# IT Guideline - Workstation

# Southern Response Earthquake Services Limited

Author: [redacted] (IT Manager)

# Document control

| Change Description | Author | Version | Date | Approved By |
|---|---|---|---|---|
| Initial Draft | [redacted] | Draft 0.1 | 21-04-2013 | |
| Review | [redacted] | Draft 0.3 | 27-05-2014 | |
| Review | [redacted] | Draft 0.4 | 8-05-2015 | |
| | | | | |

# Table of Contents

# 1) Introduction

## 1.1) Statement of intent

This document defines guidelines for the protection of SRES's workstations and information stored on them.

## 1.2) Scope

This document applies to all SRES workstations (e.g. laptops, desktops, PDAs, mobile phones with corporate information) and users of it.

## 1.3) Review

This document will be reviewed on an annual basis by the IT MANAGER. The review will assess both the content of the document and the compliance with controls identified within the document

## 1.4) Relevant References and Resources

- Use of Information Resources and Security Policy
- IT Standard – Acceptable Use
- IT Guideline – Virus Protection

## 2) Guidelines

- All desktops must be kept in secure areas
- Laptops carrying confidential data must be encrypted using BitLocker or an IT approved equivalent tool
- **ALL** smartphones, tablets, pocket PCs and other similar devices must have power on passwords/pins implemented to prevent unauthorised access. They should have password/pin protected timeouts enabled and should have encryption implemented
- All workstations must be patched according to SRES's Patch Management guidelines
- Baseline workstation operating system security standards must be developed and applied. These standards must be used to build and secure standard images that must be used to build user desktops. The images should ensure password protected screen savers are in place that cannot be changed or disabled by the users
- Users must not be permitted to make changes to workstation configurations unless explicitly permitted by their Manager and accepted by IT. This authorisation needs to be obtained and recorded in writing. As a general rule, users must not be granted Administrator access to their work stations and should be restricted from making changes to their workstations via Group policy
- All workstations must have virus and spyware protection implemented according to SRES's Virus Protection guidelines
- Details of workstation configurations must be maintained

## 3) Guideline Breaches

Failure to conform to this policy may constitute misconduct. Persistent breaches of these policies may constitute serious misconduct. The procedure for dealing with cases of misconduct, as outlined in the SRES's Code of Conduct, would be followed in such cases. Depending on the extent of any breach, the conduct of the employee/s concerned, the extent of material sent/received, a breach of these policies could result in serious consequences such as summary dismissal. It is therefore important that you read and understand these policies.