**BAIT3273 Tutorial 10**

**Azure Security**

• Secure application, compute, network

• Authentication and authorization

• Azure Active Directory, Single sign-on

**Instructions**

• Please use this document to answer all the questions in this tutorial.

• Rename the file with your student code and tutorial group number. For example, 1909846-BAIT3273-S1-2020-Tut1-RDSG01 with RDSG01 as your respective programme and group number. Besides, replace *XXXXXXXX* at the header with your student code.

• Every student must submit this doc individually at the end of the tutorial to google classroom.

**Task 1: Azure Security**

Every system, architecture, and application needs to be designed with security in mind. There's too much at risk. For instance, a denial of service attack could prevent your customer from reaching your web site or services and block you from doing business. Defacement of your website damages your reputation. And a data breach could be even worse — as it can ruin hard-earned trust, while causing significant personal and financial harm. As administrators, developers, and IT management, we all must work to guarantee the security of our systems.

Let's say you work at a company called Contoso Shipping, and you're spearheading the development of drone deliveries in rural areas-while having truck drivers leverage mobile apps to deliver to urban areas. You're in the process of moving much of Contoso Shipping's infrastructure to the cloud to maximize efficiency, as well as moving several physical servers in the company's data center to Azure virtual machines. Your team plans on creating a hybrid

solution, with some of the servers remaining on-premises, so you'll need a secure, high-quality connection between the new virtual machines and the existing network.

Additionally, Contoso Shipping has some out-of-network devices that are part of your operations. You are using network-enabled sensors in your drones that send data to Azure Event Hubs, while delivery drivers use mobile apps to get route maps and record signatures for receipt of shipments. These devices and apps must be securely authenticated before data can be sent to or from them.

So how do you keep your data secure?

1.a

• How to secure your **application**?

|  |
| --- |
| Answer: |

• How to secure your **compute** resource? Why is it important?

|  |
| --- |
| Answer: |

• How to secure your **network**?

|  |
| --- |
| Answer: |

**Task 2: Identity and access**

2.

Network perimeters, firewalls, and physical access controls used to be the primary protection for corporate data. But network perimeters have become increasingly porous with the explosion of bring your own device (BYOD), mobile apps, and cloud applications.

Identity has become the new primary security boundary. Therefore, proper authentication and assignment of privileges is maintaining control of your data.

Your company, Contoso Shipping, is focused on addressing these concerns right away. Your team's new hybrid cloud solution needs to account for mobile apps that have access to secret data when an authorized user is signed in — in addition to having shipping vehicles constantly send a stream of telemetry data that is critical to optimizing the company's business.

• Compare the different between **authentication** and **authorization**.

|  |
| --- |
| Answer: |

• **What is Azure Active Directory?**

|  |
| --- |
| Answer: |

• **Why Single Sign-On is important in cloud security?**

|  |
| --- |
| Answer: |