In Stage 2, the focus shifts to implementing a secure identity and access management framework for VIP Events by setting up Azure Active Directory (Azure AD). This foundational step ensures seamless integration with the organization's infrastructure while supporting scalability and robust cybersecurity. The output of this stage includes detailed specifications for VIP Events’ Azure AD tenant, user accounts, and group-based access control.

Note: As I no longer have access to free trial version of Azure/Microsoft Entra it will not be possible for me to attach screenshots for the below given tasks. The general structure of them have been defined, along with its utility.

**Task 1: Azure AD Tenant**

VIP Events requires its own Azure AD tenant to establish a centralized identity management system that aligns with its operational needs and future growth potential.

1. Tenant Configuration:

- Domain Name: Use a custom domain name (e.g., `vipevents.onmicrosoft.com`) to reflect the organization’s branding.

- Scalability: Ensure the tenant supports additional users, groups, and applications as the workforce grows.

- Integration: Align the tenant with existing systems such as email, file storage, and other cloud services.

- Security Features:

- Enable Conditional Access Policies to enforce security based on user location, device compliance, and risk levels.

- Activate Identity Protection to detect and respond to suspicious activities.

1. Compliance:

- Ensure the tenant adheres to industry standards (e.g., GDPR, ISO 27001) for data protection and privacy.

**Task 2: User Account Configuration**

To accommodate VIP Events’ expanded workforce, meticulously design an identity and access solution by specifying user accounts and their attributes.

User Account Attributes:

-1. Basic Information: Include attributes such as first name, last name, job title, department, and contact details.

- Password Policies:

* Enforce strong password requirements (minimum length, complexity, expiration).
* Enable self-service password reset (SSPR) for employees to recover access securely.

- Multi-Factor Authentication (MFA):

* Require MFA for all users, especially privileged accounts (e.g., CEO, Equipment Manager).
* Use methods like Microsoft Authenticator app, SMS, or hardware tokens.

2. User Roles and Accounts:

Based on the roles defined in Task 5 of Stage 1, create user accounts for the following groups:

- Equipment Handlers: Limited access to equipment management functionalities.

- Chefs and Head Chef: Access to kitchen management tools.

- Office Workers: Administrative and data management access.

- Transient Staff: Temporary accounts with limited permissions and automatic expiration.

- CEO: Unrestricted access with enhanced security measures.

3. Account Lifecycle Management:

- Automate account provisioning and de-provisioning using Azure AD workflows.

- Implement time-limited access for transient staff, ensuring accounts expire after their predefined period.

**Task 3: Group-Based Access Control Implementation**

A comprehensive group-based access control strategy is essential to ensure secure and organized access management.

1. Group Structure:

- Create security groups for each functional area:

* Dock\_Operations: Restricted to equipment handlers and managers.
* Kitchen: Limited to chefs, head chefs, and catering managers.
* Office: Accessible to office workers and management.
* Guest: Open access with restricted privileges.
* Management: Exclusive access for the CEO and senior management.

- Use dynamic groups for transient staff, where membership is automatically updated based on predefined rules (e.g., job role or employment duration).

1. Role Assignments:

- Assign Azure AD roles to groups based on their responsibilities:

* EquipHandlersRole: Equipment handlers with access to dock operations and equipment storage.
* ChefsRole: Chefs with access to kitchen-related systems.
* OfficeRole: Office workers with administrative access.
* ManagementRole: CEO and senior management with elevated privileges.

3. Access Control Measures:

- Implement role-based access control (RBAC) to streamline permissions.

- Use conditional access policies to restrict access based on location, device compliance, and risk levels.

**Documentation Summary**

The Azure AD configuration documentation serves as a critical reference for future management, audits, and optimization efforts. Key details include:

- Tenant Structure: Domain name, scalability features, and integration capabilities.

- User Accounts: List of user roles, attributes, and configurations (e.g., MFA, password policies).

- Group-Based Access Control: Security groups, dynamic groups, and role assignments.

- Policies: Conditional access policies, identity protection, and lifecycle management workflows.

This documentation ensures VIP Events has a comprehensive and accessible resource for ongoing management and optimization.