# INFORMATION SECURITY CHECKLIST

## Encryption Exemption for Direct Attached Storage (DAS) with Low Risk Information

### Introduction

1. This document is intended to assist [Information Stewards/Owners](#) in managing their encryption compliance for [Direct Attached Storage (DAS)](#) containing only Low Risk Information.

2. This document has been issued by the Chief Information Officer to supplement the [Encryption Requirements](#) standard. Questions about this document may be referred to [information.security@ubc.ca](mailto:information.security@ubc.ca).

3. To be exempt from encryption requirements, DAS must be fully compliant with either the External or Internal DAS criteria in the checklist below.

### Checklist

#### External DAS

- The DAS is an external array of drives that is not considered portable, and cannot easily be carried or moved by an average individual.
- The DAS requires a [Server](#) or host system to operate.
- The DAS is not network accessible without a host system.
- The DAS is locally mounted on a host, e.g. connected via Thunderbolt 3.
- The DAS is physically secured via security cable, locking cabinet or other similar physical security measure.
- There is no Personal Information stored on the DAS, nor will there ever be.
- The information on the DAS is Low Risk Information only and will never change to be of a higher risk level.

#### Internal DAS

- The DAS is internal and housed in a Server.
- The Server housing the DAS is physically secured via security cable, locking cabinet or other similar physical security measure.
- There is no Personal Information stored on the Server, nor will there ever be.
- The information on the Server is Low Risk Information only and will never change to be of a higher risk level.

4. The completed checklist must be submitted to [information.security@ubc.ca](mailto:information.security@ubc.ca). The CISO must be informed if the DAS is no longer compliant with the checklist.

### Related Documents

[Encryption Requirements standard](#)