Southern Response
6 Show Place
Christchurch, New Zealand

IT Guideline - Internet 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	

Table of Contents

Document control 2
Table of Contents 3
1) Introduction 4
1.1) Statement of Intent 4
1.2) Scope 4
1.3) Review 4
1.4) Relevant References and Resources 4
2) Guidelines 5
2.1) Inbound Connections 5
2.2) Outbound Connections 6
2.3) General Controls 6
3) Guideline Breach 7

1) Introduction

1.1) Statement of Intent

The Internet is a global network of computers connecting organisations and individuals. The Internet allows access to and sharing of information.

For the purposes of this document Internet use is defined as any connection that utilises the Internet Protocol, including HTTP, HTTPS, FTP, peer-to-peer (P2P) file sharing, instant messaging and streaming media.

1.2) Scope

This guideline document applies to all inbound and outbound Internet connections that involve SRES's systems (including SRES-owned laptops and portable devices).

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 - Network Security
- IT Guideline - Remote Access

2) Guidelines

2.1) Inbound Connections

Connections using the Internet to SRES systems must comply with the following rules:

- All externally accessible Internet services or applications should reside in a de-militarised Zone (DMZ) segregated from SRES's internal systems by a firewall, unless specifically excluded by IT MANAGER
- All traffic into and out of DMZs shall be filtered by the use of a gateway firewall that compiles with controls as defined in the IT Guideline - Network Security
- Connections shall not be established from the Internet into SRES's internal network, unless they comply with the SRES IT Guideline - Remote Access
- Connections established from the Internet to a DMZ, or between DMZs, or between a DMZ and the internal network, shall only be permitted on the ports/protocols required for the application to function
- The principle of "least privilege" shall be applied to all Internet facing systems. Servers shall only run the services and software necessary to provide the required business functionality, and shall be hardened as per the Network Security Policy, shall be formally documented and utilised
- Any service banners or other information that may reveal information relating to the internal working of an Internet facing device (e.g. a make or version number) will be removed whenever feasible
- Any information transmitted to or from an externally accessible Internet system which may be of a sensitive or confidential nature shall have sufficient controls applied to prevent the interception or modification of the information as it travels across the Internet. This should include encryption, digital signing of information and/or other validation controls
- All externally accessible Internet systems shall not be remotely administered (either at an application level, middleware level or operating system level) from the Internet unless the administration mechanism has been approved by the IT MANAGER
- All SRES equipment accessed from the Internet must have appropriate antivirus, spyware, adware and other malware protection
- Incoming content will be automatically scanned for viruses and other prohibited content and all prohibited content detected will be blocked

2.2) Outbound Connections

Connections from SRES systems to the Internet must comply with the following rules:
CONNECTIONS:

- Internet access will be provided to all SRES staff with network accounts.
  - This is necessary for access to business systems, including EMS, Aconex, iViis, Elvis, Mercury and Southsite.
- Extended outbound internet access will be granted to users who require access as part of their job function. All access must be approved by IT MANAGER and staff member's manager on submission of a Helpdesk request.
- Sufficient content filtering and logging shall be applied on all outbound Internet access to ensure that:
  - SRES's Internet facilities are only used only for business purposes, or limited personal purposes (as defined by IT Guideline - Acceptable Use)
  - SRES's computer resources are not utilised for any illegal or unethical purposes
  - Excessive bandwidth costs are not incurred through users' downloading bandwidth intensive non-business related files (such as streaming video and audio, pirated movies, pirated music)
  - SRES's systems are not placed at undue risk due to the introduction of trojans, viruses or worms from the Internet
  - Unapproved Internet applications and services are not relayed via approved applications and services
  - Where SRES devices are to access the Internet directly, an appropriate personal firewall must be installed
- The nature of all content filtering is to be approved by the IT MANAGER
- All users shall be made aware that their Internet activities may be monitored or restricted
- Any information transmitted to or from the Internet which may be of a sensitive or confidential nature (to either SRES, SRES's customers, or SRES's suppliers), shall have sufficient controls applied to prevent the interception or alteration of the information as it travels across the Internet
- All client and server software used for accessing the Internet or which is accessed from the Internet (for example, web browser software or web server software), shall be regularly updated to include the latest fixes for security vulnerabilities.

2.3) General Controls

The following controls will be implemented by the IT team to ensure that Internet usage does not adversely affect information security:

- Firewalls must be dedicated devices that perform no other purpose (with the exception of terminating VPN tunnels). Server based firewalls must be adequately hardened, and all firewalls must always be fully patched
- Firewalls must default to deny all traffic. Only required ports and protocols will be permitted and only to the specific addresses required. This applies to both incoming and outgoing traffic.
- All firewall rules will be commented to justify the requirement for the rule
- Network diagrams will exist that show all physical and logical WAN (wide area network) connections
- Firewall logging will be enabled for all successful and unsuccessful access, to ensure malicious activities can be identified and attacks can be investigated if required
- Incoming file attachments will be automatically scanned for viruses and other prohibited content and all prohibited content detected will be blocked
- All client and server software used for accessing the Internet, or that is accessed from the Internet (for example, web browser software or web server software), shall be

continually updated to include the latest fixes for security vulnerabilities, in line with the SRES patch management policy

- Formal procedures shall be implemented to ensure that all appropriate software patches, hot fixes, updates and service packs are implemented as soon as possible after their release.
- Software patches, hot fixes, updates and service packs will be tested in a test environment for compatibility with other SRES technology, and will go through the normal change control processes
- All users shall be regularly educated on the risks associated with using the Internet, and what constitutes acceptable and unacceptable use of the Internet.
- Contingency plans will be documented for the failure of Internet facing devices/connections and will be tested on a timely basis
- All externally accessible Internet applications or systems will be subject to independent security testing prior to the application's release and on an annual basis subsequently. This shall include, but is not limited to, any web site, mail server application, file transfer application or remote access facility, no matter what the purpose of the application or system is. SRES shall ensure testing is undertaken as appropriate, and that any deficiencies identified during the testing are appropriately addressed before the application is released.

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.