**Purpose and scope of this policy**

This policy outlines the guidelines for using personal devices (laptops, smartphones, tablets, etc.) within our organization’s premises. It aims to ensure the security of company data and systems.

As such, this policy relates to all our users. It includes the use of personal smartphones, laptops, tablets, and wearable devices and other such devices.

**Eligibility**

* All users are allowed to make use of their personal devices to access the public network within the organization.
* The internal network must only be accessed by provided devices devices, unless special approval has been granted by the IT department.

**Roles and Responsibilities**

Every user is responsible for following the guidelines within this policy. Not adhering to it may result in systems compromise and/or leakage of data which will have consequential results.

If you participate in the BYOD programme and your device has been approved for internal access, you must ensure the following:

* **Updates**:
  + Ensure your device software is up-to-date.
* **Password Protection**:
  + Use strong passwords to ensure no unauthorized access.
* **Loss/Theft**:
  + Immediately report any lost or stolen device to the IT Department for risk mitigation.
* **Security:** 
  + Install and maintain security software, as stated in the security policy.
  + Only approved software may be used to interact with the organization’s data and systems.

**Points of contact**

In the case of any question regarding to the policy, please contact the IT department.