IT Guideline - User Administration

Southern Response Earthquake Services Limited

Author: [redacted] (IT Manager)

Document control

Change Description	Author	Version	Date	Approved By
Initial Draft	[redacted]	Draft 0.1	21-04-2013	
Draft	[redacted]	Draft 0.3	27-05-2014	
Draft	[redacted]	Draft 0.4	8-05-2015	

Table of Contents

1) Introduction

1.1) Statement of Intent

This guideline document has been implemented to ensure that user administration is managed appropriately to maintain the security of electronic information.

1.2) Scope

This document applies to all IT systems and assets which provide for user-level security and access control but do not have a specific access control policy defined.

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) Granting User Access

The following controls will be implemented when granting access to SRES IT systems and information:

- Access will only be granted if there is a valid business reason for that access
- Access must not exceed that required to perform assigned business functions and must not compromise segregation of duties
- Written authorisation must be approved by the business owner (or approved delegate) of the information being accessed. Approval must be via NEW EMPLOYEE form or INTERNAL STAFF MOVE form from Southsite and will be recorded and kept for auditing purposes
- Any special conditions of use will be communicated and agreed to by users before access is granted. This must be signed off by users and will be recorded and kept for auditing purposes
- Unique IDs will be used for all access, including administrative accounts, unless the access meets the criteria for generic accounts as documented below
- The duration that access is required for will be specified on the NEW EMPLOYEE form or INTERNAL STAFF MOVE form from Southsite. All contractors and other users who require temporary access will have an account expiry set at the network level. Contractors must never be granted network access without an account expiry being set
- All temporary accounts are to be identified in the Description on the account ID
- New users will not be granted permissions that are the "same-as" existing users. All user access requests must specify the specific access required for the user, rather than modelling access on an existing users, as an existing user may have been granted additional rights that reflect the trust and responsibilities that have been earned throughout their employment
- New account passwords must be randomly generated, conform to all password complexity requirements and must be changed by the user on first login

2.2) Modifying User Access

The following controls will be implemented to ensure that access is modified appropriately:

- HR will notify all system administrators of any employee movements as they occur, to ensure access rights are modified accordingly
- Written authorisation must be approved by the business owner (or approved delegate) of the information being accessed. Approval must be via INTERNAL STAFF MOVE form from Southsite and will be recorded and kept for auditing purposes

2.3) Removing User Access

The following controls will be implemented to ensure that access is removed appropriately:

- When a user leaves the employment of SRES, all user accounts set up for their use are to be disabled immediately
- HR should notify all system administrators of any resignations two weeks prior to the employee leaving using the EMPLOYEE RESIGNATION form from Southsite. The IT MANAGER must be included in the employee leaving process to ensure all IT equipment is returned before the employee leaves

- HR will notify all system administrators of any dismissals before or at the same time as the employee is notified to ensure all access is removed immediately (as dismissed employees pose a greater risk to information security than those voluntarily leaving)

2.4) Reviewing User Access

The following controls will be implemented to ensure that access is reviewed in a timely manner:

- Business owners are responsible for reviewing access to their information in line with the specified access control policy. Where a specific access policy does not exist all access will be reviewed on an annual basis.
- The IT MANAGER is responsible for the generation of user access lists to be distributed to business owners in line with review timeframes
- The IT MANAGER is responsible for reviewing network access on a monthly basis to identify dormant user accounts (accounts that have not been used for over 90 days). Identified accounts will be immediately disabled and investigated to determine if they are still required

2.5) Privileged Accounts

The following controls will be implemented to ensure that the use of privileged accounts is appropriately controlled:

- Roles with privileged access rights will be identified and documented. Privileged access includes the ability to perform administrative tasks, modify the operation of an application, modify sensitive information, etc.
- Privileged access will be kept to a minimum. Where feasible, access should be granted on a temporary basis and revoked after use
- Where feasible, system routines will be used rather than granting privileged access to users
- Users, who are required to perform both privileged tasks and standard user operations, will be assigned separate accounts for privileged use and normal business use. This reduces the risk of accidental misuse of privilege when performing standard operations and of an attacker exploiting the privilege of the logged in account
- Formal procedures must be implemented to replace all passwords of an administrative nature for a particular system, or set of systems, in the event of a user with administrative access leaving the organisation
- Where it is not technically feasible to change on a regular basis (as outlined in the general password guidelines), this must be documented and approved by the IT manager. The maximum age for any passwords of this nature must not exceed one year, and the password must be of such a quality that it is not technically feasible to “crack” the password within the period employed
- Any password used for local administration accounts (or equivalent) on users’ desktop or laptop computers, must not be used for administrative purposes elsewhere within the network infrastructure, or for administrative access within SRES’s applications

