Southern Response
6 Show Place
Christchurch, New Zealand

PROACTIVELY RELEASED BY
SOUTHERN RESPONSE EARTHQUAKE SERVICES LTD

IT Guideline - Network Security

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	

PROACTIVELY RELEASED BY
SOUTHERN RESPONSE EARTHQUAKE SERVICES LTD

Table of Contents

PROACTIVELY RELEASED BY
SOUTHERN RESPONSE EARTHQUAKE SERVICES LTD

1) Introduction

1.1) Statement of Intent

This guideline document defines controls for the protection of Southern Response's (SRES) network infrastructure and information stored on the network.

1.2) Scope

This document applies to all SRES network equipment (e.g. firewalls, routers, switches, servers, hubs) 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

PROACTIVELY RELEASED BY SOUTHERN RESPONSE EARTHQUAKE SERVICES LTD

2) Guidelines

2.1) Authorised Connections

Only connections that comply with the controls defined below are permitted to SRES networks:

- Non-SRES devices must be authorised by the IT Operations Manager (including DSL lines, dial-up modems and wireless access points)
- All connections through the Internet must comply with the IT Guideline - Internet Security document. No direct connections are permitted into the internal network.

2.2) Network Management

Network devices must be appropriately managed to minimise the security risks to SRES information:

- Only authorised IT staff or designated service provider shall perform network management tasks (changing switch/router/firewall/server configurations, SNMP monitoring, network scanning and discovery)
- All remote network management will use encrypted connections (e.g. ssh, https). Telnet is not permitted
- Where possible, users will have unique user accounts for network administration. Where it is not possible, additional monitoring controls should be implemented
- All passwords must comply with the IT Guideline - User Administration.
- All network management processes must be documented
- All changes made to the network must comply with approved Change Management processes
- Network device logs will be reviewed on a timely basis to identify any unexpected or malicious activity. Where it is not technically feasible to review all logs other mechanisms of detecting malicious activity (intrusion detection) will be implemented
- All network configurations will be fully documented and electronic backups will be kept where feasible (e.g. firewall rule base)
- Network diagrams will exist that show both the physical and logical layout of the internal network
- Contingency plans will be documented for the failure of network devices and will be tested on a timely basis

PROACTIVELY RELEASED BY SOUTHERN RESPONSE EARTHQUAKE SERVICES LTD

2.3) Server Security

The following controls will be applied for all servers in the SRES environment:

- All servers will be “hardened” before being placed in production environments, in line with defined server hardening standards and the principle of least privilege
- Any service banners or other information that may reveal information relating to the internal working of the server will be removed whenever feasible
- All access must be authorised by the business owner or approved delegate
- Access to information will be granted on a role or group basis rather than to individuals
- Only authorised IT staff will be permitted to modify system configurations and access system files
- User access to applications must not allow them to gain access to the command prompt or perform administrative operating system commands
- Servers will be patched in line with agreed service provider patching processes

3) Guideline Breach

Failure to conform to this guideline may constitute misconduct. Persistent breaches of these guidelines 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 guidelines could result in serious consequences such as summary dismissal. It is therefore important that you read and understand these guidelines.

PROACTIVELY RELEASED BY
SOUTHERN RESPONSE EARTHQUAKE SERVICES LTD