

Due South Group

Data Protection & Information Security Policy

Document Reference: DSG-GOV-012

Version: 1.0

Approved By: Chief Executive Officer

Review Period: Annual

Classification: Public

Foreword from the Chief Executive

Information is one of Due South Group's most valuable assets.

Our clients, governments, funding organisations and business partners entrust us with commercially sensitive, technical and personal information. Protecting that information is fundamental to maintaining confidence in our organisation and to delivering projects responsibly.

Due South Group is committed to safeguarding information against unauthorised access, loss, misuse, alteration or disclosure. We recognise that effective information security is essential to protecting our business, supporting our partners and maintaining compliance with applicable legal and contractual obligations.

This Policy establishes the principles for protecting information throughout its lifecycle.

Steven Edwards

Chief Executive Officer

1. Purpose

This Policy establishes the framework for protecting personal data, confidential information and Company information assets.

Its objectives are to:

- Protect the confidentiality, integrity and availability of information.
- Comply with applicable data protection legislation.
- Support secure project delivery.
- Reduce cyber security risks.
- Protect client, donor and Company information.
- Promote responsible information management.
- Strengthen organisational resilience.

2. Scope

This Policy applies to:

- Directors.
- Employees.
- Consultants.
- Contractors.
- Temporary personnel.
- Suppliers where contractual obligations apply.
- All Company information, regardless of format or location.

Information may include:

- Personal data.
- Project documentation.
- Engineering drawings.
- Contracts.
- Financial information.
- Commercial information.
- Emails.
- Digital records.
- Paper records.

- Photographs.
- Audio and video recordings.

3. Our Principles

Due South Group is committed to:

- Respecting privacy.
- Protecting confidential information.
- Using information responsibly.
- Maintaining secure systems.
- Preventing unauthorised disclosure.
- Managing information throughout its lifecycle.
- Continually improving information security.

4. Data Protection

Where Due South Group processes personal data, we will seek to ensure that it is:

- Processed lawfully, fairly and transparently.
- Collected for legitimate business purposes.
- Limited to what is necessary.
- Accurate and kept up to date where appropriate.
- Protected through suitable technical and organisational measures.
- Retained only for as long as necessary.
- Disposed of securely when no longer required.

The Company will comply with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 where applicable.

5. Information Classification

Information should be protected according to its sensitivity.

The Company may classify information as:

- Public.
- Internal.
- Confidential.
- Restricted.

Personnel are expected to apply appropriate safeguards according to the classification of the information they handle.

6. Confidential Information

Confidential information belonging to clients, governments, funding organisations, suppliers, employees or Due South Group shall be protected at all times.

Confidential information must not be disclosed without appropriate authority or legal justification.

These obligations continue after employment or contractual relationships have ended.

7. Information Security

Due South Group will seek to protect information through appropriate administrative, physical and technical controls.

These may include:

- Strong authentication measures.
- Password management.
- Secure storage.
- Controlled access.
- Encryption where appropriate.
- Secure communication methods.
- Backup arrangements.
- Malware protection.
- Secure disposal of information.

Access to information shall be limited to those with a legitimate business need.

8. Cyber Security

The Company recognises the increasing threat posed by cyber attacks.

Personnel are expected to:

- Protect passwords and authentication credentials.
- Report suspicious emails or cyber incidents immediately.
- Use authorised software and systems.
- Keep devices secure.
- Follow Company security procedures when working remotely.

Cyber security awareness forms part of everyone's responsibilities.

9. Remote Working and Mobile Devices

Personnel working remotely or travelling shall take appropriate precautions to protect Company information.

This includes:

- Securing laptops, tablets and mobile phones.
- Avoiding the use of unsecured public Wi-Fi where sensitive information is being accessed.
- Protecting documents during travel.
- Preventing unauthorised viewing of confidential information.
- Reporting lost or stolen devices immediately.

10. Records Management

Accurate records support good governance and effective project delivery.

The Company will seek to:

- Maintain accurate records.

- Store records securely.
- Retain information for appropriate periods.
- Dispose of information securely when no longer required.

Records should be readily retrievable while protected against unauthorised access or alteration.

11. Information Sharing

Information shall only be shared where:

- There is a legitimate business need.
- Appropriate authority has been obtained.
- Contractual obligations permit disclosure.
- Legal requirements are satisfied.
- Appropriate safeguards are in place.

Care shall be taken when sharing information with governments, clients, contractors or third parties.

12. Incident Reporting

Any suspected information security incident shall be reported immediately.

Examples include:

- Loss of documents.
- Cyber attacks.
- Unauthorised disclosure.
- Data breaches.
- Theft of equipment.
- Accidental transmission of confidential information.
- Malware infection.
- Unauthorised system access.

Prompt reporting supports effective response and minimises potential impacts.

13. Training and Awareness

Due South Group will promote awareness of data protection and information security through:

- Staff induction.
- Periodic training.
- Cyber security awareness.
- Project briefings.
- Lessons learned.
- Policy updates.

Personnel are expected to remain vigilant and seek guidance whenever uncertainty exists.

14. Responsibilities

The Chief Executive has overall responsibility for promoting effective information governance within the Company.

Managers are responsible for implementing this Policy within their areas of responsibility and ensuring that personnel understand their obligations.

Every employee, consultant and contractor shares responsibility for protecting the information entrusted to the Company.

15. Monitoring and Continuous Improvement

Due South Group will continue to strengthen information security through:

- Periodic policy reviews.
- Risk assessments.
- Lessons learned.
- Incident reviews.
- System improvements.
- Staff awareness.

- Technological enhancements where appropriate.

16. Review

This Policy shall be reviewed annually or following significant legislative, organisational or technological changes.

17. Our Commitment

Due South Group is committed to protecting the confidentiality, integrity and availability of information entrusted to us.

By applying robust information governance, responsible data protection practices and effective information security controls, we seek to maintain the confidence of our clients, governments, funding partners and business partners while supporting the successful delivery of infrastructure, renewable energy and humanitarian projects.