Incident Management Policy

Confidential

Author / Owner:			
Date Issued:	August 2018		
Last Reviewed:	April 2020	Next Review:	March 2021

1. Scope

1.1. Introduction

Information forms part of the service we deliver. Without access to the right information at the right time we cannot provide the trusted advice that forms the basis of our relationship with our colleagues, customers and OEMs.

Incident Management is an important part of delivering that trust and all Markets/Regions need to ensure they have appropriate Incident Management Processes in place.

1.2. Why do we have this policy?

The purpose of this policy is to ensure that Inchcape's incident response capabilities, used to monitor and respond to security incidents have a maintained quality and integrity. The incident response capabilities can determine the magnitude of the threat presented by these incidents and assist in the response to the incidents faced.

Without an incident response capability, the potential exists that in the event that a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

1.3. What does this policy apply to?

The Incident Management Policy applies to all information systems and information system components of Inchcape that provide Critical Services to the company. This could include:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

2. Security Requirements

2.1. Basic Security Requirements

Each Market/Region must have a Security Incident Procedure developed that allows the local teams to respond to the main cyber-attacks faced by companies.

The security incident procedure must be a defined plan and address 4 stages of Incident Response

- Confirm
- Control
- Remediate
- Check

Incidents must be tracked, documented and reported to appropriate officials and if necessary authorities

2.2. Local/Regional Computer Emergency Response Teams (CERTs)

All regions must register with local and appropriate CERT websites and services. The CERT's provide valuable information regarding cyber security incidents affecting local companies. The list of CERTs can be found here - https://first.org/members/teams/

2.3. Derived Security Requirements

Security incident response capabilities must be tested annually to facilitate incident response operations. Responsibility for incident-handling operations will be assigned to an incident response team.

Incident response plans will be reviewed and, where applicable, revised on an annual basis. The review must be based on the documented results of previously conducted tests or live executions of the security incident procedure. Upon completion of procedure revision, updated plans will be distributed to key stakeholders.

2.4. Relevant Procedures and Records

As well as the security incident procedure, each market\region must have the following in place for the Critical\Important IT Services provided to the Inchcape Business

- A Critical IT Systems & Applications Record
- A 3rd Party Incident Management Contact Record
- A Local IT Business Continuity Plan