BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Selama melaksanakan kegiatan magang di PT Siloam International Hospitals Tbk pada *Divisi Cyber Security*, yang berada di bawah naungan Direktorat Teknologi Informasi (*Information Technology Directorate*). Sebagai *Intern pada bagian Identity and Access Management (IAM)*, yang memiliki peran strategis dalam memastikan keamanan dan pengelolaan hak akses pengguna terhadap sistem dan aplikasi internal perusahaan.

Sebagai bagian dari tim IAM, yang langsung dibimbing dan diawasi oleh Davis Olva Bertana, yang menjabat sebagai *Identity and Access Management Lead*. Dalam struktur organisasi, posisi ini memiliki tanggung jawab untuk memimpin, merancang, dan mengimplementasikan kebijakan manajemen identitas dan akses pengguna, guna memastikan bahwa setiap user hanya memiliki akses sesuai dengan kebutuhan dan tanggung jawabnya di lingkungan kerja.

3.2 Tugas yang Dilakukan

Sebagai *Identity and Access Management (IAM) Intern* di Divisi *Cyber Security* PT Siloam International Hospitals Tbk, tugas utama adalah mendukung pengelolaan akses pengguna terhadap berbagai aplikasi internal yang digunakan oleh karyawan di lingkungan *Head Office* maupun unit rumah sakit. Berikut uraian singkat tugas yang dilakukan:

1. Menyelesaikan permintaan akses dan perubahan user yang dialihkan dari tim Help Desk kepada tim *Identity and Access Management (IAM)*. Meliputi *Create User EMR, Create User Mysiloam, Modify Role Mapping Mysiloam/EMR, Create user Kairos, Create user HOPE, Modify User HOPE, Map/Unmap role HOPE*.
2. Melakukan pengelompokan perangkat dari Hospital Unit ke dalam grup di *Microsoft Intune* untuk memudahkan pengelolaan dan penerapan kebijakan keamanan.
3. Melakukan migrasi perangkat perusahaan ke *Microsoft Entra* sebagai bagian dari upaya integrasi sistem manajemen identitas dan akses secara terpusat.

3.3 Uraian Pelaksanaan Magang

Berikut adalah penjelasan mengenai pelaksanaan kegiatan magang yang dilakukan di PT. Siloam International Hospitals Tbk

Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

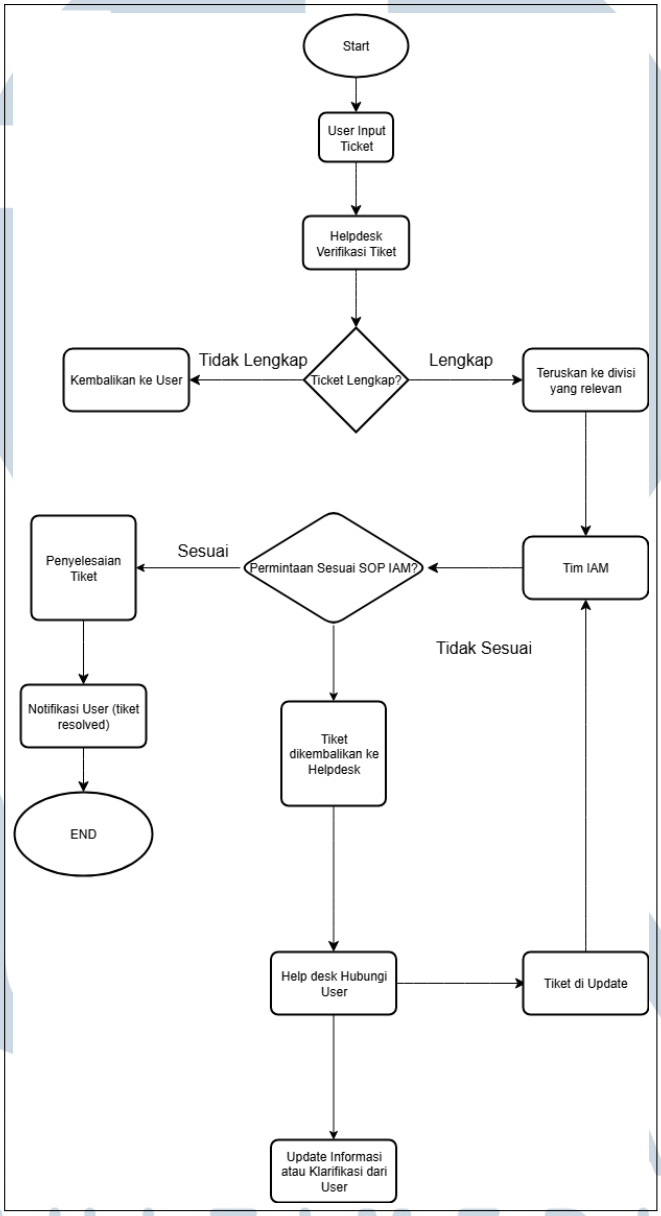
Minggu Ke -	Pekerjaan yang dilakukan
1 - 2	Memulai dengan memahami alur kerja dan fungsi dari sistem tiketing internal perusahaan sebagai sarana pengelolaan permintaan akses aplikasi. Setelah memahami proses dasar tersebut, saya mulai menangani dan mencoba menyelesaikan tiket permintaan akses yang masuk, khususnya untuk aplikasi *EMR (Electronic Medical Record)* dan MySiloam. Aktivitas ini membantu saya dalam mengenali alur proses provisioning pengguna serta meningkatkan keterampilan teknis dalam menangani kebutuhan akses sesuai prosedur yang berlaku di tim *Identity and Access Management (IAM)*.
3 - 4	Menyelesaikan tiket permintaan pembuatan akun (*create user*) untuk aplikasi EMR dan MySiloam yang diajukan melalui sistem tiketing internal. Selain itu, saya juga menangani proses pemetaan dan penghapusan *role (map/unmap)* pada kedua aplikasi tersebut sesuai dengan kebutuhan pengguna. Di samping itu, saya juga menyelesaikan tugas pengelompokan perangkat (*grouping*) dari unit-unit rumah sakit ke dalam *Microsoft Intune*, guna mendukung pengelolaan perangkat secara terpusat serta penerapan kebijakan keamanan yang konsisten di seluruh lingkungan kerja PT Siloam International Hospitals Tbk.
	Lanjut pada halaman selanjutnya

