SCOTLANDIS

Proposed ITMSP Best Practice Charter

1. **Purpose**
   This charter establishes a framework for Managed Service Providers (MSPs) to deliver secure and reliable IT services while incorporating the National Cyber Security Centre (NCSC) 10 Steps to Cyber Security. It aims to drive consistency, reduce misunderstandings, and promote a shared approach to best practices.

2. **Commitments**
   ITMSPs signing up to this charter will commit to the following shared objectives:

   I. Consistency and Shared Approach
   Drive consistency across the community and supply chain, creating a shared and consistent view to deliver best practice and create sustainable value for the Scottish Cyber Eco-System.

   II. Impact and Influence
   Create impact and influence through the services provided by MSPs, positioning Scotland as a less attractive target for threat actors.

   III. Resilience and Risk Reduction
   Drive cyber resilience, reduce risk, and enhance the ability to respond by managing services effectively.

   IV. Transparency
   Improve cyber resilience across the community and supply chain, promoting shared knowledge about risks, vulnerabilities, and threats.

   V. Alignment and Governance
   Provide alignment to the NSCS 10 Steps, and governance to improve the IT Managed Services industry as a whole.

   VI. Social Responsibilities
   Ensure MSPs consider wider social responsibilities in their operations.

3. Charter Standards

This charter sets out the standards that ITMSP's who sign up to the charter, will apply in their own organisation and in the services, they provide to customers. It will instil confidence in customers, allowing the Scottish Government to endorse ITMSPs based on their application of these standards.

I. Secure Configuration
Implement a baseline secure configuration, regularly updating and patching systems, and minimizing the attack surface.

II. Boundary Firewalls and Internet Gateways
Deploy robust firewalls, regularly reviewing and updating rules, and implementing intrusion detection and prevention systems.

III. Access Control
Enforce strong password policies, least privilege access, and regularly review and revoke unnecessary user accounts and access privileges.

IV. Patch Management
Establish a comprehensive patch management process, testing patches before deployment and implementing automated patching where possible.

V. Malware Protection
Deploy reputable antivirus and anti-malware solutions, conduct regular scans, and educate employees on safe browsing practices.

4. Proposed Enhanced Standards

I. Secure Configuration for Mobile Devices
Establish a mobile device management policy, enforce security controls, encryption, and provide guidelines for secure usage.

II. Monitoring
Implement a comprehensive security monitoring system, monitor system logs, network traffic, and user activities, and conduct regular incident response drills.

III. User Education and Awareness
Regular cybersecurity training, teach employees to identify and report suspicious activities, and promote a culture of cybersecurity awareness.

By embracing this charter and applying the standards set out above, ITMSPs aim to establish a secure and resilient cyber security environment, foster collaboration and enhance Scotland's reputation as a secure digital ecosystem. Regular reviews and updates to these guidelines are essential to adapt to evolving threats and technologies in addition to supporting organisations to achieve these standards.