yang melibatkan penyalahgunaan akses, IAIN Manado harus menetapkan prosedur yang jelas terkait manajemen akses pengguna:

- Pemberian Hak Akses: Hak akses diberikan hanya kepada individu yang membutuhkannya untuk menjalankan tugas mereka dan harus dikaji secara berkala.
- Pengelolaan Password: Pengguna diwajibkan untuk mengganti password secara berkala dan menggunakan kombinasi karakter yang kuat. Penggunaan password yang mudah ditebak harus dihindari.
- Penonaktifan Akses: Akses pengguna yang tidak lagi aktif atau yang telah meninggalkan institusi harus segera dinonaktifkan untuk mencegah penyalahgunaan.

d. Pelatihan dan Kesadaran Keamanan untuk Pengguna

Staf, dosen, dan mahasiswa perlu diberikan pelatihan yang terus-menerus mengenai ancaman fraud dan cara melindungi data mereka. Pelatihan ini mencakup:

- Pengenalan terhadap ancaman fraud: Memahami risiko-risiko seperti phishing, malware, dan social engineering.
- Cara mengidentifikasi dan melaporkan kegiatan mencurigakan: Mengajarkan pengguna untuk mengenali tanda-tanda aktivitas mencurigakan dan melaporkannya dengan cepat.
- Praktik keamanan dasar: Mengedukasi pengguna tentang cara menjaga keamanan perangkat mereka, seperti menghindari penggunaan perangkat pribadi untuk mengakses data sensitif.

e. Pemantauan dan Audit Sistem Secara Berkala

Pemantauan dan audit merupakan langkah penting dalam mendeteksi tindakan fraud secara dini. Prosedur yang harus diterapkan antara lain:

- Audit Log dan Pencatatan Aktivitas: Semua aktivitas dalam sistem harus tercatat dalam log audit yang bisa dianalisis untuk mendeteksi pola yang mencurigakan.
- Pemeriksaan Rutin: Melakukan pemeriksaan berkala terhadap sistem untuk memastikan bahwa kebijakan keamanan diterapkan dengan baik dan tidak ada celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.
- Pemantauan Trafik Jaringan: Menggunakan sistem pemantauan jaringan untuk mendeteksi adanya trafik yang tidak biasa yang dapat menandakan adanya percakapan atau akses ilegal ke sistem.

a. Implementasi Kebijakan Manajemen Risiko

Institusi harus mengidentifikasi dan menilai risiko yang dapat menyebabkan fraud dan menetapkan kebijakan untuk mengelolanya:

- Penilaian Risiko: Melakukan penilaian risiko secara berkala untuk mengetahui potensi kerentanannya.
- Kontrol Preventif dan Deteksi: Menerapkan kontrol yang dirancang untuk mencegah dan mendeteksi risiko fraud sebelum terjadi.
- Perbaikan dan Penguatan Sistem: Berdasarkan hasil penilaian risiko, sistem dan kebijakan perlu diperbaiki untuk menutup celah yang dapat dimanfaatkan untuk fraud.

f. Kolaborasi dengan Pihak Eksternal

Bekerjasama dengan pihak ketiga seperti konsultan IT atau auditor eksternal untuk melakukan evaluasi objektif terhadap kebijakan dan prosedur fraud management. Mereka dapat memberikan perspektif tambahan tentang kelemahan yang mungkin tidak terlihat oleh tim internal dan memberikan rekomendasi untuk memperbaiki kebijakan keamanan.

g. Penerapan Teknologi Anti-Fraud

Menerapkan teknologi yang dapat membantu mendeteksi dan mencegah fraud secara otomatis, Software Anti-Malware yang Memastikan bahwa perangkat yang digunakan

untuk mengakses sistem terlindungi dari program berbahaya yang dapat digunakan untuk mencuri data atau mengakses informasi secara ilegal.

Dengan menerapkan prosedur-prosedur ini, IAIN Manado dapat meningkatkan sistem pengelolaan fraud secara efektif, sehingga meminimalkan potensi ancaman yang dapat merugikan integritas dan keamanan data serta sistem informasi yang ada.

