

Contents

- PART 1** A Quick-Reference Fraud Reporting Guidance Note for Staff
- PART 2** Spatial Initiative Ltd Anti-fraud Policy & Response Plan

Policy Statement and Applicability

- This policy applies to all companies within the Spatial Initiative, namely Spatial Initiative Limited and its subsidiaries ('**Spatial Initiative**'). Spatial Initiative requires its staff, along with all people and organisations we engage with commercially, to act honestly and with integrity.
- This policy should be read in conjunction with Spatial Initiative's "**Statement of Ethics**". It is the Company's policy to conduct all of its business in an honest and ethical manner. Spatial Initiative takes a **zero tolerance approach** to fraud - and all forms of corruption and bribery associated with fraudulent or criminal acts.
- Fraud may occur internally or externally and the purpose of this document is to set out responsibilities with regard to fraud prevention, what to do if fraud or irregularity is suspected and the response and subsequent action that will be taken by management.
- This policy does not form part of any employee's contract of employment and it may be amended at any time.

PART 1

Quick-Reference Guidance Note – Reporting Fraud

DO	DON'T
<p>✓ Report your suspicions promptly</p> <p>Any suspicion of fraud or other irregularity must be reported in the first instance - and as a matter of urgency - to the Chief Finance Officer by email at Barry.Mccrane@essmodular.com</p> <p>In addition, your concerns should be reported to your line-manager (where this is appropriate) or, alternatively, to the Group HR Director Maria.Mccarthy@essmodular.com)</p> <p>✓ Make a note of your concerns</p> <p>Record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names dates and times and any witnesses</p> <p>Notes do not need to be overly formal, but should be timed, dated and signed</p> <p>Timeliness is most important. The longer you delay writing up, the greater the chances of recollections becoming distorted</p> <p>✓ Retain any evidence you may have</p> <p>The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation</p>	<p>! Don't be afraid of raising concerns</p> <p>Our Whistleblowing Policy provides protection for employees who raise reasonably held concerns through the appropriate channels</p> <p>You will not suffer discrimination or victimisation as a result of following these procedures and the matter will be treated sensitively and confidentially</p> <p>! Don't convey your concerns to anyone other than authorised persons</p> <p>This will avoid compromising any investigation. Furthermore, there may be a perfectly reasonable explanation for the events that give rise to your suspicion</p> <p>! Don't approach the person you suspect or try to investigate the matter yourself</p> <p>Any attempt to gather evidence by persons who are unfamiliar with these rules may destroy the case or compromise the investigation</p>

The Fraud "Warning Signs":
Things to look out for...

- Urgent and unexpected requests to approve large payments ahead of public holidays or late on Friday afternoon – this is a common fraud tactic as detection may be delayed for several days
- Suspicious activities, uncharacteristic behaviour or unexpected displays of conspicuous wealth
- Unexpected requests by email, phone or letter to change payment details or contact details – this is a common fraud tactic and independent checks must be made before making changes
- Emails with unexpected attachments and especially from non-work related addresses which contain suspicious language or spelling errors
- Unsolicited requests for sensitive financial information, banking details or IT information
- Documents, data, information or applications that appear odd, altered or tampered with
- Unexplained changes to a standard procedure or the way somebody works
- Evidence that existing procedures have been bypassed or short-circuited
- Unusual requests to provide commercially sensitive, confidential or personal information

Sometimes things just don't "look right" or "sound right"... Don't be afraid of voicing instinctive concerns

Examples of fraud risk relevant to Spatial Initiative

- Changes requested to third party bank details to divert loans, grants and supplier payments
- Needlessly obtaining our sensitive financial, banking or IT information
- False orders or claims for work undertaken or false applications for payment
- Fraudulent procurement activities such as bid collusion, bribery or other contract-related fraud
- Actual or attempted theft of operational assets including high-value equipment
- Property fraud including diversion of rent, unauthorised use and encroachment
- Inappropriate disclosure or manipulation of data or information for financial gain
- IT / cyber-attacks including installation of ransom ware, viruses and similar malware
- Miscellaneous employee related fraud including falsified working hours and expense claims and the misuse of corporate credit cards

PART 2

Spatial Initiative Anti-Fraud Policy

1.0 Definitions of Fraud

1.1 The Fraud Act 2006 identifies:

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position

These are criminal offences liable to criminal prosecution.

