**Cryptography For Redback Operations:**

* Protection and confidentiality of data and files.
* Safety of communication.
* Authorised access only.

**Encryption Standards:**

**Advanced Encryption Standard (AES)**

Symmetric Encryption algorithm which is primarily used when using the same key for both encryption and decryption.

**ISO/IEC 19790:2012**

This standard covers many topics including how the encryption is implemented, authentication, testing and configuration management.

**ISO/IEC 24759:2017**

This will cover how the testing process works and allowing for their to be impartialness when any testing occurs.

The following standards which are listed need to be reviewed and they must be followed accordingly.

**Classification Levels:**

* Open/Public
* Private/Confidential

Individuals will need to be able to determine which files they need to be deemed public and which ones are more private and will need encryption.

**Encryption Software:**

VeraCrypt

* This is a solid software which our company can utilise as it is cost-free and contains many options which can be used. This includes different algorithms such as AES and Serpent which are highly regarded; however, they are difficult to use.

BitLocker

* This is a full disk encryption software which means it allows for an entire disk to gain the effects of encryption, where instead of being file by file. This is an easy-to-use software for all devices; however, it can only be used for devices on windows, which can be limiting for company use.

Nord Locker

* This is a safe and very secure option as it allows for only the user to access the data, while also being very easy to use and set up. Additionally, it also allows for both windows and MAC devices to utilise. However, this is a file by file-based encryption instead of it being a disk-based encryption, while also costing money as it is subscription based.

AxCrypt

* This is another subscription-based file by file encryption software however it offers an easy-to-use secure protection as it allows for password protection for access to any encrypted file. There is also a free version of this software which can be tested by the company and can be upgraded to the premium at any time which expands the range of benefits.

**Expected Users and Devices:**

This implementation plan has been developed to be used company-wide, however it does mainly pertain to the developers as it is something important to consider when creating or modifying company data.

Additionally, amongst the devices that would be covered by this plan, they would include companywide personal devices which all members contain. As for the hardware within the company, it would primarily pertain to the raspberry pi hardware.

**Regulatory Compliance:**

Regular audits which have said need to be conducted throughout our team will help ensure that our standards and use of encryption are being used accordingly.

**References:**

Encryption Standards:

<https://www.iso.org/standard/52906.html>

<https://www.iso.org/standard/72515.html>

<https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography>

<https://www.passcamp.com/blog/data-encryption-standards-what-you-need-to-know/#:~:text=Common%20Data%20Encryption%20Standards,at%20rest%20and%20in%20transit>.

Encryption Software’s:

<https://www.techrepublic.com/article/encryption-software/>

<https://sourceforge.net/projects/veracrypt/> - VeraCrypt

<https://axcrypt.net/pricing/> - AxCrypt

<https://nordlocker.com/?utm_campaign=off489&utm_content=tr&utm_term=affiliate&utm_medium=affiliate&utm_source=aff66760> – Nord Locker