5. Prosedur Deteksi

Prosedur deteksi fraud bertujuan untuk mengidentifikasi tindak penipuan atau penyalahgunaan dalam sistem TI secara cepat dan efektif. Berikut adalah langkah-langkah esensial dalam prosedur deteksi:

a. Pemantauan Real-Time

Pemantauan aktivitas sistem secara real-time menggunakan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) untuk mendeteksi akses yang tidak sah atau aktivitas mencurigakan di jaringan dan aplikasi.

b. Pencatatan dan Analisis Log

Semua aktivitas dalam sistem dicatat dalam log audit yang dapat dianalisis secara rutin untuk mendeteksi anomali. Analisis pola (pattern analysis) digunakan untuk mengidentifikasi perilaku yang tidak biasa, seperti akses di luar jam kerja atau perubahan data tanpa izin.

c. Penggunaan Teknologi Deteksi Anomali

Menggunakan perangkat lunak berbasis machine learning atau anomaly detection untuk mendeteksi perilaku yang tidak sesuai dengan pola normal pengguna atau transaksi yang mencurigakan.

d. Pengawasan Akses Data Sensitif

Melakukan pengawasan terhadap perubahan atau akses ke data sensitif. Setiap perubahan pada data penting harus tercatat, dan sistem harus memberikan peringatan jika ada akses yang tidak sah.

e. Penilaian dan Pemindaian Kerentanannya

Melakukan vulnerability scanning untuk mendeteksi kerentanannya yang dapat dimanfaatkan untuk fraud. Selain itu, melakukan penetration testing secara rutin untuk mengidentifikasi potensi celah keamanan.

f. **Kolaborasi Tim Keamanan dan Audit**

Tim IT dan audit internal harus bekerja sama dalam mendeteksi dan mengevaluasi insiden fraud, dengan laporan yang cepat dan tepat waktu untuk direspons dengan langkah mitigasi.

Dengan menerapkan prosedur-prosedur ini, IAIN Manado dapat secara proaktif mendeteksi fraud dan mengambil langkah-langkah preventif yang tepat.

6. Prosedur Penanganan

Penanganan fraud yang efektif sangat penting untuk meminimalkan dampak dan mencegah kerugian lebih lanjut. Berikut adalah langkah-langkah esensial dalam prosedur penanganan fraud di IAIN Manado:

a. Identifikasi dan Verifikasi Insiden Fraud

Langkah pertama adalah mengidentifikasi dan memverifikasi insiden yang dicurigai sebagai fraud. Tim IT dan audit internal harus segera melakukan pemeriksaan awal untuk memastikan bahwa kejadian tersebut merupakan tindakan fraud, bukan kesalahan sistem atau operasional.

b. Isolasi dan Penghentian Akses

Setelah fraud teridentifikasi, langkah selanjutnya adalah mengisolasi dan menghentikan akses pengguna yang terlibat dalam aktivitas fraud.

c. Menonaktifkan akun atau kredensial yang digunakan oleh pelaku.

Memutuskan akses ke sistem atau data yang terpengaruh untuk mencegah penyalahgunaan lebih lanjut.

d. Pengumpulan Bukti

Untuk proses investigasi lebih lanjut, penting untuk mengumpulkan bukti yang terkait dengan insiden fraud.

e. Mencatat log aktivitas yang relevan.

Mengumpulkan data dan dokumentasi yang mendukung dugaan fraud. Memastikan bahwa bukti dikumpulkan dengan cara yang sah dan tidak merusak integritas data.

f. Investigasi Internal

Tim audit internal bekerja sama dengan tim IT untuk melakukan investigasi menyeluruh terhadap insiden fraud.

g. Penelusuran lebih lanjut terhadap pola aktivitas yang mencurigakan.

Wawancara dengan individu yang terlibat atau yang mungkin memiliki informasi terkait insiden. Analisis data dan sistem untuk mengidentifikasi celah yang dimanfaatkan oleh pelaku.

h. Pelaporan kepada Pihak Berwenang

Jika investigasi menunjukkan adanya tindak fraud yang melibatkan pelanggaran hukum, langkah selanjutnya adalah melaporkan insiden kepada pihak berwenang, seperti aparat penegak hukum atau regulator yang berwenang.

i. Evaluasi dan Tindakan Perbaikan

Setelah penanganan insiden fraud, evaluasi menyeluruh dilakukan untuk mengidentifikasi penyebab dan celah yang digunakan oleh pelaku.

