<< Organisation Logo>>

<< Bring Your Own Device (BYOD)/Hand-Held Device Policy >>

Version: 1.0
Date

Version: xx   **Date: xx**   **Company Name: xx**

Security Level: Internal   **Page 1 of 5**
NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,   **www.nethostlegislation.co.uk**

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Contents

Contents

INTRODUCTION

DOCUMENT PURPOSE

The use of Bring Your Own Device (BYOD)/Hand-Held Device is increasing in the industry, providing services and constant connectivity to staff and 3rd parties to the [organisation]. Due to the fact that BYOD/Hand-Held Devices need to be properly managed, they present new threats to Information Assets.

This policy establishes rules for the proper use of BYOD/Hand-Held Device in order to protect the **Confidentiality of Sensitive Data**, the **Integrity of data and Applications**, and the **Availability of services**.

SCOPE

This policy applies to all Employees, Consultants, Vendors, Contractors and others using business or private BYOD/Hand-Held Device.

POLICY

Below are statements must be complied with.

Policy Statements

No:	Statements
	ICT Team shall define Applications/Systems that private BYOD/Hand-Held Device are authorized to connect. This must be identified and documented accordingly.
	In highly restricted facilities (E.g. Data Centers/Disaster Recovery Centre, private BYOD/Hand-Held Device MUST be prohibited. In that case, mobile devices MUST be collected prior to the user/staff's entrance into the facility.
	Any non-business-owned BYOD/Hand-Held Device able to connect MUST first be approved
	If allowed, privately- BYOD/Hand-Held Device MUST comply with this security policy and applicable policies, and MUST be inventoried along with corporate handhelds, but

Version: xx   **Date: xx**   **Company Name: xx**

Security Level: Internal   **Page 4 of 5**
NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,   www.nethostlegislation.co.uk

	identified as private. This is in order to prevent theft of corporate data with unmanaged handhelds (i.e. owner of device is not identified).
	Staff assigned to use BYOD/Hand-Held Devices MUST be trained in order to ensure the proper use of devices and corporate resources. A focus on corporate applications and basic security features is mandatory.
	An inventory of BYOD/Hand-Held Device in use, associated owner name and identity for network access control(NAC) is mandatory. This inventory MUST take in to account at least but not be limited to the following list of identifiers: - Device name - Owner's ID - Device serial number - Device's MAC address - Owner's ID (user) - Device capabilities (Bluetooth, IrDA, Camera, etc.)
	Procedure for reporting lost BYOD/Hand-Held Device MUST exist and be clearly communicated to all staff