Southern Response
6 Show Place
Christchurch, New Zealand

IT Standard - Acceptable Use

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 0.4	27-05-2014	
Review	[redacted]	Draft 0.5	8-05-2015	

Table of Contents

1) Introduction

1.1) Statement of Intent

The purpose of this Standard is to outline the acceptable use of computer equipment at Southern Response.

These rules are in place to protect the employee and Southern Response. Inappropriate use exposes Southern Response to risks including virus attacks, compromise of network systems and services, and legal issues. This document applies to employees, contractors, consultants, temporaries, and other workers at Southern Response, including all personnel affiliated with third parties.

The overriding goal of this document is to protect Southern Response's technology-based resources (such as corporate data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to Southern Response's public image.

1.2) Scope

This document applies to all equipment that is owned or leased by Southern Response on all equipment used for Southern Response business by affiliated or contracted third parties. It also applies to any sub-contractor or supplier an affiliate or third party might engage on Southern Response business unless otherwise agreed directly with Southern Response

This document applies to all Southern Response employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize mobile computers to access the organisation's data and networks via wireless means. Access to enterprise network resources is a privilege, not a right. Consequently, employment at Southern Response does not automatically guarantee the granting of access privileges.

This document is complementary to any previously implemented standards or policies dealing specifically with network access and remote access to the enterprise network.

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 Guideline - User Administration
- IT Guideline - Remote Access
- IT Guideline - Network Security
- IT Guideline - Internet Security
- IT Guideline - Email Security
- IT Guideline - Workstation
- IT Guideline - Wireless
- IT Guideline - Virus Protection

2) Standards

2.1) Overview

Southern Response's intentions for publishing IT Acceptable Use Standards are not to impose restrictions that are contrary to Southern Response established culture of openness, trust and integrity. Southern Response is committed to protecting Southern Response's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly on internet, intranet, or extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Southern Response. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Southern Response employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these standards, and to conduct their activities accordingly.

2.2) Introduction to information security

What is information security?

Information is a business asset and as with any other asset, it needs to be protected from misuse, theft and damage. Information security is concerned with the protection of information assets i.e. to ensure they are only accessible to the right people (confidentiality), that they are complete and accurate (integrity) and that they are available when required (availability).

Why is information security important to me?

As defined above, information is a business asset. Unless it is properly protected Southern Response risks lost revenues, increased expenses and damage to reputation, all of which affect the overall profitability of the business.

What are my responsibilities?

Information security is the responsibility of all users and everyone must understand and comply with the policies and procedures outlined within this document. Non-compliance will be treated as misconduct and may result in disciplinary action, including dismissal, through Southern Response Human Resources processes.

Additionally, you may have specific information security responsibilities outlined within your job description, or given to you by your manager. In this case you must consult with the IT Manager to identify other policies, procedures and standards that apply to you.

2.3) General Use and Ownership

- While Southern Response's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Southern Response. Because of the need to protect Southern

Response's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Southern Response.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating standards concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- Southern Response recommends that any information that users consider sensitive or vulnerable be encrypted. For standards on information classification, see the Information Security Policy.
- For security and network maintenance purposes, authorised individuals within Southern Response may monitor equipment, systems and network traffic at any time.
- Southern Response reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4) Security organisation

Within Southern Response, information security is managed by IT Manager. The user contact for any queries relating to this is through the IT Helpdesk, or directly to the IT Manager and/or Human Resources Manager if sensitive information is involved. They will answer any questions or queries regarding information security and should be consulted if any policies, procedures or standards are not fully understood.

2.5) User awareness and education

User awareness and education is an important part of information security. All users are required to participate in information security training as part of the induction process and as part of the ongoing user awareness and education programme.

It is your responsibility to ensure you understand information security policies and procedures. Where information provided is unclear it is expected that you will seek help from IT Helpdesk. In instances where external security advice or training is required, this will be organised and approved by the IT Helpdesk.

As part of the ongoing commitment to information security, you will be asked to confirm understanding of your information security responsibilities and agree to abide by the policies and procedures within this document on an annual basis.