j. Perbaikan Sistem

Memperbaiki kelemahan dalam sistem atau kebijakan yang memungkinkan terjadinya fraud. Menyusun kembali prosedur dan kontrol keamanan untuk mencegah terulangnya kejadian serupa di masa depan.

k. Komunikasi dengan Pihak Terkait

Komunikasi yang jelas dan transparan perlu dilakukan kepada pihak-pihak terkait, termasuk pihak internal (staff, dosen, dan mahasiswa) serta pemangku kepentingan lainnya. Hal ini penting untuk menjaga kepercayaan dan memberikan informasi terkait langkah-langkah mitigasi yang telah diambil.

l. Penerapan Sanksi dan Tindakan Disipliner

Setelah investigasi selesai, jika terbukti ada pihak yang terlibat dalam fraud, tindakan disipliner atau sanksi yang sesuai harus diberikan. Ini bisa mencakup pemecatan, pencabutan hak akses, atau langkah-langkah hukum sesuai dengan kebijakan internal IAIN Manado dan hukum yang berlaku.

m. Evaluasi dan Perbaikan Prosedur Keamanan

Setelah insiden fraud diatasi, IAIN Manado harus mengevaluasi dan memperbaiki prosedur keamanan TI yang ada. Hal ini termasuk memperbarui kebijakan akses, pengawasan, dan pelatihan staf agar sistem TI menjadi lebih tahan terhadap ancaman fraud di masa depan.

Dengan mengikuti prosedur penanganan yang terstruktur ini, IAIN Manado dapat menangani insiden fraud dengan cepat dan efektif, serta mengurangi risiko terulangnya kejadian serupa di masa yang akan datang.

7. Pemantauan dan Evaluasi

Tahapan Pemantauan dan Evaluasi Fraud Management IT di IAIN Manado adalah sebagai berikut :

- Pemantauan Berkala Pemantauan aktivitas sistem dan pengguna secara real-time untuk mendeteksi aktivitas mencurigakan, seperti penggunaan data sensitif atau akses tidak sah. Log audit dianalisis secara rutin untuk menemukan pola anomali.
- Penilaian Keberhasilan Deteksi Fraud Evaluasi terhadap efektivitas sistem deteksi fraud, apakah insiden dapat terdeteksi tepat waktu dan apakah respons yang diambil sudah sesuai. Ini termasuk analisis keberhasilan perangkat deteksi, seperti IDS/IPS.
- Audit Keamanan Rutin Melakukan evaluasi dan audit keamanan secara berkala untuk menilai apakah kebijakan dan kontrol yang diterapkan sudah memadai dalam mencegah dan mendeteksi fraud.
- Evaluasi Kinerja Tim Penanganan Fraud Menilai respons tim dalam menangani insiden fraud, termasuk kecepatan dan ketepatan dalam memitigasi dampak fraud, serta penyempurnaan prosedur penanganan.
- Pembaruan Kebijakan dan Prosedur Mengkaji dan memperbarui kebijakan serta prosedur manajemen fraud berdasarkan hasil evaluasi, untuk memastikan sistem tetap efektif dalam menghadapi ancaman baru.
- Pelaporan dan Komunikasi Menyusun laporan berkala yang mencakup temuan dan langkah-langkah perbaikan, serta berkomunikasi dengan pemangku kepentingan mengenai kebijakan dan prosedur yang telah diperbarui.

Dengan tahapan ini, IAIN Manado dapat memastikan efektivitas manajemen fraud dan memperbaiki kebijakan serta sistem yang ada untuk mencegah fraud di masa depan.

8. Penegakan Kebijakan

Penegakan kebijakan fraud management di IAIN Manado sangat penting untuk menciptakan sistem yang aman dan transparan, serta mencegah terjadinya penyalahgunaan atau tindakan fraud. Berikut adalah langkah-langkah esensial dalam penegakan kebijakan fraud management di IAIN Manado:

- Sosialisasi Kebijakan Fraud

  Kebijakan fraud management harus disosialisasikan kepada seluruh civitas akademika di IAIN Manado, termasuk dosen, staf administrasi, dan mahasiswa, agar mereka memahami pentingnya kebijakan ini dan peran mereka dalam mencegah fraud.
- Pengawasan dan Kepatuhan

  Tim audit internal dan TI harus melakukan pengawasan terhadap implementasi kebijakan fraud secara rutin. Pengawasan ini mencakup pengecekan terhadap prosedur yang diikuti oleh setiap individu dan pemantauan terhadap pemenuhan standar keamanan yang ditetapkan.