Tabel 3.1 Pekerjaan yang dilakukan tiap minggu selama magang (lanjutan)

Minggu Ke -	Pekerjaan yang dilakukan
5-9	Menyelesaikan berbagai tiket permintaan akses yang berkaitan dengan pembuatan dan pengelolaan akun pengguna untuk beberapa aplikasi internal PT Siloam International Hospitals Tbk. Tugas tersebut meliputi pembuatan akun pengguna (*create user*) pada aplikasi EMR, MySiloam, Kairos, dan HOPE. Selain itu, tim juga menangani permintaan untuk melakukan modifikasi mapping role pada aplikasi MySiloam dan EMR, serta melakukan perubahan data pengguna (*modify user*) dan proses pemetaan maupun penghapusan role (*map/unmap role*) pada aplikasi HOPE, EMR, dan Kairos. Seluruh tugas ini dilaksanakan sesuai dengan prosedur yang berlaku di tim *Identity and Access Management (IAM)*, guna memastikan setiap pengguna memiliki akses yang tepat sesuai dengan tanggung jawabnya.
10 - 22	Menyelesaikan berbagai tiket permintaan akses yang berkaitan dengan pembuatan dan pengelolaan akun pengguna untuk beberapa aplikasi internal PT Siloam International Hospitals Tbk. Tugas tersebut meliputi pembuatan akun pengguna (*create user*) pada aplikasi EMR, MySiloam, Kairos, dan HOPE. Selain itu, tim juga menangani permintaan untuk melakukan modifikasi mapping role pada aplikasi MySiloam dan EMR, serta melakukan perubahan data pengguna (*modify user*) dan proses pemetaan maupun penghapusan role (*map/unmap role*) pada aplikasi HOPE, EMR, dan Kairos. Seluruh tugas ini dilaksanakan sesuai dengan prosedur yang berlaku di tim *Identity and Access Management (IAM)*, guna memastikan setiap pengguna memiliki akses yang tepat sesuai dengan tanggung jawabnya. Di samping itu, saya juga berperan dalam proses migrasi perangkat perusahaan dari *Active Directory (AD)* ke *Microsoft Entra*. Migrasi ini dilakukan sebagai bagian dari inisiatif modernisasi manajemen identitas dan perangkat, guna mendukung pengelolaan akses yang lebih terpusat, aman, dan efisien di seluruh lingkungan kerja PT Siloam International Hospitals Tbk.

