sse For a better world of energy

Group Cyber Security Policy

Policy statement

SSE’s policy on cyber security is that everyone working for, and on behalf of the company is aware of the relevant procedures and takes personal responsibility for keeping information, systems and related assets safe and secure.

Policy purpose

The purpose of the policy is to reflect the growing risk posed to SSE by cyber crime and to encourage employees to “Be Aware, Take Care, Stay Secure”.

This policy is owned by the Chief Information Officer and is one of a suite of group-level policies that promote a healthy business culture, guide decision and actions as expected by the company’s stakeholders, and make SSE a responsible company that people want to invest in, buy from, work for and partner with.

M. N. Wallis

Michael Wallis
Chief Information Officer

Alistair Phillips-Davies
Chief Executive Officer

Doc Ref: PO-GRP-003	**Version:** 1.0
Effective Date: April 2020	**Review Date:** March 2021

POLICY PRINCIPLES

The following principles highlight how we expect the policy statement to be achieved, and should be used to guide behaviours, decision making and action:

Information Security	• SSE remains vigilant to the threat of cyber-crime and the need to understand associated risks. We will: ○ take all the steps we can to keep our information and systems secure and embed controls within our technologies, processes and behaviours. ○ apply different levels of controls based on our Board approved cyber risk appetite. ○ respond promptly to attempts of unauthorised access to our information and systems and continually improve to prevent them reoccurring.
Critical National Infrastructure	• SSE recognises its responsibility for a large part of the UK's Critical National Infrastructure and seeks to ensure that our systems, assets and people are safe and secure, and that our customers are not put at risk. Our operational technology is at the core of our business, and in delivering essential services to citizens of the United Kingdom we seek to identify and mitigate the cyber risks to these systems.
Third Parties	• Interaction with third parties is managed to ensure that they understand their commitments to handle our information and systems legally and protect it appropriately.
Processes and Standards	• Established information security processes, in conjunction with the relevant standards, define how we will keep our information, systems and services secure. SSE utilises an industry standard framework to deliver a robust, repeatable, defensible, and cost-effective approach to managing cyber security risk. • SSE's Guide to Ethical Business Conduct sets out clearly the behaviours and standards expected of all of our employees when utilising SSE information, systems and services and support them in doing the right thing.
Employee Monitoring	• SSE monitors use of systems and services to ensure they are being used securely.