holibob

Portable Media Use - Policy

Version: 3

29 October 2024

Table of Contents

1 Introduction

Any Holibob system or removable storage media used for work purposes must be encrypted to The Company's standards.

Security encryption is a mandatory measure and one of the most important methods we have to protect our own and our Partner's information.

2 What is 'removable' media?

Laptops and USB memory sticks are The Company's most commonly used examples of removable media.

Removable storage media includes:

- Laptops
- USB memory sticks
- Writeable CDs/DVDs
- External hard drives
- Off-line file repositories such as instances of OneDrive, and DropBox that are outside of The Company's infrastructure
- File-sharing systems typically used for the transfer of large files

Our Security guidance specifies that USB memory sticks and other user-removable media should not be used to store data that is owned by The Company or our Partners.

Only in exceptional circumstances, where there is compelling business justification and where specific written approvals have been granted by senior management, should approved USB sticks with device encryption be used.

2.1 USB memory sticks

This guidance is intended to ensure that our data remains secure and to mitigate the potential impact of lost devices.

1. You must only connect approved external removable storage media to company systems and devices.

2. Connecting non-approved memory sticks is a breach of our security guidelines, and could result in disciplinary action.
3. If there is a genuine business requirement to save, retrieve or transfer data via removable media, you must obtain written approval from a person at the director level or above.
4. Each request is evaluated by senior management and the operational security team, to recommend the safest and most appropriate method to contain the risk of loss.
5. Normally, you'll get a response within 5 working days.
6. Requests to use a memory stick or other removable media will normally only be granted when there is no other practical alternative. Where approval is granted. only encrypted memory sticks or other removable devices provided by The Company are permitted for the given use case
7. Use of memory sticks or other removable devices will be subject to stringent conditions and permitted only after user training.

If you need further assistance or information about this process please speak with your line manager and/or the operational security team.

2.2 How do I know if my laptop, or USB stick, is encrypted?

All equipment provided through The Companies is encrypted and protected to TheCompany's security standards.

You must use approved processes to obtain any equipment used for business purposes, including mobile computing devices and removable media.

2.3 What's expected of you

Keeping our information safe is everyone's responsibility.

Anyone using portable computing equipment must take particular care to safeguard the equipment and the information stored on it.

Failure to do so may result in disciplinary procedures.