Group Cyber Security Policy

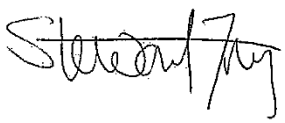
Policy statement

SSE's cyber security policy exists to support everyone at SSE to be responsible for the security of our networks, digital systems and data on which the organisation relies to ensure we can use technology and information effectively to deliver our business operations, growth targets and meet regulatory commitments.

Policy purpose

The purpose of this policy is to set out how SSE manages the cyber risks it faces from cyber threats to our networks, digital systems and data. These threats can come from adversarial sources such as cyber-criminals and nation states, as well as from non-adversarial factors. This policy applies to all our communities (inc. SSE employees, contingent workers and contract partners) supporting them 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.



Stewart Fry

Chief Information Officer

Martin Pibworth

Chief Executive Officer

Doc Ref: PO-GRP-003

Version: 3.00

Effective Date: April 2026

Review Date: April 2027

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:

Govern	• SSE employs a management system for cyber security and resilience, by: ○ Ensuring organisational context and continuous improvement informs our cyber risk management strategy, expectations and policy. ○ Establishing governance and oversight activities for cyber risk management, supported by defined roles, responsibilities and authorities, and metrics. ○ Employing procedures that ensure compliance with applicable cybersecurity regulations, and safeguard Critical National Infrastructure and essential services.
Identify	• Cyber risks are managed by: ○ Maintaining inventories of hardware, software, services, systems and suppliers used by SSE to achieve business purposes. ○ Understanding risks through identification, validation and recording of asset vulnerabilities and threat exposure, assessed in terms of likelihood and impact. ○ Responding to risks in a prioritised, planned, tracked and communicated manner in line with our risk appetite. ○ Integrating cyber security into broader supply chain risk management processes and deliver risk-based controls and proportionate supplier assurance.
Protect	• Security controls are implemented to prevent or lower the likelihood or impact of cyber incidents, by: ○ Building our people's awareness and competence to perform cyber security activities and clearly setting out the behaviours and standards expected of our employees. ○ Limiting access to assets and systems to authorised users. ○ Adopting secure by design principles especially in new projects and programmes to build security in from the outset.

	○ Managing the confidentiality, integrity and availability of our data whilst in use, at rest, and during transit. ○ Managing platform and infrastructure security across IT and OT systems. ○ Managing system asset's vulnerability, threat exposure, and resilience consistent with our risk appetite.
Detect	• Possible cyber incidents are found and analysed, by ○ Understanding threats and monitoring assets to find anomalies, indicators of compromise, and other potentially adverse events. ○ Analysing anomalies, indicators of compromise and other potentially adverse events to detect cybersecurity incidents.
Respond	• Actions regarding detected cybersecurity incidents are taken, by: ○ Actively managing, communicating and reporting cybersecurity incidents with appropriate stakeholders. ○ Investigating cybersecurity incidents to understand the course of events and the root cause, and to preserve necessary incident data for future reference. ○ Mitigating cybersecurity incidents by preventing expansion and reducing impact.
Recover	• Assets and operations affected by cybersecurity incidents are restored, by: ○ Executing incident recovery plans that prioritise recovery actions, verify restoration assets (e.g. backups) and restored assets, and re-establish operational-norms. ○ Coordinating recovery activities with appropriate stakeholders.

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.

Managing Directors & Directors are responsible for implementing and operating SSE's cyber security management system to ensure adequate management of cybersecurity risks and compliance with applicable regulations. They are also responsible for promoting a positive culture towards cyber security through visible, proactive, and consistent leadership to achieve positive cyber security outcomes for SSE.

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 and systems to keep it or them 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.

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.

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 and the associated Technology Acceptable Use 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 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
- 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 – Employee Rules
- SSEnet – Cyber Defence

Complementary Policy:

- PO-GRP-004 Group Data & Information Management Policy.