Use of Information Resources and Security Policy

Contents

Policy Owner and Approval	▪ The Owner of this policy is the IT Manager. ▪ This Policy has been approved by the Chief Executive Officer. ▪ The Committee responsible is the Audit, Risk and Compliance Committee.
Review Date	February 2017
Effective Date	5 April 2012

Introduction

Purpose and Scope

Southern Response provides IT Resources to enable Users to carry out their work for Southern Response, and allows limited use which is not work related.

This policy defines what Southern Response considers appropriate use of IT Resources.

This policy applies to all personnel of, and independent contractors to, Southern Response and board members, business partners and official visitors who may operate or access Southern Response's IT Resources ('Users'), irrespective of their location.

Definitions

Definitions relating to the Policy can be found at Appendix 1.

General Principles

Responsibility of Users

Users of Information Resources must:

- use them in an efficient, trustworthy and responsible manner;
- read this policy and understand what is required to comply with this policy, any other applicable Southern Response policy,) and the general law;
- ensure that usage of Information Resources is conducted with appropriate confidentiality and discretion;
- ensure that they only use the Information Resources that they are authorised to use;
- report any breach of this policy that comes to their attention to their manager;
- speak to their manager if they are in any way unsure about any aspect of this policy or its implementation.

Company Responsibilities

Southern Response:

- may vary this policy from time to time at their discretion and will advise Users of such changes;
- will monitor the use of all Information Resources and systems. This includes, but is not limited to, use of internet, email and telephones and all other communications made through the use of Information Resources;
- have full right of access to all information on or within, or transmitted to, its Information Resources and systems (Users have no expectation of privacy when using Information Resources);
- will co-operate with any authority or, at its discretion any third party, in the investigation of any allegation, offence or civil wrong;
- may restrict or extend access to Information Resources at their discretion.

If inappropriate or inconsistent activity is identified, the nature and conditions of the breach will be reviewed with the other party and an appropriate course of action will be agreed.

Breaches of this policy

A breach of this policy may result in a discontinuation of privileges in respect of some or all Information Resources. It may result in disciplinary action being taken, up to and including dismissal without notice or termination of a contract (as applicable).

General Conditions of Use

Personal Use

Users must use Information Resources principally for authorised work-related purposes.

Personal use is permissible on a limited basis, provided that Users adhere to the terms of this policy. Non-work related activity should be during authorised breaks only and, generally, should be limited to no more than three hours each week.

Reasonable personal use must not interfere with a User's duties or obligations and must not be contrary to Southern Response's interests.

Personal Telephone Calls and Text Messages

Personal telephone calls and texts are permitted but must be kept brief and made or received at work only when absolutely necessary. Where personal toll calls or calls to mobile phones are made, or where a personal facsimile is sent, costs are to be reimbursed to Southern Response.

Illegal or Undesirable Purposes

Information Resources must not be used for illegal or undesirable purposes. Users must not transmit or store inappropriate material which may include, but is not limited to, material that could be interpreted as pornography, lewd jokes, any form of harassment, defamatory comment or chain letters/emails/correspondence.

Breaches of Law

Users must not breach any patent, copyright, law, Southern Response operating protocol or Southern Response policy in respect to their usage of Information Resources.

Intentional access of technology such as computer systems without authorisation is a crime in New Zealand.

Confidentiality Obligations

All Users should be aware of the confidentiality obligations in their employment agreements / contracts and nothing in this policy should be read as reducing or setting aside these obligations.

Southern Response recognises User rights, as private citizens, to communicate with the media and connect socially on the Internet about matters outside of their work. This policy is not designed to infringe upon those rights rather to confirm obligations as they relate to Southern Response and its business.

There is potential for behaviour outside of work to impinge on Southern Response's reputation or to cause it some form of commercial harm, or impact on the proper discharge of duties. Accordingly, Users are not to reveal information about Southern Response, its activities or their role within Southern Response, on any internet-based forum i.e. Facebook, Twitter, blog sites etc. without the express approval of the Chief Executive Officer. Nor should any User post confidential or proprietary information relating to Southern Response's operations on the Internet.

Intellectual Property

Some intellectual property of material produced on Southern Response's computer resources is the subject of a written agreement and deed between AMI/IAG and Southern Response.

That agreement and deed sets out the ownership and use of relevant information created and held on AMI/IAG's systems. The provisions of this agreement will be advised to Users as applicable.

Passwords and PINs

Users are responsible for anything that occurs under their Logon and must not share their PIN or password with anyone (unless required by Information Technology department), nor allow it to be readily accessed. Users must not print any password or PIN or write down any password or PIN in a place where others may find it, or allow their password or PIN to be used by others.