- Sistem Pengendalian Internal

  Implementasi sistem pengendalian internal yang kuat diperlukan untuk memastikan kebijakan fraud dilaksanakan dengan benar. Hal ini termasuk pengawasan akses, prosedur pengelolaan data, serta pembatasan hak akses pengguna yang tidak berwenang.
- Pelatihan dan Pendidikan

  Secara berkala, IAIN Manado harus mengadakan pelatihan untuk meningkatkan pemahaman mengenai kebijakan fraud management, teknik deteksi fraud, serta langkah-langkah yang perlu diambil jika terjadi fraud. Ini juga termasuk pelatihan tentang keamanan siber dan perlindungan data.
- Penerapan Sanksi

Kebijakan fraud harus dilengkapi dengan sistem sanksi yang tegas bagi individu yang terbukti terlibat dalam tindakan fraud. Sanksi ini harus mencakup tindakan disipliner yang jelas, seperti pemecatan, pencabutan hak akses, atau tindakan hukum sesuai dengan ketentuan yang berlaku.

- Evaluasi Berkala

  Untuk memastikan bahwa kebijakan fraud management tetap relevan dan efektif, perlu dilakukan evaluasi berkala terhadap kebijakan dan prosedur yang ada. Evaluasi ini dilakukan untuk menyesuaikan kebijakan dengan perkembangan teknologi, ancaman baru, dan dinamika internal organisasi.

- Komunikasi Terbuka dan Transparansi

  IAIN Manado harus memastikan adanya komunikasi terbuka terkait kebijakan fraud, sehingga semua pihak memahami pentingnya kebijakan ini dalam melindungi integritas institusi. Selain itu, setiap insiden fraud yang terjadi harus ditangani secara transparan dan dilaporkan kepada pihak terkait.

Dengan langkah-langkah penegakan kebijakan ini, IAIN Manado dapat memperkuat pengawasan, meningkatkan kesadaran, dan memastikan kebijakan fraud management berjalan efektif di seluruh unit, termasuk UPT TIPD.

BAB III : Penutup

1. Kesimpulan

Fraud management di IAIN Manado, khususnya melalui UPT TIPD, sangat penting untuk menjaga integritas sistem informasi dan melindungi data sensitif yang dikelola. Melalui kebijakan yang jelas, pemantauan yang efektif, dan prosedur penanganan yang tepat, IAIN Manado dapat mencegah, mendeteksi, dan menangani insiden fraud dengan cepat. Deteksi dini dan pengawasan aktif terhadap akses sistem serta penggunaan teknologi yang tepat menjadi kunci utama dalam mencegah tindakan fraud.

Pencegahan fraud dilakukan dengan menerapkan kontrol akses yang ketat, kebijakan penggunaan sistem yang jelas, serta pelatihan keamanan kepada seluruh civitas akademika. Selain itu, prosedur pengaduan fraud yang transparan dan mudah diakses, seperti melalui formulir pengaduan online atau langsung ke UPT TIPD, memberikan kesempatan bagi individu untuk melaporkan dugaan fraud dengan aman dan terjamin kerahasiaannya. Langkah-langkah ini membantu menciptakan lingkungan yang lebih aman dan responsif terhadap ancaman fraud.

Penegakan kebijakan fraud management yang disiplin dan evaluasi berkala terhadap kebijakan dan prosedur yang ada akan memastikan bahwa tindakan fraud dapat diidentifikasi dan ditanggulangi dengan cepat. Melalui kolaborasi antara tim TI, audit internal, dan pihak terkait lainnya, IAIN Manado dapat mengelola risiko fraud dengan lebih efektif. Dengan demikian, pengelolaan fraud yang baik tidak hanya melindungi aset digital tetapi juga meningkatkan kepercayaan civitas akademika terhadap sistem yang ada.

Lampiran

- **Formulir Pelaporan Insiden Fraud IT**

  Pelaporan Fraud secara daring dapat diakses melalui Website IAIN Manado, UPT TIPD dan link tautan langsung yaitu : *https://s.id/laporInsidenFraudIT*

- **Protokol Respon Insiden**