# **DP201 - Designing an Azure Data Platform Solution**

## Lab 4 – Azure Security Design Considerations

**Exercise 1**

**Task 1: Defence in depth approach**

Use the table below to document the security requirements for AdventureWorks. You can use requirements as identified from the AdventureWorks case study. You should also suggest security requirements that are missed but should be considered to ensure that AdventureWorks has proper security coverage.

|  |  |
| --- | --- |
| Requirement | Defence in Depth Category |
| Make sure that our offices and shops have sufficient security and visitors desks etc. | Physical Security |
| Make sure Staff are trained in physical security of their assets such as not connecting to Public Wifi without VPN and watching who is around when doing sensitive tasks / monitor view filters. | Physical Security |
| Make sure that all staff use MFA especially those with privileged access | Identity and Access |
| Make sure that we have strong identity procedures for our API’s especially when providing data to external parties. | Identity and Access |
| As much as possible use Least Privilege principles when granting administration and access rights. | Identity and Access |
| Azure DDoS protection in place | Perimeter |
| As much as possible services and assets should be locked down to known IP’s using NSG’s and Service level firewalls. | Network |
| No open to web access should be enabled for any azure services | Network |
| Where possible Just In Time access to resources should be employed. | Network |
| All data stores should be encrypted at rest and in transit. | Compute |
|  |  |
| Any applications with access to the estate should follow application bets practices | Application |
| Applications should utilise Application Firewalls where possible. | Application |
| Any infrastructure as a service or container based applications should be managed and regularly patched. | Application |
| Applications should undergo Security reviews and penetration testing before go live and then at a regular interval. | Applications |
| Applications themselves should implement strong Identity management as the first line of defence. | Applications |
| Applications should manage their Application Keys very carefully and separately from the application code (Azure key Vault etc) | Applications |
| We should carefully consider all data collected and eliminate any sensitive data we do not need to store. | Data |
| All Data should be classified so appropriate measures can be implemented against them | Data |
| Apprioriate Data Level measures should be implemented such as Data Masking where appropriate. | Data |
| Data should be assessed for its uses for compliance with regulations in all countries the data is stored / used. | Data |
| A zero trust / Least privilege approach should be sued for Data access. | Data |