1.2 'Cyber fraud' may be defined as the generic term commonly employed when information technology has been used to manipulate programs or data dishonestly, e.g. by altering, substituting, destroying records or creating spurious records or where the use of an IT system was a material factor in the perpetration of a fraud. This includes theft or fraudulent use of computer time and resources. Examples include altering, substituting or destroying records, or creating spurious record.

1.3 Commercial fraud may also lead to civil action. The term describes a range of different activities, in respect of which there may be a number of causes of action. These may include deceit, conspiracy, breach of fiduciary duty, breach of trust, dishonest assistance and conversion – amongst others.

1.4 Spatial Initiative has a separate **Anti-Bribery and Corruption Policy**. If you are unsure which category of crime has occurred you must report your suspicions without delay as directed in the Spatial Initiative **Whistleblowing Policy**.

1.5 Fraud may take many different forms. Spatial Initiative's business routinely encounters a number of fraud-risks associated with its operations including:

- False payment claims
- Fraudulent procurement / contract fraud
- False or duplicate invoices / false orders / diversion of funds
- Theft of property assets / theft of operational assets
- Inappropriate disclosure of information / IT attacks including ransom ware
- Employee-related fraud including falsified working hours and expenses

1.6 The Chief Executive Officer has overall accountability for managing the risk of fraud.

1.7 All Line Managers have day-to-day responsibility for the prevention and detection of fraud and are responsible for:

- Identifying the risks to which systems, operations and procedures are exposed
- Developing and maintaining effective controls to prevent and detect fraud
- Ensuring that controls are being complied with

1.8 All staff must act with propriety in the use of company resources and in the handling and use of company funds.

2.0 Reporting

2.1 Should any member of staff or contractor suspect that a fraud may have been committed or attempted or identify evidence of irregular, improper or suspicious behaviour they should report the matter to the Chief Finance Officer by email at Barry.mccrane@essmodular.com. In addition, your concerns should be reported to your line-manager (where this is appropriate) or, alternatively, to the Group HR Director Maria.mccarthy@essmodular.com

3.0 Fraud Response Plan

3.1 Spatial Initiative has prepared a quick-reference Guidance Note (see **Part 1** of this document) and Fraud Response Plan (see **Part 2**, Section **6.0** onwards in this document). The Fraud Response Plan contains a list of key actions to follow in the event that fraud is suspected, or it is believed that fraud has been attempted.

4.0 Disciplinary Action

4.1 In the case of proven fraud, or suspected fraud of a serious nature, Spatial Initiative will always take the following actions:

- Refer the matter to the police or appropriate reporting authority
- When appropriate, seek prosecution at the earliest possible juncture
- Seek to recover any loss resulting from fraud, if necessary, through civil action.

4.2 The Chief Executive Officer will determine whether to invoke action in accordance with established disciplinary procedures if staff have acted inappropriately in connection with attempted or actual fraud.

5.0 Conclusion

5.1 Spatial Initiative views fraud very seriously. All instances will be investigated rigorously and promptly and appropriate action will be taken including seeking prosecution in cases of proven fraud.

5.2 For advice and guidance in relation to fraud concerns please contact the Chief Finance Officer by email at Barry.mccrane@essmodular.com or, alternatively, the Group HR Director Maria.mccarthy@essmodular.com

Spatial Initiative Ltd Fraud Response Plan

6.0 What is Included?

- 6.1
- Notifying suspected fraud and attempted fraud
 - Recording your concerns and retaining evidence
 - The investigation process
 - Reporting process
 - Liaison with police and NAO
 - Initiation of recovery action

7.0 Notifying Suspected Fraud and Attempted Fraud

7.1 Please do not convey your concerns to anyone other than authorised persons – see

below and Quick Reference Guidance Note.

- 7.2 It is important that all staff are able to report their concerns without fear of reprisal or victimisation and are aware of the means to do so. Spatial Initiative will provide protection for employees who raise reasonably held concerns through the appropriate channels. You will not suffer discrimination or victimisation as a result of following these procedures and the matter will be treated sensitively and confidentially. Please see Spatial Initiative **Whistleblowing Policy** for further details.
- 7.3 Any suspicion of (attempted) fraud, theft or other irregularity must be reported in the first instance - and as a matter of urgency - to the Chief Finance Officer by email at Barry.mccrane@essmodular.com.
- 7.4 In addition, your concerns should be reported to your line-manager (where this is appropriate) or, alternatively, to the Group HR Director (Maria.mccarthy@essmodular.com)
- 7.5 The Chief Finance Officer is required to promptly notify the Head of Compliance when fraud (or attempted fraud) has been reported and share relevant information – providing that this will not compromise the independence or outcome of any investigation. This is to ensure that internal controls can be immediately reviewed and additional resilience measures put in place where necessary.
- 7.6 Every effort will be made to protect an informant's anonymity if requested.

