Information Systems Access Control Policy

the SES GROUP

www.thesesgroup.co.uk

The SES Group is committed to the correct use and management of access controls throughout the company. Unmanaged access to information could lead to the unauthorised disclosure or theft of information, fraud and, in extreme, legal action. This policy is mandatory and sets out the correct use and management access controls for the SES Group.

Where possible all computer systems and infrastructure must be password protected.

Each computer system must have a designated information owner who is responsible for managing and controlling access to the system. The information owner must hold a position at director level and he/she must approve and sign all requests for access to the system. Alternatively the information owner may nominate a member(s) of their management team who will have the authority to sign and approve requests for access to the system on their behalf.

All computer systems must have a designated system administrator who is responsible for the day to day administration of the system including the creation and management of system access accounts for authorised users.

Access to computer systems and networks must be strictly controlled by a formal written registration and de-registration process.
Access to computer systems must be controlled by the use of individual user accounts. The use of generic or group access accounts to access computer systems is prohibited

Access to the network domain will generally be controlled by the use of individual user access account's, however the use of generic / group access accounts will be permitted

Access rights and privileges to computer systems and network domains will be allocated based on the specific requirement of a user's role rather than on their status

The criteria used for granting access privileges must be based on the principle of "least privilege" whereby authorised users will only be granted access to a computer system and network domain which are necessary for them to carry out the responsibilities of their role.
Care must be taken to ensure that access privileges granted to users do not unknowingly or unnecessarily undermine essential segregation of duties.

The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the computer system or network. Each administrator must have a specific admin level account, which is only used for system administrative purposes, and is kept separate from their standard user access account

All new requests for access to the computer systems must be made in writing using the Access Request Form

Line managers must complete the request on behalf of a new user and send it to the administrator for their approval and to create the new account.
New accounts will not be created unless a signed request form is completed

As soon as a user leaves the employment of the SES Group all his/her information systems and network access accounts must be revoked immediately. Line managers must request the deletion of a user's access accounts as soon as they have been informed by the user that they are leaving the employment of the SES Group. The request must be made in writing using the Remove Access Request Form and sent to the administrator for the request to be actioned.

Access to all information systems and networks must be controlled via strong password authentication schemes.

User access accounts must be created in such a way that the identity of each user can be established at all times during their usage. Each user access account must be unique and consist of at least a user name and password set. All passwords created must be in line with the requirement of the SES Group Password Policy

Where possible the computer systems must be configured to:

- Force users to change their password at their first logon.
- Automatically 'lock' a user account after a number of consecutive failed login attempts.
- Automatically 'lock' or log out user accounts after 30 minutes of inactivity. Where this is not possible, users must be instructed to manually log off or 'lock' their computer/device (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time and at the end of the each working day.

When available audit logging and reporting must be enabled on all computer systems.

The Information Security Manager is the person designated to take charge of the computer systems. Some of their responsibilities are delegated to an outsourced IT specialist who are the administrator and monitor for the day to day running of the computer systems.

The administrator is responsible for:

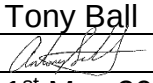
- Complying with the terms of this policy and all other relevant policies, procedures, regulations
- Taking appropriate and prompt action on receipt of requests for user registration, change of privileges, password resets and de-registration of users in accordance with this policy and the procedures for the computer system;
- Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy
- Ensuring all passwords generated for new user accounts and password resets meet the requirements of the Password Standards Policy
- Ensuring that appropriate records of system activity, including all authorized user registrations, change of privileges and de- registration are maintained and made available for review to the appropriate personnel
- Notifying the Information Security Manager, if they suspect a user is responsible for misusing the information system or is in breach of this policy;
- Informing the Information Security Manager owner immediately in the event of a security incident involving the system;

Each Line Manager is responsible for:

- The implementation of this policy
- Ensuring that all members of staff who report to them are made aware of and are instructed to comply with this policy
- Ensuring complete and timely user access requests are forwarded to the Administrator allowing sufficient time for the creation of the required user account prior to the users start date;
- Ensuring that each user they request access fulfills all the criteria (principle of "least privilege") for the requested computer system
- Ensuring they make timely requests for the suspension of all user accounts belonging to members of their staff who are going on maternity leave or leave or those on long term sick leave;
- Ensuring they make timely requests for the deletion of all user accounts belonging to members of their staff who are leaving the employment the SES Group

Each user is responsible for:

- Complying with the terms of this policy applicable legislation;
- Respecting and protecting the privacy and confidentiality of the computer systems and network they access, and the information processed by those systems or networks
- Ensuring they only use user access accounts and passwords which have been assigned to them
- Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties
- Changing their passwords at least every 90 days or when instructed to do so by the administrators
- Complying with instructions issued by administrators
- Reporting all misuse and breaches of this policy to their line manager.

Name:	Tony Ball
Signature:	
Date:	1st May 2017

1	AS	TB - MD	01/05/17	N/A First Issue
Revision	Prepared by	Approved by	Issue Date	Description of Modifications Made