

# Group Cyber Security Policy

---

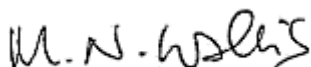
## Policy statement

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 cybercrime 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.



**Michael Wallis**

Chief Information Officer



**Alistair Phillips-Davies**

Chief Executive Officer



## 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	<ul style="list-style-type: none"> <li>• SSE remains vigilant to the threat of cyber-crime and the need to understand associated risks. We will:           <ul style="list-style-type: none"> <li>○ take all the steps we can to keep our information and systems secure and embed controls within our technologies, processes and behaviours.</li> <li>○ apply different levels of controls based on our Board approved cyber risk appetite.</li> <li>○ respond promptly to attempts of unauthorised access to our information and systems and continually improve to prevent them reoccurring.</li> </ul> </li> </ul>
Critical National Infrastructure	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
Third Parties	<ul style="list-style-type: none"> <li>• Interaction with third parties is managed to ensure that they understand their commitments to handle our information and systems legally and protect it appropriately.</li> </ul>
Processes and Standards	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Employee Monitoring	<ul style="list-style-type: none"> <li>• SSE monitors use of systems and services to ensure they are being used securely and in accordance with SSE Policies, Standards, Guidance and published documents.</li> </ul>



## ROLES AND RESPONSIBILITIES

This policy applies to all SSE employees, contingent workers and people contracted to provide services to the Company through third parties.

Where we operate internationally, we will utilise our Group Policies as a default, subject to legal or regulatory requirements of the relevant international domain, and relevant local policies and supporting procedures.

**Managers** are responsible for making sure that their teams understand and comply with the policy and supporting procedures as well as complete any relevant cyber training and report any potential security incident under the 30-minute rule.

**All employees, including everyone working on behalf of the company** must comply with the policy and supporting procedures and complete any relevant cyber training and report any potential security incident under the 30-minute rule.

All SSE employees have an individual responsibility to work in a way that protects us all from cyber threats. It is our duty to understand the risks, learn how to recognise something unusual and take all the steps we can to keep ourselves and our information and systems secure. This means: -

- Being Aware by being vigilant at all times, in different places and situations.
- Taking Care by knowing what you must do with SSE information to keep it secure.
- Staying Secure by taking actions which will keep you and SSE cyber secure.

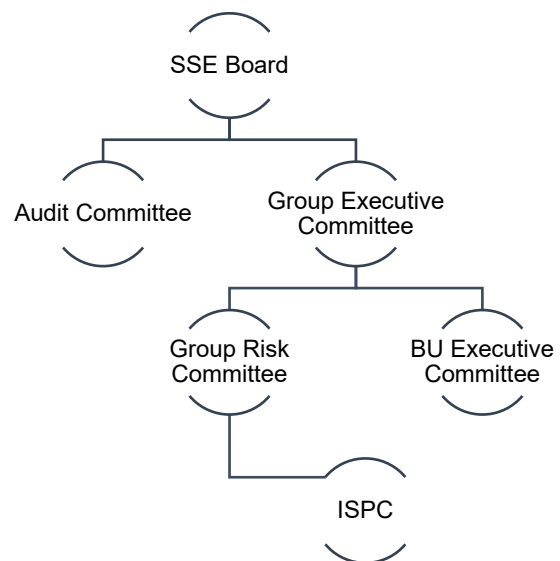


## GOVERNANCE

The **SSE plc Board** and **Group Executive Committee** are responsible for the oversight for this policy including the approval of any changes to the policy. This policy is reviewed annually as part of an evaluation process.

The **Information Security and Privacy Committee** (ISPC) supports SSE’s Chief Information Officer to make sure that the policy is adhered to through awareness, training and monitoring of policy implementation.

Incidents and breaches are reviewed and where appropriate opportunities for improvement are actioned.





## TRAINING

SSE has an Ethics and Compliance eLearning programme for key topics to ensure we are all aware of our responsibilities for doing the right thing.

### **Cyber Security – Everyone**

It is mandatory for all employees to complete this eLearning course annually. Comprising of four short modules, this shows you how to recognise and avoid falling victim to a phishing attack, how to classify and handle sensitive information and how to stay safe online when working from home or wherever you are.

### **Cyber Security – Operational Technology**

Mandatory for certain colleagues and optional for all. This eLearning course highlights important knowledge for those who use hardware and software to monitor or control physical devices, processes and events that relate to our networks, power generation and gas storage.

### **Cyber Security – Privileged Users**

This eLearning course explains the responsibilities and obligations associated with having higher levels of access to systems or information. This is mandatory for some colleagues and is recommended for anyone who wants to learn more.



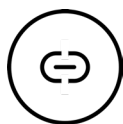
## SPEAKING UP

All employees are expected to comply with the policy and supporting procedures and complete all relevant training. Failure to adhere to the policy can have very serious consequences for SSE including safety issues, significant fines, breach of regulation and reputational impact. Not adhering to this policy (and supporting procedures) may result in withdrawal of systems access, and / or HR disciplinary measures up to dismissal.

Employees can discuss anything that falls short of our expected high standards of ethical conduct and compliance, with their line or any other manager within the business. Alternatively, any concerns can be raised internally at [Speakup@sse.com](mailto:Speakup@sse.com) or externally through SafeCall using:

- Phone:
  - UK - 0800 915 1571
  - Ireland - 1800 812 740
  - All other countries +44 800 915 1571. If you are more comfortable speaking in your own language, an independent telephone interpreter will be made available.
- Email: [sse@safecall.co.uk](mailto:sse@safecall.co.uk)
- [www.safecall.co.uk/report](http://www.safecall.co.uk/report)

*Any wrongdoing brought to light through the Whistleblowing Policy will result in internal disciplinary procedures, possible dismissal and criminal prosecution of individuals involved.*



## SUPPORTING DOCUMENTS

SSE's Guide to Ethical Business Conduct [Doing the Right Thing](#) sets out clearly the behaviours and standards expected of all of our employees.

Additional guidance and supporting documents can be found on:

- Document Library – [Information Security](#)
- Document Library – [STM-HR-001 Employee Rules](#)
- [SSEnet Cyber Secure site](#)

Complementary Policy:

- PO-GRP-004 [Group Data & Information Management Policy.](#)