3.3.1 Penjelasan Pekerjaan Yang Dikerjakan

A Tiket Permintaan Akses



Gambar 3.1. Flowchart Sistem Tiketing Helpdesk - IAM

Alur kerja sistem tiketing dimulai ketika seorang pengguna atau karyawan mengalami masalah atau memiliki permintaan terkait akses sistem, seperti pembuatan akun, perubahan hak akses, atau keperluan lainnya. Permasalahan ini kemudian diinput ke dalam sistem ticketing oleh pengguna melalui *platform Siloam*

Helpdesk dengan memilih kategori tiket yang sesuai. Setelah tiket terkirim, tim *Helpdesk* akan menerima dan memverifikasi informasi yang tercantum dalam tiket tersebut. Jika informasi masih belum lengkap atau tidak sesuai dengan prosedur, tiket akan dikembalikan kepada pengguna untuk dilengkapi kembali. Namun, apabila tiket sudah lengkap dan sesuai, maka *Helpdesk* akan meneruskannya ke divisi yang relevan.

Dalam hal ini, jika isi tiket berkaitan dengan pengelolaan identitas dan akses pengguna, tiket akan diarahkan ke tim *Identity and Access Management (IAM)*. Tim IAM kemudian akan memproses tiket sesuai dengan SOP yang berlaku, seperti membuat akun baru, melakukan pemetaan atau penghapusan peran (*role mapping*), memodifikasi data pengguna, serta memverifikasi permintaan hak akses. Setelah tiket diselesaikan sesuai prosedur, statusnya akan diubah menjadi "*Resolved*", dan pengguna akan mendapatkan notifikasi bahwa permintaan telah dipenuhi.

Namun, apabila permintaan tidak sesuai dengan protokol atau kebijakan IAM—misalnya terdapat kekurangan data atau permintaan bertentangan dengan ketentuan yang berlaku—maka tiket akan dikembalikan ke *Helpdesk* dengan disertai keterangan. Selanjutnya, pihak *Helpdesk* akan menghubungi pengguna untuk memberikan klarifikasi atau meminta informasi tambahan. Setelah informasi tersebut diperoleh dan diperbarui, tiket dapat dikirim ulang ke tim IAM untuk diproses kembali. Proses ini bertujuan untuk memastikan permintaan yang masuk ditangani secara tepat, efisien, dan sesuai dengan standar keamanan informasi perusahaan.

A.1 Aplikasi yang digunakan

A.1.1 *Siloam Helpdesk*

Helpdesk Siloam adalah sistem ticketing yang digunakan oleh seluruh karyawan Siloam untuk melaporkan kendala teknis maupun mengajukan permintaan akses terhadap aplikasi tertentu. Bagi tim IAM, Helpdesk menjadi pintu masuk utama dalam menerima permintaan seperti pembuatan akun, perubahan role, atau *unmapping akses*. Proses ini dimulai dari pengguna yang mengisi tiket dengan deskripsi kebutuhan mereka, lalu diverifikasi oleh tim *Helpdesk*. Jika permintaan tersebut berkaitan dengan manajemen identitas atau akses, tiket akan diteruskan ke tim IAM. Melalui sistem ini, seluruh aktivitas IAM terdokumentasi dengan baik dan dapat dilacak untuk kebutuhan audit maupun evaluasi SLA (*Service Level*

Agreement). Selain itu, jika ada tiket yang tidak sesuai dengan ketentuan, tim IAM dapat mengembalikan tiket kepada Helpdesk untuk dikonfirmasi ulang ke pengguna.

A.1.2 HOPE

HOPE adalah sistem internal yang digunakan oleh divisi *Human Resources (HR)* di Siloam Hospitals untuk menyimpan dan mengelola data kepegawaian. Informasi yang tersedia di HOPE mencakup status karyawan (*active/resign*), jabatan, unit kerja, hingga data kontrak dan cuti. Aplikasi ini memiliki peran penting dalam proses kerja IAM karena menjadi referensi utama untuk validasi identitas pengguna sebelum akun dibuat atau hak akses diberikan. Misalnya, sebelum tim IAM melakukan *create user atau role mapping* di aplikasi EMR atau Kairos, informasi di HOPE akan digunakan untuk memastikan bahwa karyawan bersangkutan memang memiliki jabatan dan unit kerja yang sesuai. Selain itu, jika terdapat perubahan status kepegawaian seperti *resign* atau mutasi, data tersebut akan digunakan IAM untuk melakukan *unmapping role* atau menonaktifkan akun pengguna agar sesuai dengan kebijakan keamanan informasi perusahaan.

