|  |  |
| --- | --- |
| **Document Name** | **Physical Media Handling** |
| **Version** | **0.2** |
| **Last updated by** | **Anjaly T A** |
| **Approved By** | **Inderjit Singh Bedi** |
| **Released on** | **25-10-2022** |

# Introduction

Physical Media Handling is the critical aspect for any organization’s communication method. It is of utmost importance that the policy is defined at an organizational level to establish the need to secure information and information processing facilities. Access any kind of physical media should be controlled on the basis of business and security requirements.

# Objective

The purpose of this Policy is to prevent unauthorized access to any physical media by any unauthorized people. This Policy is designed to protect physical media devices from unauthorized change, or destruction, whether intentional or accidental.

# Scope

The scope of this Policy includes all XTRACAP employees. Each employee is responsible for carrying out his or her responsibilities under this Policy.

# Policy

**4.1 Management of Removable Media**

Obviously, this presents two clear risks, loss of information and corruption of information or introduction of unknown software when the device is reintroduced onto the organisations network.

If no longer required, information should be deleted/destroyed and made unrecoverable. If necessary, authorisation should be required and records of this kept. Cryptography should be considered in order to protect from loss of data. If the media is being removed for backup purposes, it should be stored separately (think co-location) to remove the risk of correlated threats, but security should be considered for offsite storage, and multiple copies could be considered on discrete devices to protect against degradation of the data. Removable drives should only be permitted as a conscious choice to accept rather than the other way around. IT departments need to be aware that enabling the USB sockets on the CEOs computer for ease of use is often the most straightforward way for a 3rd party to gain access (physically or logically) to the organisations network.

Documented procedures are required to cover the handling of removable media.

**4.2 Disposal of Media**

This should be done securely, and disposal records should be kept. If devices containing sensitive data are damaged it should be a consideration to physically destroy them rather than sending them to a third party for repair.

**4.3 Physical Media Transfer**

If subcontracted, a list of approved carriers / couriers should be maintained, and procedures put in place for the identification of those couriers. Logs of identification of information, time of transfer and receipt should be maintained – this should form part of the procedures.

# Enforcement

Violations of this Policy include, but are not limited to: accessing information which the individual has no legitimate access to; enabling unauthorized individuals to access the media; disclosing media in a way which violates applicable policy, Policy or other relevant regulations or laws; or inappropriately modifying or destroying information. Violations may result in access revocation, corrective action up to and including dismissal, and/or civil or criminal prosecution under applicable law.