Southern Response
6 Show Place
Christchurch, New Zealand

IT Guideline - Remote Access

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

The purpose of this guideline document is to define standards for connecting to Southern Response's (SRES) internal network from any host. These standards are designed to minimise the potential exposure to SRES from damages which may result from unauthorised use of SRES resources. Damages include the loss of sensitive or organisational confidential data, intellectual property, damage to public image, damage to critical SRES internal systems, etc. This policy also sets out the roles and responsibilities of remote access users and administrators and applies to all parties remotely accessing or administering SRES information resources.

1.2) Scope

This document applies to all SRES employees, contractors, vendors and agents remotely connecting to the SRES network. This document applies to remote access connections used to do work on behalf of SRES, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this document include, but are not limited to, internet VPN, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

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) General

- It is the responsibility of SRES employees, contractors, vendors and agents with remote access privileges to SRES's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SRES
- SRES must provide approval for all means of remotely accessing SRES information assets.
- All resources gaining remote access to SRES information assets must have an SRES approved personal firewall deployed if the access is to be obtained over the Internet (e.g. using VPN)
- Remote access will not be granted automatically. A valid business case with approval from an appropriate SRES employee (System Owner, IT Department Representative and/or employee's manager or third party's SRES contact) will be required before remote access is granted
- Only SRES resources can be used to access SRES information assets remotely. Where non SRES resources are required for access, a justifiable business case must exist and approval must be explicitly obtained from an appropriate SRES representative. Further, the requirements set out in the section titled "Use of Non SRES Resources" must be met
- Third parties requiring remote access to SRES resources for support purposes must have this access approved by an appropriate SRES representative. This access will be restricted on an 'as needed' basis and access will only be permitted for the time period that the support is required for, and only to those resources that require support. This access will be terminated as soon as the support activities are over
- Remote access will only be provided via a single point of entry
- Dial-up access (e.g. modem access) to SRES information assets is not permitted. If dial-in/dial-out access is required, then the access ports must be strictly controlled. All dial-out access requests must have a justifiable business case that has been approved by appropriate SRES representative and modems used for dial-out should be configured for "dial-out" only and must only be switched on when in use
- Remote access users must be educated on the risks surrounding the use of remote access technology. This will include signing a "User Guidelines" document that will outline the following:
    - Remote access systems will only be used for SRES business purposes and cannot be used to exploit SRES systems and services for personal gain
    - The need to protect logon information and the use of a personal firewall if connecting over the Internet
    - Places where it is appropriate to gain remote access to SRES resources which do not include public places such as airports and internet kiosks
    - All policies pertaining to SRES information assets must be followed when these assets are accessed remotely
    - Provision of contact details and phone numbers to be used both in and out of normal operating hours, to get help and to report any outages or security breaches

2.2) Use on Non SRES Resources

- All policies and security standards applicable to SRES computer equipment are applicable to non SRES computer equipment when used to access SRES information assets
- These requirements must be formally communicated to any party wishing to use non SRES computer equipment to gain access to SRES corporate resources. The acceptance of these requirements must be formally recorded as signoff from the party and maintained for future reference. Adherence to these requirements must be formally reconfirmed on an annual basis
- When non SRES computer equipment is used to access SRES information assets, approval has to be obtained from an appropriate SRES representative and the following requirements must be met:
  - All SRES specific data introduced to the non SRES computer equipment must be removed once use of this data has lapsed
  - A robust, SRES approved, personal firewall must be used
  - Virus control measures meeting SRES standards must exist on the non SRES computer equipment
  - Any data introduced to SRES systems via non SRES computer equipment must be appropriately scanned at the non SRES computer equipment and on the SRES system for viruses
  - The non SRES computer equipment is also subject to SRES's media disposal procedures. These are to be applied to the non SRES computer equipment at the termination of the user's employment or contractual arrangement, or in the event that their computer (or any storage media) is to be disposed of
- Written confirmation must be obtained from the user that all SRES information has been removed from the non SRES computer on the termination of a user's employment or contractual arrangement
- Business Partners can be permitted access to SRES information resources using their equipment, only when SRES has obtained confirmation that Business Partner systems are secure and will not present a security or virus risk to SRES information assets

2.3) Requirements

- Secure remote access must be strictly controlled. No unauthenticated remote access is to be permitted. All remote access over the Internet is to be controlled using at least two factor authentication. Further, all remote access to sensitive or confidential information is to be controlled via two factor authentication.
- At no time should any SRES employee provide their login or email password to anyone, not even family members.
- SRES employees and contractors with remote access privileges must ensure that the personal computer or workstation, which is remotely connected to SRES's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user
- SRES employees and contractors with remote access privileges to SRES's corporate network must not use non SRES email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SRES business, thereby ensuring that official business is never confused with personal business
- Routers for dedicated ISDN lines configured for access to the SRES network must meet minimum authentication requirements of CHAP
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time
- Frame Relay must meet SRES minimum authentication requirements
- Non-standard hardware configurations used to access SRES information assets, and their security configurations, must be approved by SRES
- All hosts that are connected to SRES internal networks via remote access technologies must use the most up-to-date anti-virus software. Third party connections must comply with these requirements as well
- Personal equipment that is used to connect to SRES's networks must meet the requirements of SRES owned equipment for remote access.
- Organisations or individuals who wish to implement non-standard Remote Access solutions to the SRES production network must obtain prior approval from SRES
- 128 bit encryption using a robust encryption mechanism is required for any remote access over a publicly accessible network
- The following user account controls are to be implemented on accounts used to remotely access SRES corporate resources:
    - Idle connections are to be disconnected after five minutes of inactivity
    - User accounts are to be locked out after 3 invalid logon attempts. The accounts are only to be re-activated by an administrator or the Helpdesk after the identity of the requester has been confirmed

2.4) Auditing

- The list of users with remote access should be verified every 6 months. System owners to be provided with a list of users with remote access to their systems who should then verify and approve this list
- Appropriate Intrusion Detection Systems should be in place over remote access solutions
- Adherence to this standard must be independently verified at least annually
- “War-dialing” and other techniques may be performed at least every six months to identify and remove any rogue dial-up access points into the SRES network
- All successful and unsuccessful remote access attempts into the SRES network should be logged. All unsuccessful access attempts must be reviewed weekly to identify any attempts to hack into the SRES network

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.