Southern Response
6 Show Place
Christchurch, New Zealand

IT Guideline - Virus Protection

Southern Response Earthquake Services Limited

Author: [redacted] (IT Manager)

Document control

Change Description	Author	Version	Date	Approved By
Initial Draft	Gen-i	Draft 0.1		
Draft	[redacted]	Draft 0.2	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 has been developed to manage the risks to SRES IT systems and information from the introduction of viruses and other malicious code.

1.2) Scope

This document applies to all SRES computer systems and users of those systems.

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

2) Guidelines

2.1) Anti-Virus Requirements

The following requirements must be implemented to minimise the risk of virus infection:

- Anti-Virus software will be installed on ALL Servers, Desktops and Laptop PCs, including those in Development, Test and DMZ zones. Where possible, Anti-Virus software will also be installed on PDAs and other portable devices that connect to the SRES network
- Anti-Virus software will be installed on mail and web gateways to scan all incoming and outgoing data
- The required software settings and configurations for all Anti-Virus software installations will be documented. This standard will be reviewed by IT MANAGER on an annual basis and the Anti-Virus product(s) used will be re-evaluated
- Anti-Virus software will allow for centralised management, alerting and reporting on security events
- Anti-Virus software must be configured to perform real-time virus scanning for computers on the SRES network, and scanning of data on removable media before it is copied to SRES computers
- Complete Anti-Virus scans must be performed before each information backup
- Anti-Virus software must be able to quarantine/clean or alert administrators (via pager or email) immediately if a virus is detected
- Anti-Virus software must allow for real-time updating of virus signatures for all computers, including those located in DMZs and isolated network segments. Where automated updates are not technically feasible manual processes must be developed to ensure Anti-Virus signatures are updated on a regular basis
- Anti-Virus software on user PCs must be configured so that users cannot disable Anti-Virus protection or uninstall Anti-Virus software
- Non-SRES computers (e.g. Contractor laptops) that connect to the SRES network must have Anti-Virus software that has up-to-date and is approved by the IT MANAGER

2.2) Anti-Virus Management

A successful Anti-Virus solution must encompass adequate management controls to monitor the environment and detect and manage any virus outbreaks:

- The Anti-Virus management server will be checked and reported on a monthly basis by designated Service Provider to confirm that all Anti-Virus signatures have been applied successfully. Where the management server does not provide this functionality other mechanisms must be used to confirm signature updates (e.g. manual checks or scripted queries)
- Administrators must respond to all virus alerts immediately, assessing the risk of the outbreak and if necessary initiating the incident response processes in line with Incident Management or Business Continuity processes
- All virus alerts (where the Anti-Virus software does not automatically delete/quarantine/clean a virus) should be recorded, along with the actions taken to remove the virus. If possible the source of the virus should also be recorded so that controls can be implemented to protect against future outbreaks
- New computer systems must have Anti-Virus software installed as part of the standard build process and procedures must be in place to ensure Anti-Virus signatures are updated before placing the system in the production environment
- All systems should be audited for compliance with the Anti-Virus guidelines on an annual basis. This is in addition to the monthly operational checks and will include a review to ensure all systems are running the latest version of Anti-Virus software and that all settings are configured as expected

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.