A.1.3 *Siloam User Management System*

UMS merupakan sistem utama yang digunakan oleh tim IAM untuk mengelola identitas digital seluruh karyawan dan vendor di lingkungan Siloam Hospitals. Sistem ini berfungsi sebagai pusat data pengguna (*user repository*) yang menyimpan informasi penting seperti nama, NIK, jabatan, unit kerja, serta status kepegawaian. Dalam praktiknya, UMS digunakan untuk melakukan provisioning (pembuatan akun), modifikasi, hingga *deprovisioning* (penonaktifan akun) di berbagai sistem dan aplikasi internal Siloam, seperti EMR, MySiloam, Kairos, dan HOPE. Dengan UMS, proses manajemen akun menjadi lebih terpusat, efisien, dan terdokumentasi. Selain itu, UMS juga membantu memastikan bahwa hak akses yang diberikan kepada pengguna sesuai dengan jabatan dan unit kerja mereka, sehingga IAM dapat menerapkan prinsip *Role-Based Access Control (RBAC)* secara konsisten dan akurat.

B *Grouping Intune*

Grouping Intune Device merupakan proses pengelompokan perangkat seperti laptop, desktop, dan tablet milik karyawan ke dalam grup-grup tertentu melalui platform *Microsoft Intune*, berdasarkan kriteria seperti unit kerja, lokasi rumah sakit, jabatan, atau fungsi operasional perangkat. Proses ini sangat penting dalam mendukung kebijakan manajemen perangkat dan keamanan sistem di lingkungan rumah sakit. *Microsoft Intune* sendiri merupakan layanan berbasis cloud yang menyediakan fitur *Mobile Device Management* (MDM) dan *Mobile Application Management* (MAM), sehingga memungkinkan administrator mengelola perangkat secara terpusat [4]. Bagi tim IAM, grouping ini mempermudah proses pemetaan akses pengguna, karena perangkat yang sudah tergolong dalam grup tertentu dapat diberikan hak akses sesuai perannya secara lebih cepat dan terkontrol [5]. Misalnya, perangkat milik tenaga medis yang tergabung dalam grup "Medis" akan otomatis mendapatkan akses ke sistem EMR (*Electronic Medical Record*), sedangkan perangkat tim keuangan bisa diatur dengan kebijakan akses yang berbeda, sesuai kebutuhan dan sensitivitas data. Selain itu, *grouping* perangkat melalui *Intune* juga memberikan keuntungan dalam hal *monitoring* dan manajemen keamanan. Tim IT dapat secara langsung melacak status perangkat, menerapkan pembaruan sistem, atau mendistribusikan aplikasi secara terpusat ke grup tertentu tanpa harus melakukan konfigurasi satu per satu. Dalam konteks IAM, hal ini mendukung prinsip *Zero Trust Security* karena memungkinkan tim memastikan bahwa hanya perangkat yang sah, terdaftar, dan tergrouping sesuai protokol yang dapat mengakses aplikasi perusahaan [6]. Dengan begitu, pengelolaan akses menjadi lebih presisi, cepat, dan sesuai dengan kebijakan keamanan informasi yang berlaku di Siloam Hospitals. Secara keseluruhan, *grouping Intune device* berperan penting dalam memperkuat kolaborasi antara tim IAM dan tim IT operasional dalam menjaga keamanan, efisiensi kerja, dan kepatuhan terhadap standar industri kesehatan seperti *ISO/IEC 27001* [7] serta mendukung praktik manajemen identitas berbasis peran dan akses yang diatur melalui *Microsoft Entra Identity Governance* [8].

Dalam proses *grouping Intune device* di lingkungan PT Siloam International Hospitals Tbk, tim IAM bertanggung jawab untuk mengelompokkan perangkat berdasarkan unit rumah sakit masing-masing. Proses ini dilakukan dengan penuh kehati-hatian karena pemindahan perangkat ke grup tertentu pada *Microsoft Intune* berpotensi menyebabkan perangkat tersebut ter-logout secara otomatis atau

mengalami gangguan sistem sementara. Oleh karena itu, sebelum melakukan eksekusi tugas, tim IAM harus melakukan koordinasi terlebih dahulu dengan tim IT di masing-masing *Hospital Unit*. Koordinasi ini bertujuan untuk menentukan waktu yang tepat dan relatif luang agar proses grouping tidak mengganggu operasional penting rumah sakit. Dengan pendekatan kolaboratif ini, proses grouping dapat dilakukan secara efisien dan minim risiko terhadap layanan dan aktivitas di unit rumah sakit.

C Migrasi *Company Device AD ke Microsoft Entra*

Migrasi device dari *Active Directory (AD)* ke *Full Entra* merujuk pada proses pemindahan perangkat-perangkat milik perusahaan, seperti laptop dan komputer kerja, dari sistem manajemen tradisional berbasis *on-premise (Active Directory Domain Services)* ke sistem modern berbasis *cloud*, yaitu *Microsoft Entra* (dulu dikenal sebagai *Azure Active Directory*).

