



# Cyber security exercise report

## Bring Your Own Device (BYOD)

Prepared by: \_\_\_\_\_

Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

## Executive summary

Our team ran a discussion-based cyber security exercise session on the reported date using the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) Exercise in a Box. This report summarises the results of this exercise and includes recommendations for our organisation to consider.

## Discussion outcomes

What we learned from running the exercise:

How our understanding of preventing this type of cyber security threat changed:

What will we look to change or implement:

## Team statements

We rated our confidence against the following statements:

### Observations from Inject 1: Business data

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Your organisation tracks or restricts business data stored on personal devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has an efficient process for managing any legal or regulatory issues surrounding the use of personal devices to deliver your business.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 2: Device management

Your organisation has an effective method of segregating access to corporate data on personal devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has a sensible approach for dealing with security incidents involving personal devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has a clear policy describing procedures in the case a personal device must be seized or wiped.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 3: Risk management

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Your organisation has a clear policy and guidance on how to secure personal devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employees are given training in order to make them aware of BYOD policy and the need to keep their personal devices secure.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has controls in place to prevent the spread of malware should a personal device become infected.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 4: Policies

Your organisation is aware of the positives and negatives of a BYOD policy and has made a well-informed decision to implement this model over alternative ownership models.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has an effective BYOD policy that protects against unauthorised access to business data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has procedures in place to ensure that when staff leave, their access to business services and data via personal devices is revoked.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>