| Version | 1.0 |
|---|---|
| Issue Date | 17th March 2020 |

بسم الله الرحمن الرحيم

**National Centre for Information Technology**
64, Kalaafaanu Hin'gun, Male', Republic of Maldives

# ESTABLISHING A WORK-FROM-HOME ENVIRONMENT

## 1. Introduction

### 1.1. Scope

This control applies to all systems, people and processes that constitute the organisation's resources, including board members, directors, employees, suppliers, political appointees, and other parties who have access to the organizations information systems.

This guideline sets out the key information security-related elements that must be adhered while working from home via the established work-from-home arrangement to ensure that the organisations resources are protected

This policy **does not** address the human resources aspects of work-from-home such as health and safety, absence monitoring, job performance and contractual issues. These will be handled by the HR department separately and must also be in place before the work-from-home arrangement begins.

### 1.2. Purpose

A work-from-home arrangement is issued as per employment guidelines and other set working agreements between the organisation and the employee. It usually involves the employee working from home while work is assigned to the employee by their respective supervisors according to the organizations need.

The introduction of a work-from-home arrangement, if managed effectively, has the potential to benefit both the individual and the organisation. The individual will gain greater flexibility in working arrangements and possibly avoid having to come to work premise during state of emergencies.

## 1.3. Policy

### 1.3.1. Putting a Work-from-home Arrangement in place

From an information security point of view there are various aspects that need to be considered in each work-from-home arrangement by the organization. The policy of the organisation in these areas should comply with the following sections.

Furthermore, a work-from-home agreement should be signed between organization and employee prior to allowing work-from-home. This will be ensured by the Human Resource Department (or as per the instructions by the Head of Organization/ZV)

# 2. Procedure

## 2.1. Initial Risk Assessment

Before a work-from-home arrangement can commence there should be an initial risk assessment of the proposed environment to determine the nature of the work to be carried. This task will be carried out by the staff responsible to ensure the information security of the respective organization.

## 2.2. Nature of the Work

A major part of the risk assessment concerns the type of activities that are to be carried out as part of the arrangement. A full understanding needs to be gained of:

a) The classification of the information that will be stored on local device and processed as part of the role.
b) The method of access to the information
c) Whether the role requires that classified information to be printed locally
d) The business criticality of the role and the consequences if it were unavailable

## 2.3. Physical Security

The risk assessment should consider the physical security of the proposed work location:

a) Is there enough room to house the required equipment safely?
b) Is it in a separate area of the living accommodation?
c) Can the work area be secured e.g. via a locked door when not in use?
d) Identify and make a list of who else has access to the work area?

e) Will the work-from-home setup be visible from outside the accommodation e.g. through a window?
f) What is the likelihood of theft in the surrounding area?
g) Can paper documents be locked away securely?

## 2.4. Equipment

### Option 1:

Only client equipment provided by the organization is used for work-from-home arrangements. In this case, or organization may provide the following:

a. A laptop or desktop PC with keyboard and mouse
b. A printer/scanner
c. Secure storage e.g. drawers or a cupboard

In this case the equipment remains the property of the organisation at all times and must be returned to the organization when asked to do so

### Option 2:

In the event that the organization is unable to provide organization's equipment, the organization may opt to allow for individual's own devices such as laptops or PCs after ensuring the security of the devises as per section 3.6 (Backup and Virus Protection)

## 2.5. Backup and Virus Protection

Where possible, no data will be stored on the client machine. In the event that this is unavoidable it is the responsibility of the employee to ensure it is backed up to the organizations network as soon as possible.

Virus protection must be provided on all relevant organization issued equipment and configured to update automatically.

When using employee's own device, it is the responsibility of the employee to ensure that the device is protected from computer viruses.

### 2.6. Agreement Termination

In the event that the work-from-home agreement is terminated for whatever reason, all equipment that was supplied as part of the arrangement must be returned to the organization as soon as possible.

## 3. Technical Support

All issues related to work-from-home should be reported to Information Technology Task Force (ITTF) hotline number 3302211 or emailed to 3302211@ncit.gov.mv by the organization.

For assistance with establishing the VPN at each organization, IT managers should contact the ITTF for assistance and other details.