Потрібно заздалегіть визначити особу яка буде відповідати за фізичну безпеку пристроїв та серверів при переїзді. Потрібно встановити постійний візуальний нагляд за всіма компонентами.

Встановлення мережі.

Мережа буде складатися з трьох підмереж базуючись на поверхах будівлі, так як організація роботи фірми узгоджена за поверхами, для зручності керування та сегментації для підсилення безпеки. У разі необхідності можуть бути створені додаткові підмережі для ще більшої сегментації для захисту секретних даних.

* **Пристрої** підключаються до **комутатора** на кожному поверсі для локального обміну файлами та ресурсами.
* **Комутатор** підключається до **маршрутизатора** на кожному поверсі для забезпечення доступу до Інтернету.
* **Маршрутизатори** на різних поверхах об'єднуються між собою за допомогою кабелів для забезпечення стабільного з'єднання між підмережами.
* Один **маршрутизатор** на першому поверсі підключається до лінії постачальника Інтернету для забезпечення доступу до глобальної мережі.
* **Пристрій з віртуальною машиною**: Підключений основний маршрутизатор до пристрою (сервер або комп'ютер), на якому буде запущена віртуальна машина з програмним брандмауером.
* **Мережевий комутатор**: Підключіть пристрій з віртуальною машиною до мережевого комутатора. Це дозволить підключити кілька підмереж до одного пристрою.

Також буде створений окремий доступ бездротової мережі для тимчасових працівників. Мережа буде окремою та ізольованою з назвою vip300, vip310, vip320 на кожному поверсі.

Підмережі будуть названі за принципом поверхів:

Vip50, vip60, vip70.

Також будуть окремі мережі з бездротовим доступом:

Vip150, vip160, vip170.

Кожен поверх відповідає своєму завданню , тому і призначення мережі буде відповідно до потреб поверху.

На першому поверсі ми маємо підрозділ обладнання. Матимуть доступ такі пристрої і відповідні посади до них:

4 оператори обладнання та планшети для роботи - будуть підключені до бездротової мережі vip150. Керівник обладнання та його настільний комп'ютер s gkfyitn - відповідно будуть підключені до мережі vip50 та vip150.

Кухарі та шефкухарі будуть підключені до мережі vip60 та vip160. Три портативні комп'ютери, три планшети та один настільний комп'ютер.

Працівники офісу будуть підключені до мережі vip70, vip170. Сюди входитимуть: 3 настільні комп'ютери; кейтеринг менеджер - 1 настільний комп'ютер, планшет та телефон; генеральний директор - 1 настільний комп'ютер, планшет та телефон.

Політика підключення до мережі : надійні паролі підключення та політики відповідності які забезпечують відповідність певним вимогам, таким як антивірусне програмне забезпечення або оновлення системи, перед тим, як дозволити підключення до мережі.

Ролі працівників:

**Роль обробника обладнання (EquipHandlersRole)**

**Роль менеджера обладнання (EquipManagerRole):**

**Шеф-кухар (ChefsRole)**

**Роль шеф-кухаря (HeadChefRole)**

**Роль менеджера кейтерингу (CateringManagerRole):**

**Роль офісних працівників (OfficeWorkersRole):**

**Роль генерального директора (власника) (CEORole):**

**Тимчасова роль (TempRole):**

Рекомендації з фізичної безпеки: вхід у може бути ппосилений перевіркою біометричних даних або аутентифікація за допомогою ключа доступу у вигляді бейджа. Також встановлення відеокамер та автоматичне замикання дверей на кожному поверсі і дозвіл за наявною ключкартою.

Налаштування AAD.

Створення орендаря. Додавання орендаря з назвою фірми.

Створення користувачів: для кожного працівника буде створений користувач Azure.

Також буде створено групи для обєднання користувачів за їхніми посадовими обовязками. Буде створена група обладнання , група кухарів, група офісних працівників, група адміністраторів та група для тимчасових працівників.

До кожної групи буде створена та реалізована політика доступу та безпеки з мінімальними дозволами які потрібні для виконання їх роботи. Група менеджерів буде мати окремий підвищений захист такий як доступ вчасно, умовний доступ. До всіх користувачів буде запроваджена політика багатофакторної аутентифікації. Також політики будуть визначати складність паролю та його дії на певний проміжок часу.

Налаштування та призначення ролей.

**Роль обробника обладнання (EquipHandlersRole)** надає доступ до основних функцій управління обладнанням у додатку VIP Foods. Вона дозволяє ефективно відстежувати та управляти кулінарними інструментами та ресурсами.

**Роль менеджера обладнання (EquipManagerRole)** ця роль пропонує розширені можливості для контролю та управління повним спектром функцій обладнання. Це забезпечує оптимальне використання та обслуговування кулінарних ресурсів.

