**1.Purpose**

Information that’s collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, as well as possible judgements being made against Southern Asset Management.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

**2.Scope**

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

**Who is covered under the Information Security Policy?**

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

**3.Policy elements**

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

* Accurate and kept up-to-date
* Collected fairly and for lawful purposes only
* Processed by the company within its legal and moral boundaries
* Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

* Communicated informally
* Stored for more than a specified amount of time
* Transferred to organizations, states or countries that do not have adequate data protection policies
* Distributed to any party other than the ones agreed upon by the data’s owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

* Let people know which of their data is collected
* Inform people about how we’ll process their data
* Inform people about who has access to their information
* Have provisions in cases of lost, corrupted or compromised data
* Allow people to request that we modify, erase, reduce or correct data contained in our databases

**4.Actions**

To exercise data protection we’re committed to:

* Restrict and monitor access to sensitive data
* Develop transparent data collection procedures
* Train employees in online privacy and security measures
* Build secure networks to protect online data from [cyberattacks](https://resources.workable.com/cyber-security-policy)
* Establish clear procedures for reporting privacy breaches or data misuse
* Include contract clauses or communicate statements on how we handle data
* Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)
* Processed lawfully, fairly and in a transparent manner in relation to individuals.
* Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
* Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

**5.Access control and Asset Handling**

Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties. All laptops and mobile devices are password protected.

Our BMS and Portal have two factor authentication. A Virtual Private Network is required to access the BMS which is authorised by the software management company. Anti Virus software is installed on mobile devices.

The CEO of Southern Asset Management can register access to employees to access all information systems and services. This access is removed if an employee leaves the business.

**6. Communications security**

Southern Asset Management will maintain network security controls to ensure the protection of information within its networks. Southern Asset Management will also provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities. This is in line with the classification and handling requirements associated with that information.

**7. Physical and environmental security**

We have numerous security measures in place at Southern Asset Management including our site being on a secure gated premises which is locked out of hours. We have mobile CCTV set up on site along with an alarm which alerts the Management Team of any issues on site. Only specific members of the team own a set of site keys. The premises is double locked.

**8. Supplier relationships**

Southern Asset Management’s information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

**9. Information security incident management**

Guidance will be available on what constitutes an information security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated by the CEO. The appropriate action to correct the breach will be taken, and any learning built into controls.

**10. Information security aspects of business continuity management**

Southern Asset Management will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters. This is to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience. Business continuity plans must be maintained.

**11.Training**

All employees of Southern Asset Management are required to read and review this policy during their induction to their job. Procedures around information security are shown to employees during induction and training as required. Any updates are communicated as required.

**12.Disciplinary Consequences**

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possible legal action.

**POLICY OWNER:** Stephen Southern- CEO

**SIGNATURE**:

**DATE:** November 2024

**POLICY REVIEW DATE**: November 2025