Guidelines and Standards relating to account management and security are available to all staff on the company intranet (Southsite).

- IT Acceptable Use Guideline

Viruses

Southern Response will install and maintain up-to-date protection against invasive attacks by viruses, worms, Trojans and other malicious software vehicles, reasonably to protect against infection through Southern Response systems.

Users must take reasonable steps to ensure that Information Resources are not corrupted through computer viruses or physically damaged in any other manner.

System Specific Protocols

AMIGO Files

Users must not alter or copy AMIGO data or files that are not directly related to legitimate Southern Response activity pertaining to earthquake claims processing.

Having access to a file in AMIGO does not grant Users authority to copy or alter it.

Updating of data should only reflect actual activity executed by Users in respect of correctly authorised actions for claims.

Users must not:

- update policy or customer data in AMIGO; or
- change the location of a file in AMIGO.

Data Warehouse Files

Users will not have direct access to the AMI/IAG Data Warehouse .

Any data required to be received by Southern Response from the Data Warehouse will be delivered through standard Current Reports and ad hoc reports referred to in the CMSSA.

Installation and Deletion of Software

Users should not install any software or applications into, or remove any software or applications from, the Southern Response environment.

If Users require additional or changed software to be made available in the Southern Response environment, or any third party application supported or maintained by Southern Response (including but not limited to EMS, iViis, AMIGO, Aconex, Great Plains, Southsite), they are required to prepare and submit a request through the IT department for consideration and approval (or not), as a formal change.

Copyright

Users will be required to observe and respect the provisions of copyright legislation, in respect of any or all software applications and information resources to which they have been granted access.

Software Defects

All software failures and defects for services being provided to Southern Response internally or through third party providers must be reported to the IT Helpdesk.

Connection to Southern Response

Only hardware that is provided and supported by Southern Response's duly appointed and authorised managed service provider will be permitted to connect to the Southern Response network.

Connection to AMI/IAG

Only hardware that is provided and supported by Southern Response IT or their duly appointed and authorised managed service provider will be permitted to connect to the AMI/IAG network.

Remote Access

Users who have been authorised to access the Southern Response network remotely will use secure Virtual Private Network (VPN) connections.

Authorised AMIGO users may access the AMIGO system from the Southern Response network or through a VPN connection..

All Southern Response access, whether via the network or remote VPN, will be subject to this policy.

Internet and Intranet

Southern Response will maintain internet and intranet environments that will be accessible to all staff.

Relevant Links

Procedures and Policies

- 17. External Communications;
- 19. Solving Employment Problems.

Relevant References and Resources

- Unsolicited Electronic Messages Act 2007
- Film, Video and Publication Classification Act 1993
- Copyright Act 1994 and its amendments
- Defamation Act 1992
- Human Rights Act 1993
- Privacy Act 1993
- Southern Response IT Standards (available to all staff on Southsite)
  - IT Acceptable Use
  - Network Security
  - Internet Security
  - Email Security
  - User Administration
  - Workstation
  - Wireless
  - Virus Protection

Appendix 1 – Definitions

Information Resources	Information Resources include (but are not limited to): ▪ Southern Response's information technology and equipment, including its computer network, laptops, mobiles phones, the internet and associated services/resources (including email) and all associated equipment and software; and ▪ Southern Responses designated service and support providers and resources, including Spark Digital, Olympic Software, iViis, Aconex and AMI/IAG.
AMI/IAG	AMI, formerly AMI Insurance Ltd. which will retain the AMI name, and is owned by IAG (NZ) Holdings Limited post separation from Southern Response Earthquake Services Limited.
Users	All personnel of, and independent contractors to, Southern Response, board members, business partners and official visitors who may operate or access Southern Response's Information Resources.
CMSSA	Claims Management Services Support Agreement outlines the resources and services AMI/IAG agrees to provide to Southern Response.
Personnel	Applies to all employees and other personnel providing services to Southern Response (e.g. independent contractors), together defined as "Southern Response Personnel".

Appendix 2 - Statement of Understanding

Employee Signature

- I have read the Use of Information Resources and Security Policy and understand what is required to comply with it.
- I understand that AMI/IAG and Southern Response may vary this policy from time to time at their discretion and will advise Users of such change.
- I understand that should any breach of the policy by someone else arise, this does not absolve me from my obligations and does not provide a justification for a breach on my part.
-

Signed:	Date:
Name: *Please print*	

Version Control

Version	Date	Author	Description
1.00	30 March 2012	[redacted]	Policy Created
1.1	14/05/2012	P Rose	Review
2.0	8 May 2015	[redacted]	Scheduled review and update
2.1	27/05.2015	P Rose	CE approved