**Шеф-кухар (ChefsRole)** ця роль надає доступ до функцій приготування їжі та управління кухнею. Шеф-кухарі можуть використовувати додаток для оптимізації кулінарних процесів та покращення співпраці на кухні.

**Роль шеф-кухаря (HeadChefRole)** ця роль надає підвищений доступ до загальних функцій управління кухнею. Вона надає шеф-кухарю інструменти для ефективної координації та керівництва кулінарними операціями.

**Роль менеджера кейтерингу (CateringManagerRole)** ця роль полегшує планування та управління кейтеринг-подіями. Вона включає функції координації заходів, планування меню та управління логістикою для забезпечення безперебійного надання кейтерингових послуг.

**Роль офісних працівників (OfficeWorkersRole)** ця роль надає доступ до офісних функцій та функцій управління даними в додатку VIP Foods. Це покращує комунікацію та співпрацю між кулінарною та адміністративною командами.

**Роль генерального директора (власника) (CEORole)** ця роль надає необмежений доступ до всіх функцій додатку VIP Foods. Вона дозволяє здійснювати стратегічний нагляд і приймати рішення, а також забезпечує всебічний контроль над платформою.

**Тимчасова роль (TempRole)** ця роль пропонує обмежений доступ до дозволів, необхідних для виконання поточних завдань. Дозволи автоматично вимикаються після закінчення заздалегідь визначеного періоду, забезпечуючи тимчасовий і безпечний доступ, пристосований до нагальних потреб користувача.

Розподіл ролей по групам:

група обладнання: **Роль обробника обладнання (EquipHandlersRole)**

група кухарів: **Шеф-кухар (ChefsRole)**

група офісних працівників: **Роль офісних працівників (OfficeWorkersRole)**

група для тимчасових працівників: **Тимчасова роль (TempRole)**

**Група адміністраторів: Роль генерального директора (власника) (CEORole), Роль менеджера кейтерингу (CateringManagerRole), Роль шеф-кухаря (HeadChefRole), Роль менеджера обладнання (EquipManagerRole).**

**Тестуваня доступу.**

### **Перевірка інтеграції програми з Azure AD:**

1. **Увійдіть** до порталу Azure і перейдіть до розділу Azure Active Directory.
2. **Перейдіть** до App registrations і виберіть вашу програму VIP Foods.
3. **Виберіть** Authentication і переконайтеся, що налаштування автентифікації відповідають вимогам вашої програми (наприклад, налаштовані URI перенаправлення, використання токенів ID тощо).
4. **Перейдіть** до API permissions і переконайтеся, що додані всі необхідні дозволи для вашої програми. Наприклад, переконайтеся, що є дозволи для доступу до Microsoft Graph API або інших ресурсів, необхідних для вашої програми.
5. **Виберіть** Certificates & secrets і переконайтеся, що ваш додаток має дійсний секрет або сертифікат для автентифікації.

### **2. Тестування автентифікації:**

1. **Виконайте тестові входи** для різних облікових записів користувачів і перевірте, що вони успішно автентифікуються через Azure AD.
2. **Перевірте журнали автентифікації** в Azure AD, щоб переконатися, що всі входи успішні і жодних помилок не виникає.

### **Перевірка призначених користувацьких ролей:**

1. **Перевірте, що функції додатку доступні** лише для користувачів з відповідними ролями. Наприклад, користувачі з роллю "читач" повинні мати доступ лише до функцій перегляду, а користувачі з роллю "учасник" - до функцій редагування.

### **4. Використання груп користувачів для ролей:**

1. **Переконайтеся, що групи користувачів у Azure AD** налаштовані відповідно до ролей і обов'язків (як було описано раніше).
2. **Зіставте групи користувачів з ролями** у вашій програмі VIP Foods.
3. **Виконайте тестування доступу** для користувачів різних груп, щоб переконатися, що вони мають відповідні права доступу.

### **1. Перевірка налаштувань MFA на рівні організації:**

1. **Увійдіть** до порталу Azure.
2. **Перейдіть** до Azure Active Directory -> Security -> Multi-Factor Authentication.
3. **Перевірте політику MFA** для вашої організації. Переконайтеся, що MFA увімкнено для всіх користувачів або для певних груп користувачів відповідно до політики безпеки вашої організації.

### **2. Перевірка налаштувань MFA для конкретних користувачів:**

1. **Виберіть** Azure Active Directory -> Users.
2. **Знайдіть користувача**, для якого потрібно перевірити налаштування MFA.
3. **Перейдіть** до Authentication methods.
4. **Перевірте, чи налаштовано MFA** для цього користувача (наприклад, через додаток Microsoft Authenticator, SMS або телефонний дзвінок).

