DEVICE USER AGREEMENT POLICY

Name of Organisation: Pony Partnerships CIC.
Venue/address for which policy applies: All venues.
Date of last review: 1st September 2024
Date of next review: 31st August 2025
Name of author: Danielle Mills

Introduction

Mobile devices, such as smartphones and tablets, are important tools for our organisation. However, mobile devices also represent a significant security risk as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to data breaches and system infection.

Pony Partnerships CIC has a requirement to protect its information assets in order to safeguard its customers, intellectual property, and reputation. This document outlines a set of practices and requirements for the safe and secure use of mobile devices.

Roles & Responsibilities

The Board of Directors is responsible for maintaining this policy and ensuring that it is fully implemented.

Policy Scope

1. All mobile devices, whether owned by Pony Partnerships CIC or owned by employees, which have access to corporate networks, data, and systems, not including corporate IT-managed computers or laptops. This includes smartphones and tablet computers.
2. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted, and any exemption authorised by the Danielle Mills (Director)

Policy

1. Technical Requirements
    a. Devices must use the following Operating Systems: Android 12 or later, IOS 14 or later.
    b. Devices must have data encryption enabled at all times.
    c. Devices must be configured with a secure PIN/password that complies with Pony Partnerships CIC's password policy. This password must not be the same as any other credentials used within the organisation. In addition, where supported, devices should be secured using biometric security (e.g. Touch ID).
    d. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

User Requirements

1. Users must report all lost or stolen devices to Pony Partnerships CIC IT (Danielle Mills, Director) immediately.
2. If a user suspects that unauthorised access to company data has taken place via a mobile device, the user must report the incident to Danielle Mills (Director).
3. Devices must not be “jailbroken”* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
4. Users must not load pirated apps/software or illegal content onto their devices.
5. Applications must only be installed from official platform-owner approved app stores. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact (Danielle Mills, Director)
6. Devices and all apps/software must be kept up to date with manufacturer-provided patches/updates.
7. Users should avoid the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in the body of text or as an attachment, they must notify Danielle Mills (Director) immediately.
8. Users should avoid opening or saving any work-related documents using personal email accounts or personal document storage. All documents should only be sent, opened, and saved using Pony Partnerships logins as provided through Office 365.
9. Users must not allow Pony Partnerships data to backup or synchronise to personal email accounts or data storage.
10. Users must not use corporate workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.
11. Users must ensure that they have taken steps to ensure the electrical safety of any devices used on site, particularly those that are plugged into the mains.
12. Users must use virus protection on all devices when they are connected to the Pony Partnerships Wireless Internet.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.