Pada *Active Directory* konvensional, perangkat dikendalikan melalui server lokal (*domain controller*), yang memerlukan konektivitas ke jaringan internal perusahaan. Sementara itu, *Microsoft Entra* menyediakan manajemen identitas dan akses yang lebih fleksibel melalui *cloud*, memungkinkan pengelolaan perangkat secara jarak jauh, integrasi dengan *Microsoft Intune* (untuk manajemen endpoint), serta akses yang lebih aman menggunakan kebijakan *Conditional Access*, *MFA (Multi-Factor Authentication)*, dan *Zero Trust Architecture*.

C.1 Manfaat dari migrasi

Migrasi perangkat dari *Active Directory (AD)* ke *Microsoft Entra* memberikan sejumlah manfaat penting bagi PT Siloam International Hospitals Tbk dalam mendukung transformasi digital dan keamanan sistem informasi. Salah satu manfaat utamanya adalah peningkatan fleksibilitas akses. Dengan sistem berbasis *cloud*, perangkat yang telah terhubung ke *Microsoft Entra* memungkinkan karyawan untuk mengakses aplikasi dan sistem perusahaan dari luar jaringan kantor secara aman, yang sangat relevan dalam mendukung model kerja *hybrid atau remote*. Selain itu, proses migrasi ini juga memungkinkan perusahaan untuk menerapkan manajemen perangkat yang terpusat melalui integrasi dengan *Microsoft Intune*, sehingga pengaturan kebijakan keamanan, update perangkat, dan pelacakan inventaris dapat dilakukan dengan lebih efisien dan real-time.

Dari sisi keamanan, migrasi ke Entra memungkinkan implementasi fitur keamanan modern, seperti *Single Sign-On (SSO), Multi-Factor Authentication (MFA), dan Conditional Access*, yang secara signifikan dapat mengurangi risiko akses tidak sah dan kebocoran data.[9] Hal ini juga mendukung prinsip *Zero Trust Security*, di mana setiap akses pengguna dan perangkat akan divalidasi berdasarkan identitas dan konteksnya.[10] Bagi tim *Identity and Access Management (IAM)*, sistem ini memberikan kemudahan dalam melakukan *provisioning dan deprovisioning* akun, serta pengaturan hak akses yang lebih cepat, akurat, dan sesuai kebijakan perusahaan. Dengan demikian, migrasi ini tidak hanya memperkuat postur keamanan siber perusahaan, tetapi juga meningkatkan efisiensi dan kepatuhan operasional terhadap standar keamanan informasi yang berlaku.

3.4 Kendala dan Solusi yang Ditemukan

A Kendala

Selama pelaksanaan magang di Divisi *Cyber Security* bagian *Identity and Access Management (IAM)*, tim menghadapi beberapa kendala yang cukup signifikan. Pada awal masa magang, terdapat kesulitan dalam memahami alur sistem tiket serta perbedaan teknis dari masing-masing aplikasi internal seperti EMR, MySiloam, Kairos, dan HOPE. Selain itu, terbatasnya akses pada sistem IAM di awal magang juga menghambat untuk menyelesaikan tiket secara mandiri. Tantangan lain muncul dalam proses migrasi perangkat dari *Active Directory* ke *Microsoft Entra*, di mana beberapa perangkat mengalami kegagalan migrasi akibat ketidaksesuaian konfigurasi teknis. Tak hanya itu, keterlambatan komunikasi lintas divisi, khususnya antara *Help Desk* dan tim IAM, juga menjadi kendala dalam mempercepat penyelesaian tiket dan validasi data.

B Solusi

Untuk mengatasi kendala tersebut, tim secara aktif melakukan observasi dan mencatat alur kerja dari setiap aplikasi yang digunakan, serta berkonsultasi langsung dengan *Lead* IAM, Dvis Olva Bertana, guna memperdalam pemahaman sistem. Setelah melalui proses pengajuan, akses terhadap sistem diberikan secara penuh sehingga dapat mulai menangani tiket secara langsung. Prosedur migrasi *Entra* turut dipelajari dan *Microsoft Endpoint Manager* digunakan untuk melakukan pemantauan serta grouping ulang perangkat yang bermasalah. Dalam

menghadapi kendala komunikasi, dilakukan komunikasi proaktif melalui *follow-up* menggunakan *Microsoft Teams dan email*, serta pencatatan kronologi tiket secara terstruktur agar proses koordinasi antar tim berjalan lebih efektif.