### **3. Тестування MFA для користувачів:**

1. **Створіть тестові облікові записи користувачів** або використовуйте існуючі облікові записи для тестування.
2. **Увійдіть до облікового запису** користувача через веб-браузер або клієнтську програму.
3. **Виконайте сценарії тестування**, щоб переконатися, що користувачам вимагається додатковий метод автентифікації під час входу (наприклад, введення коду з мобільного додатку).

### **4. Перевірка журналів автентифікації:**

1. **Перейдіть** до Azure Active Directory -> Sign-ins.
2. **Перегляньте журнали автентифікації** для перевірки успішних і невдалих спроб входу з використанням MFA.
3. **Аналізуйте журнали** на предмет виявлення будь-яких невідповідностей або помилок в конфігурації MFA.

Ведення журналів і моніторинг в Azure AD

### **Де знайти журнали Azure AD**

1. **Увійдіть** до порталу Azure.
2. **Перейдіть** до розділу Azure Active Directory.
3. **Виберіть** Sign-ins у меню зліва. Тут ви знайдете журнали вхідних подій користувачів.
4. **Виберіть** Audit logs у меню зліва для перегляду аудиторських журналів. Тут реєструються всі дії, такі як призначення ролей, зміни в атрибутах користувачів та інші адміністративні дії.

### **2. Перевірка журналів на успішні та невдалі входи**

1. **Перейдіть** до розділу Sign-ins.
2. **Перегляньте** список записів. Для кожного запису ви побачите статус (успішний або невдалий вхід), користувача, який виконав спробу входу, та інші деталі.
3. **Фільтруйте** записи за статусом, щоб легше знайти потрібну інформацію.
4. **Перевірте причини невдалих спроб входу** (наприклад, неправильний пароль, заблокований обліковий запис) для аналізу і вирішення проблем.

### **3. Перевірка журналів на призначення ролей**

1. **Перейдіть** до розділу Audit logs.
2. **Використовуйте фільтри** для пошуку записів, пов'язаних з призначенням ролей.
   1. **Виберіть** Category -> Role Management.
3. **Перегляньте** деталі кожного запису, щоб переконатися, що ролі були призначені правильно.
   1. Інформація буде включати користувача, якому було призначено роль, дату і час події, а також адміністратора, який виконав дію.

### **4. Перевірка журналів на зміни в атрибутах користувачів**

1. **Перейдіть** до розділу Audit logs.
2. **Використовуйте фільтри** для пошуку записів, пов'язаних зі змінами в атрибутах користувачів.
   1. **Виберіть** Category -> User Management.
3. **Перегляньте** деталі кожного запису, щоб переконатися, що всі зміни були виконані правильно.
   1. Інформація буде включати змінені атрибути, користувача, адміністратора, який виконав зміни, та дату і час події.

Політики безпеки.

### **Налаштування політики автентифікації користувачів в Azure AD**

1. **Увімкніть багатофакторну автентифікацію (MFA) для всіх користувачів**:
   1. Увійдіть до порталу Azure.
   2. Перейдіть до Azure Active Directory -> Security -> Conditional Access.
   3. Натисніть New policy, щоб створити нову політику умовного доступу.
   4. Введіть назву для політики (наприклад, "Політика MFA для всіх користувачів").
   5. У розділі Assignments виберіть Users and groups, а потім виберіть All users для застосування політики до всіх користувачів.
   6. У розділі Cloud apps or actions виберіть Select all apps для застосування політики до всіх додатків.
   7. У розділі Access controls виберіть Grant і встановіть прапорець Require multi-factor authentication.
   8. Натисніть Create, щоб зберегти політику.
2. **Налаштуйте політику автентифікації для адміністраторів**:
   1. Створіть окрему політику умовного доступу для адміністраторів, щоб забезпечити додатковий рівень безпеки для привілейованих облікових записів.
   2. Виберіть Users and groups, а потім виберіть групу адміністраторів.
   3. Застосуйте ті ж налаштування, що і для політики MFA для всіх користувачів, але додайте додаткові умови, такі як обмеження доступу лише з певних IP-адрес або пристроїв.
3. **Використовуйте політики умовного доступу для захисту важливих ресурсів**:
   1. Створіть політику умовного доступу, яка вимагатиме багатофакторну автентифікацію при доступі до критично важливих ресурсів.
   2. Виберіть Cloud apps or actions і виберіть конкретні додатки або ресурси, які потрібно захистити.
   3. У розділі Conditions додайте умови, такі як розташування, тип пристрою або ризик входу.

