Virtual Private Network (VPN) Policy

1. Purpose

1.1 This policy complements Metaverse VR Ltd's (MVR) Remote Working Policy, both are integral to establishing a secure remote working access environment for MVR employees.

1.2 The aim of this policy is to outline the guidelines for the use of Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to access MVR's network securely.

2. Policy

2.1 All employees, contractors and consultants with remote access privileges to the MVR network are required to use a VPN-enabled connection. This policy strictly applies to VPN connections using Cisco AnyConnect only. No other VPN or remote access software is authorised by MVR.

2.2 Approved employees and third parties (contractors) can access MVR's VPN service, which operates as a "user-managed" service. This means users are responsible for choosing an Internet Service Provider (ISP), managing installation, installing any required software and covering associated costs where applicable. Refer to the Remote Access Policy for more detailed instructions.

3. Scope of the Policy

3.1 This policy applies to all MVR employees, Directors, and anyone engaged by MVR or its subsidiaries.

3.2 Self-employed consultants or contractors must also comply with this policy, and MVR ensures they are provided with a copy.

4. Responsibility for the Policy

4.1 The Senior Leadership Team (SLT) are responsible for ensuring this policy is adhered to.

4.2 The success of this policy depends on individual compliance. Employees are to read and understand this policy and raise any questions with their managers for clarification.

Registered in England: 13684068, VAT No: GB 399750824.
Registered office: 3.05, Innovation and Collaboration Hub Portsdown Technology Park, North Hill Portsmouth, PO6 3RU
Tel: +44 (0) 2393 552 794 Email: info@metaverse-vr.co.uk