2.6) Generic Accounts

The following controls will be implemented to ensure that the use of generic accounts is appropriately controlled:

- The use of a generic account must be specifically authorised by the appropriate Business Owner and the IT MANAGER. A register of all generic accounts will be maintained that documents the purpose of the account and mitigating security controls
- As accountability is reduced when generic accounts are used, appropriate reviews of activity conducted with generic accounts will be performed, on a timeframe as agreed by the business owner, to mitigate this

2.7) Password Security

Domain accounts

The level of controls required for passwords is dependent on the importance of the information that is being accessed. The following controls will be implemented for domain account passwords:

- Each user account must have a password, to be kept secret by the user, not written down or disclosed to another SRES employee or third party, including IT staff
- Passwords must be 'strong' and adhere to the following rules:
    - Must not be valid word or name
    - Must include at least one number and one uppercase letter, and special characters. This will be enforced through technical means by deploying minimum password length parameters and password complexity rules on systems
    - No less than 8 characters in length
    - Must not be the same as any of the 24 previous passwords
    - Must not consist of in whole or part an easy-to-remember or easily guessed number or string
- The following account lockout controls should be implemented:
    - Accounts are locked out after 5 invalid logon attempts
    - The system 'remembers' the failed logon count for an unlimited period of time
    - Once accounts have been locked out, they can only be unlocked by a systems administrator after they have appropriately verified the account holder's identity
- Passwords must be changed regularly, as enforced by the individual systems,
    - Active Directory user passwords to be changed at least every 42 days
- Users will not use cyclical passwords. For example, users will not add a numeric at the end of the password in sequence
- If a user is new, temporarily absent or unavailable, or if a password is forgotten, a temporary password may be assigned for one-off use, but it must be changed immediately after use
- Passwords must never be stored in clear text
- Passwords must never be transmitted across any network (both internal and external), unless encrypted in a robust manner
- A formal process must be defined for the resetting (or other similar changes) of user passwords. This process must sufficiently identify the user making the password change request, and confirm that the user has the appropriate authority to make the request
- All users must be regularly educated in a formal manner (through such means as the provision of user security awareness guidelines and security awareness training) on their responsibilities for password management.

The above controls should be used as a guideline when determining password security within other systems.

Other System Accounts

A number of systems accessed regularly by some of all SRES staff have specific security guidelines that vary from those set by the domain accounts

SRES managed systems:

- EMS
    - access guidelines are defined and managed by SRES IT
    - users are set up using Microsoft Office365 accounts.
    - Passwords are not currently required to be changed.
    - password complexity is applied (7 char minimum, mixture of lower case, upper case, numeric
- Southsite
    - Accounts and passwords are set by SRES reception
    - access guidelines are defined and managed by SRES IT
- Great Plains (Financial)
    - Users require two separate passwords to connect to Great Plains (GP)
    - Active Directory (AD) password to log on to network
    - GP password which is not linked to AD password
    - Users need to be domain connected to access GP, ie must be internal SR and AD authenticated
    - Only designated SR users have Great Plains icon installed on laptops. Other users do not have local admin rights to install icon
    - GP has the "enforce system password changes" setting applied.
- iViis
    - access guidelines are defined and managed by SRES IT
    - user accounts require
        - a minimum of 8 characters
        - 60 day change of password
        - Combination of alpha, numeric and non-alpha

External managed systems:

- PayGlobal (Payroll)
    - two separate passwords to connect to PayGlobal
    - Initial secure access to connect to PayGlobal portal, locked by IP address
    - Secondary usercode & password to log in to PayGlobal application
    - Minimum password size: 8
    - Expiry: after 28 days of non-use
    - Password change: annually
    - History: 2 passwords
- AMIGO
    - access guidelines are as defined and managed by AMI
    - Access is by device and pin
- ELVIS & MERCURY
    - access guidelines are defined and managed by Arrow International
- Aconex
    - access guidelines are defined and managed by Arrow

2.8) Two-factor Authentication

For systems where there are high security requirements such as to financial systems, username and password authentication may not provide sufficient comfort. In such cases, two-factor authentication will be used, where users are required to authenticate using something that they know (username/password) and something that they have (usually a smart-card, token or digital certificate).

Two factor authentication is applied for:

- Remote Access to SRES – domain login and RSA smart tokens (keyfobs).
- PayGlobal – as defined by PGOS, including subnet restrictions
- Great Plains – SR domain plus application level access and authentication

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.