2.6) Data classification and handling

To ensure appropriate controls are implemented, information and information systems must be given risk classifications. Users who are responsible for the creation of information must be familiar with this section of the standard and are responsible for ensuring that information is assigned a classification and appropriately labelled. All users must be aware of the commonly used classifications detailed below:

- Public – the information can be disclosed to the public, copied and distributed freely. Examples of public information are press releases and job adverts.
- Internal Use Only – the information can only be disclosed to non-Southern Response employees after a non-disclosure agreement has been signed. The information should not be freely distributed and can only be copied when there is a valid business need. Such information includes employee's calendars, phone directories and office communications.
- Confidential – access to the information is on a "need-to-know" basis and must be approved by the business owner of the information. This is information that you would

not want to be known by competitors, customers, the media or other employees. The information should:

- Not be copied or distributed without the permission of the owner
- Not be left unattended (e.g. on a desk or printer)
- Not be discussed with, or in the vicinity of, people without authorisation to know the information
- Only be sent using secure methods (prearranged faxes to non-shared numbers, encrypted emails, recorded delivery mail or courier). Email encryption software is available on request from the XXX
- Be locked away when not in use
- Be clearly labelled as Confidential
- Be securely destroyed when no longer required. Secure disposal bins are located in all offices for paper and removable media. All hardware disposals must be coordinated through the IT Helpdesk.

In instances where information is not clearly labelled, it is the user's responsibility to determine the appropriate classification by consulting the owner of the information before disclosing, copying or distributing the data.

Removable media including CDs, floppy disks and USB memory sticks (and other removable storage devices) are especially susceptible to loss or theft. As such it is especially important to ensure information held on removable media is classified and handled appropriately. Encryption mechanisms are available for all types of removable media and if required can be provided by the IT Helpdesk.

Data removal or destruction must conform to the appropriate rules for the label given and in accordance with the information retention cycles required by Southern Response. If you are unsure ask IT Manager.

2.7) Communications and operational security

Account and password security

Usernames and passwords should not be written down or disclosed to any person at any time, including senior management and IT staff. The following standards are provided to show some do's and don'ts to make easily remembered secure passwords:

- Don't use single words for your passwords, instead use a combination of words e.g. "thefatcat", or letters taken from a phrase e.g. "To be the best you have to work the hardest" = "2btbuh2wth"
- Do use a combination of upper and lower case and numbers e.g. rather than using "thefatcat", use "Th2F5tC5t", where the first letter of every word is capitalised, and e=2,a=5
- Don't cycle through passwords using numbers as the first or last character e.g. 1Southern Response, 2Southern Response. The reason why this is not a good idea is automated password guessing programs try this type of password. It is better to cycle through password if the number is in the middle of the password e.g. Eco1ab, Eco2ab. Better still; don't cycle through passwords at all!
- Do use special characters as well as numbers, lower and upper case letters including !@#$%^&*(){}<>
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed monthly; user level passwords should be changed every 2 months.
- DO NOT USE any of the above examples!

Operational policies

You are required to follow all operational policies, procedures and standards that are applicable. Your manager will communicate relevant policies, procedures and standards to you.

Security incidents

If there is an information security incident or suspected incident the IT Helpdesk or IT & Data Manager must be notified immediately. Security incidents include loss or theft of paper-based information, removable media (e.g. floppy disk, CD-Rom) or computer hardware, unauthorised disclosure, access, or modification of data and infection with computer viruses.

If you suspect that your computer is infected with a virus or has been accessed by a malicious user you should:

- Immediately remove the network cable from your computer
- Leave your computer as is - do not attempt to fix the problem yourself
- Contact the IT Helpdesk.

For software malfunctions and system errors that may occur:

- Any errors and screen output should be recorded
- Use of the computer should be stopped immediately
- The network cable should be removed from the computer
- The IT Helpdesk should be contacted.

Modification of software and hardware configurations

Users are not permitted to modify software of hardware configurations without the approval of the IT Manager. This includes:

- changing operating systems settings
- changing application settings
- installing or removing software, including applications downloaded from the Internet
- disabling virus protection
- adding or removing users
- changing user privileges
- adding, removing or modifying computer hardware

Software purchases

All software purchases must be reported to the IT & Data Manager.

System development

Any development or modification of information systems must be approved by the IT Manager, including use of wireless networks. This ensures that appropriate information security controls are included within the systems.

Use of contractors and third parties

If you engage contractors or other third parties their access to Southern Response information must be approved by the IT Manager.

Use of personal computing devices (BYOD)

The use of personal computing devices (Laptops, PDAs, Home PCs) to access the Southern Response network or store Southern Response information is not permitted without the approval of the IT Manager.

