ScotlandIS

IT Managed Service Provider

Best Practice Charter

Copyright © ScotlandIS

Mission Statement

The mission of the ITMSP Charter is to create a community that will deliver secure and trusted client services to build cyber resilience throughout the supply chain and the Scottish economy.

Definition of ITMSP

For the purpose of the ScotlandIS ITMSP Charter, the definition includes but is not limited to:

- Information Security Providers (ISP) (Clear that ISP does not mean Internet Service Provider)
- Managed Service Provider (MSP) and
- Managed Security Service Provider (MSSP)

An ITMSP must deliver regular, ongoing and/or continuous administration, maintenance, management, service and support of a customers:

- Data
- IT Infrastructure
- IT Networks and/or IT Systems

- ITMSP services are provided on the customer's premises, in the ITMSP's data centre or in a 3rd party data centre, including hyperscale cloud, remotely or in person

- An ITMSP provides clarity and definition on the management of the services provided ensuring clarity between ITMSP and customer on what is and what is not within scope

- An ITMSP outlines the processes involved in the shared responsibilities of the service provision. Ensuring clarity on shared responsibility between ITMSP and customer

- AN ITMSP has agreed, appropriately managed and privileged access to perform essential or sensitive functions; process and/or store business data

- AN ITMSP provides or is capable of providing education and guidance to improve cyber security and business resilience either themselves or through partners

- An ITMSP delivers their own native services and may collaborate or provide services in conjunction with other suppliers including provider and reseller of software as a service, cloud computing etc

Copyright © ScotlandIS

Objectives of the ITMSP Best Practice Charter

- Drive consistency across the community and supply chain
- Reduce misunderstandings in service delivery
- Create a shared approach and a consistent view on delivering best practice and improve standards across the ITMSP industry
- Create sustainable value for Scottish eco-system, reflecting guiding standards
- Create impact and influence through the services provided by ITMSP's
- Drive resilience, reduce risk and increase ability to respond
- Share knowledge about risks vulnerabilities and current threats
- Ensure ITMSP's consider wider social responsibilities

Commitments

ITMSPs signing up to this charter will commit to the following shared objectives:

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

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

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

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

- Alignment and Governance
  Provide alignment to Cyber Essentials Controls and governance to improve the IT Managed Services industry as a whole

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

Copyright © ScotlandIS

ITMSP Best Practice Charter
Essential Standards

ITMSP's will commit to applying all of the following standards. These will apply in their own organisation and in the services they provide. By applying these standards, they will instil confidence in customers and improve cyber security throughout the supply chain.

- Secure Configuration
  Implement a baseline, secure configuration minimising the attack surface.

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

- Access Control
  Use and enforce strong password policies, least privilege access and multi-factor authentication as a minimum. Regularly review and revoke unnecessary user accounts and access privileges.

- Security Update Management
  Establish a comprehensive patch management process and implement automated patching where possible.

- Malware Protection
  Manage an appropriate antivirus and anti-malware solution that conducts regular scans. Educate employees on safe browsing practices.

- Asset Management
  Employ an asset management process to control assets, patch levels and understand their relevant vulnerabilities and priorities.

Copyright © ScotlandIS

IT Managed Service Provider
Enhanced Standards

ITMSP's will commit to applying all of the Essential Standards **and at least two** of the following additional Enhanced Standards:

And at least 2 of the following Enhanced Standards:

- Cyber Essentials Plus
  Maintaining annual accreditation

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

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

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

- Back Ups
  Establish an effective and secure back up management process with regular monitoring and testing.

- Testing
  Establish an effective testing process including intrusion, PEN, regression or software testing.

Copyright © ScotlandIS

Sponsorship and Partnership Agreement

Sponsorship
ITMSP's seeking to sign up to the Best Practice Charter will require sponsorship from existing members of the Charter Working Group. They will also be required to attend network events and contribute to review and development of the charter.

Partnership Agreement
By signing up to the ITMSP Best Practice Charter we commit to applying the required **Essential/Enhanced standards** (Delete as appropriate).

We will work collaboratively with the ITMSP community to support other organisations to achieve these standards in order to establish a secure and resilient cyber security environment, foster collaboration and enhance Scotland's reputation as a secure digital ecosystem. We understand that regular reviews and updates to these guidelines will be carried out and that these are essential to adapt to evolving threats and developments in technologies.

Karen Meechan – CEO For and on behalf of ScotlandIS

K Meechan

____

Organisation Signatory

____

Copyright © ScotlandIS