Southern Response
6 Show Place
Christchurch, New Zealand

IT Guideline - Email 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

1) Introduction

1.1) Statement of Intent

Electronic mail (E-mail) allows quick and convenient information transfers, both internally and externally, between Southern Response (SRES), business partners and the community.

E-mail's ease of use makes it susceptible to accidental and malicious misuse. The objective of this policy is to ensure appropriate email usage that does not compromise SRES's information security or legal requirements, and enables the achievement of SRES's organisational objectives.

1.2) Scope

This guideline document applies to all employees and non-employees that use SRES's email systems to send and receive electronic mail.

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
- Code of Conduct
- IT Standard – Acceptable Use

2) Guidelines

2.1) User Responsibility

Emails must be treated in the same way as any other written communications and must be professional both in content and tone. Email users must comply with the following requirements:

- Emails must be checked at least daily and there should be prompt acknowledgement of all email requests
- Always review the address line before sending a message to ensure that you are sending it to the right person/people
- Keep all emails short and to the point
- Copy only to people that need to know. Keep the message concise, use a meaningful subject line and list all required actions clearly

2.2) Acceptable Use

The following uses of email are considered acceptable and are permitted:

- Emails sent and received in the performance of job responsibilities and do not constitute prohibited use as defined below
- Personal emails that do not affect the performance of job responsibilities and do not constitute prohibited use as defined below

2.3) Prohibited Use

The following uses of email are strictly prohibited and may result in disciplinary actions as outlined within the Code of Conduct:

- Personal use that affects the performance of job responsibilities
- Transmission of information classified as SENSITIVE (confidentiality), MEDIUM (integrity) or PRIORITY (availability) or above without the approval of the business owner. Information classified as RESTRICTED or above must be only be transmitted using a secure encryption mechanism as approved by the IT MANAGER
- Sending of unsolicited bulk email (SPAM) and chain letters
- Sending or receiving of information (text and graphics) which may be construed as offensive or obscene
- Sending or receiving of information that is illegal (including breach of copyright)
- Disclosure of confidential information without approval of the business owner
- Release of information to the media without appropriate approval
- Sending or receiving of executable files (exe, bat) and scripts (vbs, pl, etc) that are not approved by the IT HELPDESK
- Wilful or neglectful distribution of viruses

2.4) IT Team Responsibility

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

- Users will be granted unique email addresses, unless there is a valid business requirement to share an address. Where an address is shared, specific procedures will be developed for access to and use of the address
- Incoming emails and file attachments will be automatically scanned for viruses and other prohibited content. Where prohibited content is detected the email may be quarantined for further investigation or immediately deleted
- Virus signatures and SPAM filters will be updated as soon as new files are available
- Content management rules (e.g. allowed file attachment types, blocked words) will be developed, applied and reviewed on a 6 monthly basis
- All emails stored on the mail server will be backed up daily
- All inbound and outbound emails are archived for discovery purposes.
- Data Loss Prevention (DLP) tools are deployed to prevent staff from accidentally or maliciously sending content via email that may breach privacy or security guidelines
- Staff will be provided with advice and other guidance as needed to support good practice through company meetings, email or Southsite.

3) Breach of Policy

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 policies could result in serious consequences such as summary dismissal. It is therefore important that you read and understand these guidelines.