Information backups

It is important that any information required in the future is appropriately backed up. Information stored on servers, including your personal drive, is backed up daily by the IT department. Users are responsible for ensuring the following information is backed up:

- Information stored on your local hard disk – you should only store information on your local hard disk if you are working at a remote location without network connectivity. This information should be moved to your home drive when your network connection has been restored.
- Information stored on PDAs and other mobile devices – if you are using a mobile device to store information that requires to be backed up, you must consult with the IT & Data Manager to identify an appropriate process. You must not synchronise mobile devices without the prior approval of the IT & Data Manager.
- Paper-based information – any information used must be backed up appropriately.

Exchange of information

Any information exchanged between Southern Response and third-parties should be conducted in a secure manner:

- All information must have an identified data classification before being distributed to another party (this should have been assigned by the business owner
- It is the responsibility of the sender to ensure appropriate controls are applied to information sent, based in the data classification
- When confidential information is sent the sender must confirm the information has been received by the intended recipient
- If a regular information exchange is required the IT Manager should be notified, both to ensure the exchange is secure, and to investigate automating the process.

2.8) Security and Proprietary Information

- The user interface for information contained on internet, intranet, or extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality standards, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorised access to this information.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less, or by logging-off (control-alt-delete) when the host will be unattended.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Southern Response email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Southern Response, unless posting is in the course of business duties.
- All host devices used by the employee that are connected to the Southern Response internet, intranet or extranet, whether owned by the employee or Southern Response, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

2.9) Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Southern Response authorised to engage in any activity that is illegal under local, state, federal or international law while utilizing Southern Response-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

If you are unsure please check with your immediate manager or supervisor.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Southern Response.
- Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Southern Response or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Southern Response computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Southern Response account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to IT Manager is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Southern Response employees to parties outside Southern Response.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Southern Response's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Southern Response or connected via Southern Response's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Uploading or sharing of company information in blogs, chat rooms or social networks such as Facebook etc without express permission of Southern Response IT Manager
- Representing individual views as though they are Southern Response views on blogs, chat rooms or social networks such as Facebook, etc without express permission of Southern Response IT Manager.

2.10) Internet Acceptable Use

- The company's IT resources should not be used to attack or interfere with any other computer or network
- Only represent yourself as who you are on the Internet
- The Internet should not be used to transmit confidential, political, obscene, threatening, or harassing materials
- Software should not be downloaded from the Internet and installed on the company's PCs. If you absolutely need to do so, please clarify this with IT.
- Material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity should not be downloaded. Accessing any source or destination addresses that may involve such material is strictly prohibited. Many source or destination addresses that contain such material have been blocked using a web content filter and procedures have been implemented to automatically notify IT of anyone trying to access such addresses.
- Non-work related material should not be downloaded from the Internet. Approval in writing should be requested form your Manager if you need to do this
- FTP downloads have been disabled and will only be permitted after appropriate authorisation has been provided
- Legal protection provided by copyright and licenses to data and software should be respected
- Ensure that the information you a accessing is valid, complete, accurate and current
- Keep your personal Internet use to a minimum
- Access to social media (such as Facebook, Twitter etc) has been blocked, with the exception of approved staff who require access for business purposes. Requests for access should be made to the IT & Data Manager.
- Access to web based email (such as Hotmail, Yahoo mail, etc.) may be blocked. Access to web based email can create vulnerabilities that lead to risk in our internal network from virus threats
- Streaming media (video or radio broadcasts), Skype, and Instant Messaging (web chat) may be blocked, and access will not be allowed to prevent our Internet services being slowed down by unwanted traffic

2.11) Physical security

All non-public information should be physically secured at all times. If strangers are seen without a temporary access card or visitor badge their presence should be investigated immediately.

2.12) Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment in accordance with Southern Response Human Resources policies in force at the time.

The Southern Response reserves the right to audit individual usage of equipment and service provided by the Southern Response in accordance with Southern Response Human Resources policy and local, regional or national legal standards.

3) Guideline Breach

Failure to conform to this standard may constitute misconduct. Persistent breaches of these standards may constitute serious misconduct. The procedure for dealing with cases of misconduct, as outlined in the Southern Response'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 standards could result in serious consequences such as summary dismissal. It is therefore important that you read and understand these standards.