Для забезпечення мережевої конфігурації для веб-програм в Azure можна налаштувати політику обмеження доступу до певних віртуальних мереж. Ось покрокова інструкція для цього:

### **1. Створення політики мережевої конфігурації в Azure:**

1. **Увійдіть** до порталу Azure.
2. **Перейдіть** до розділу Azure Policy:
   1. Виберіть All services у лівій панелі навігації.
   2. Введіть Policy у полі пошуку та виберіть Policy зі списку.
3. **Створіть нову політику**:
   1. Натисніть Definitions в меню зліва.
   2. Натисніть + Policy definition.
   3. Введіть назву для політики (наприклад, "Обмеження доступу до віртуальних мереж").
   4. Виберіть категорію політики, наприклад, Networking.
4. **Введіть визначення політики**:
   1. Використовуйте JSON для визначення умов та дій політики. Наприклад:

json

{  
 "properties": {  
 "displayName": "Allow resources only in specific virtual networks",  
 "description": "Ensures that resources are only deployed within approved virtual networks.",  
 "policyRule": {  
 "if": {  
 "allOf": [  
 {  
 "field": "type",  
 "equals": "Microsoft.Network/virtualNetworks/subnets"  
 },  
 {  
 "field": "Microsoft.Network/virtualNetworks/subnets/vnetName",  
 "in": [  
 "approved-vnet-1",  
 "approved-vnet-2"  
 ]  
 }  
 ]  
 },  
 "then": {  
 "effect": "deny"  
 }  
 }  
 }  
}

1. **Натисніть** Save для збереження політики.

### **2. Призначення політики мережевої конфігурації:**

1. **Перейдіть** до розділу Assignments у меню Policy.
2. **Натисніть** + Assign policy для призначення створеної політики.
3. **Виберіть область** застосування (наприклад, підписка або ресурсна група).
4. **Знайдіть та виберіть** створену політику зі списку визначень.
5. **Налаштуйте параметри** призначення, такі як назва та опис призначення.
6. **Натисніть** Assign для збереження призначення політики.

### **3. Моніторинг та перевірка політики:**

1. **Перейдіть** до розділу Compliance у меню Policy.
2. **Перевірте статус відповідності** призначеної політики. Тут ви зможете побачити ресурси, які відповідають або не відповідають політиці.
3. **Аналізуйте результати** та вживайте заходів для виправлення будь-яких невідповідностей.

### **Важливість тестування політик у невиробничому середовищі**

**Тестування політик у невиробничому середовищі** є критично важливим кроком перед їх впровадженням у виробниче середовище. Це допомагає забезпечити, що політики працюють належним чином та не порушують роботу важливих ресурсів.

#### **Потенційні ризики, пов'язані з реалізацією політик**

1. **Перерви в роботі**:
   1. Неправильно налаштовані політики можуть призвести до обмеження доступу або недоступності критично важливих ресурсів, що може вплинути на продуктивність і операційну ефективність.
2. **Втрата даних**:
   1. Неправильне налаштування політик мережевої конфігурації може призвести до порушення підключення, що може вплинути на доступ до даних і можливість їхнього збереження.
3. **Безпекові проблеми**:
   1. Неправильні налаштування політики автентифікації можуть створити вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до ресурсів.

#### **Переваги тестування перед впровадженням**

1. **Виявлення та виправлення помилок**:
   1. Тестування політик у невиробничому середовищі дозволяє виявити та виправити будь-які помилки або невідповідності без впливу на виробниче середовище.
2. **Перевірка сумісності**:
   1. Тестування допомагає перевірити, чи політики сумісні з існуючими налаштуваннями та інфраструктурою, запобігаючи потенційним конфліктам.
3. **Оцінка впливу**:
   1. Тестування дозволяє оцінити, як політики впливають на роботу додатків і користувачів, забезпечуючи можливість вносити корективи перед впровадженням.
4. **Документування результатів**:
   1. Результати тестування можна задокументувати для подальшого аналізу та вдосконалення процесів. Це допоможе створити надійну базу знань для майбутніх змін.

### **Кроки тестування політик у невиробничому середовищі**

1. **Створення невиробничого середовища**:
   1. Створіть ізольоване середовище, яке максимально відповідає виробничому.
2. **Впровадження політик**:
   1. Впровадьте політики автентифікації користувачів та мережевої конфігурації у невиробниче середовище.
3. **Виконання тестових сценаріїв**:
   1. Розробіть і виконайте тестові сценарії, які включають всі можливі варіанти використання політик.
4. **Аналіз результатів**:
   1. Перегляньте результати тестування, виявивши будь-які невідповідності або помилки.
5. **Внесення коректив**:
   1. Внесіть необхідні корективи до політик на основі результатів тестування.
6. **Повторне тестування**:
   1. Виконайте повторне тестування після внесення коректив, щоб переконатися, що всі проблеми були вирішені.

### **Документування результатів тестування**

1. **Збережіть результати тестування**:
   1. Занотуйте всі результати тестування, включаючи успішні та невдалі сценарії.
2. **Включіть скріншоти**:
   1. Документуйте кожний крок і результати за допомогою скріншотів.
3. **Підготуйте звіт**:
   1. Підготуйте детальний звіт з результатами тестування для подальшого аналізу та впровадження.