8.0 Recording Concerns and Retaining Evidence

- 8.1 Promptly record all relevant details, such as the nature of your concern, the names of parties you believe to be involved and details of any telephone or other conversations together with names dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, dated and signed.
- 8.2 Timeliness is most important. The longer you delay writing up your concerns, the greater the chances of recollections becoming distorted.
- 8.3 It is important to retain any evidence you may have discovered. The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation. Preserving time-sensitive electronic evidence, or messaging is particularly important.

9.0 The Investigation Process

- 9.1 Suspected fraud must be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both Spatial Initiative and the rights of the individual(s) suspected. Suspicion must not be treated as guilt to be proven.
- 9.2 The Chief Finance Officer will trigger the investigation process, notifying the Chief Executive Officer that an independent investigation is required (where appropriate).
- 9.3 The investigation process will vary according to the circumstances of each case and will be determined by the Chief Finance Officer in consultation with key staff such as the Head of Compliance and the Chief Executive Officer. An “Investigating Officer” will usually be appointed to take charge of the investigation on a day-to-day basis. This may be the Chief Finance Officer, or his nominee.

- 9.4 If necessary and appropriate, the Investigating Officer will appoint an investigating team. This may normally comprise staff from within the Compliance Team, but may be supplemented with other resources – whether internal or external.
- 9.5 In the case of suspected internal fraud or related misconduct, and where initial investigations reveal that there are reasonable grounds for suspicion, to facilitate the on-going investigation it may be appropriate to suspend an employee against whom an accusation has been made. This decision will be taken by the Chief Executive Officer and/or the Chief Finance Officer in consultation with the Group HR Director. Suspension should not be regarded as disciplinary action nor should it imply guilt.
- 9.6 From the outset, it is important, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate steps to secure physical assets, including computers and any records thereon, and all other potentially evidential documents. They will also ensure, in consultation with the appropriate line manager and the Group Head of IT Services, that appropriate controls are introduced to prevent further loss.
- 9.7 The Investigating Officer will ensure that a detailed record of the investigation is maintained. This should include a chronological file recording details of all telephone conversations, discussions, meetings and interviews (identifying who was present and what was said), details of documents reviewed, tests and analyses undertaken, the results and their significance. Everything should be recorded, irrespective of the apparent significance at the time.
- 9.8 All interviews will be conducted in a fair and proper manner. Where there is a possibility of subsequent criminal action, the police will be consulted and interviews may be conducted under caution in compliance with the Police and Criminal Evidence Act (PACE), which governs the admissibility of evidence in criminal proceedings.
- 9.9 The findings of the investigation will be reported to the Chief Executive Officer, the Chief Finance Officer, the Group HR Director and other key staff as appropriate.
- 10.0 Reporting Process**
- 10.1 Throughout any investigation, the Investigating Officer will keep the Chief Executive Officer and other appropriate officers informed of progress and any developments. These reports may be verbal or in writing.
- 10.2 On completion of the investigation, the Investigating Officer will prepare a full written report setting out:
- Background as to how the investigation arose
 - What action was taken in response to the allegations
 - The conduct of the investigation
 - The facts that came to light and the evidence in support
 - Action taken against any party where the allegations were proved
 - Action taken to recover any losses
 - Recommendations and/or action taken by management to reduce further exposure and to minimise any recurrence
- 10.3 To raise awareness of fraud risk, the Chief Executive Officer, in consultation with Chief Finance Officer and the Head of Compliance, may decide to circulate an internal communication containing an anonymised summary of the risk event.

11.0 Liaison with Police

- 11.1 The police generally welcome early notification of suspected fraud - particularly that of a serious or complex nature. The Chief Executive Officer, following consultation with the Chief Finance Officer and having taken legal advice, will decide if and when to contact the police. If a decision is taken to notify the police, the Chief Finance Officer will report fraud events to the police on behalf of the company.

12.0 Initiation of Recovery Action

- 12.1 Spatial Initiative will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct. This may include civil action against third parties involved in the fraud, or whose negligent actions contributed to the fraud, to recover any losses.