CODE OF CONDUCT

SRG Specialist Risk Group

WHO IS SPECIALIST RISK GROUP?

Specialist Risk Group (SRG) is a leading specialist insurance group delivering solutions across niche and complex risk markets, serving more than 120,000 clients internationally.

Behind every solution we provide is a team of specialists who are passionate about what they do. Our people thrive on tackling complex challenges, finding creative solutions and delivering exceptional outcomes for clients. We call this Difficult. Done Well. It's more than a strapline, it's a reflection of the expertise, commitment and entrepreneurial spirit that define SRG.

WHAT WILL THIS CODE TELL YOU?

This Code of Conduct sets out the standards and behaviours expected of everyone working for and on behalf of the SRG group of companies. It provides guidance on how to make the right decisions, manage risks, and act in line with our values and regulatory responsibilities.

We are proud of the culture we are building; one that values respect, supports our colleagues, and enables everyone to reach their full potential with ambition and confidence.

CONTENTS

Chapter 1
Our Culture & Ways of Working

Message from the CEO 8
Our Values & Behaviours 10
Our Responsibilities 14
Risk Management 16
Training & Development 18
Concerns & Speaking Up 20

Chapter 2
Preventing Financial Crime

Financial Crime 24
Economic Sanctions 26
Gifts & Hospitality 28
Conflicts of Interest 30
Third-Party & Counterparty Risk 32

Chapter 3
Protecting Information & Systems

Data Protection 36
Types of Confidential Information 38
Cyber Security 40

Chapter 4
Relationships with Our Community

Modern Slavery 44
Vulnerable Customers 46
Environmental, Social & Governance (ESG) 48
Health & Safety 50

OUR CULTURE & WAYS OF WORKING

1

MESSAGE FROM THE CEO

Warren Downey
Group Chief Executive Officer

Our business is built on trust. Trust from our colleagues, clients, trading partners, regulators, and shareholders. We deliver on our promises, putting clients' interests first while meeting regulatory expectations.

Delivering on our promises becomes more critical as we expand our number of specialisms internationally, embracing new markets, colleagues, and cultures. Our Code of Conduct therefore sets out the standard of behaviour we expect from every colleague in SRG across all the markets we operate in.

Our values of being kind, positive and thoughtful underpin everything we do at SRG. These naturally extend into expectations around how we treat each other and the professional standard of care we exercise in serving our customers and meeting our obligations.

Our Code of Conduct isn't just a document. It lays the foundation for our standards around respect, trust, professionalism, and inclusion. We operate in highly dynamic and fluid regulatory environments. Going above and beyond when we're discharging our regulatory obligations is critical to our stakeholder relationship and reputation.

With our international growth, our reputation transcends geographical boundaries. Our Code of Conduct allows us to protect that reputation consistently wherever we operate. My expectations are that this Code of Conduct becomes a living part of our culture. It applies to us all and to me, regardless of seniority, function, or market.

Please do take the time to read it, embrace it, and ask questions if anything is unclear. Remember, strong conduct cultures build stronger client and stakeholder relationships, retain better talent, and build more sustainable partnerships with our markets.

Our Code of Conduct sets the tone for the future of SRG's growth journey.

OUR VALUES & BEHAVIOURS

Guided by our principles of being a good colleague and hitting our numbers, we're building a company we're proud to tell our friends and family about.

Our Values of Kind. Positive. Thoughtful. underpin everything we do at SRG.

These are the Values which underpin the professional and ethical behaviours SRG expects of all colleagues. We set clear behavioural expectations and collective responsibility for how we treat each other in the workplace.

We are committed to maintaining the highest standards of integrity across our business. Our zero-tolerance approach to misconduct is supported by a culture that encourages colleagues to speak up and report concerns with confidence.

Our behaviour in the workplace policy and clear behavioural framework ensures we manage and monitor conduct and take a firm stance against all misconduct including harassment, bullying, discrimination and violence.

Why are our Values Important?

Our Values lay the foundation for our Culture and directly impact our reputation. They set the premise for the behaviours expected of all colleagues within the SRG group, regardless of role, location or language. It's important that we keep our Values alive as we continue to grow and expand internationally.

How do I know what is expected of me?

Being a Good Colleague is a shared objective; for every colleague at all levels. Exhibiting kindness, positivity and thoughtfulness should be threaded through all our interactions and communications. The extension of this is adhering to regulations and any policies that your role might be governed by. You should make every effort to seek guidance on this from your Manager, the People and Culture team or the Compliance team. It is also important to familiarise yourself with the expectations set out in the career level framework. Depending on your level of seniority; we set clear expectations at each level on how we should conduct ourselves; being mindful of the impact and influence we have on others.

OUR VALUES & BEHAVIOURS

Guided by our principles of being a good colleague and hitting our numbers, we're building a company we're proud to tell our friends and family about.

Our Values of Kind. Positive. Thoughtful. underpin everything we do at SRG.

We embrace an open and diverse culture and expect that all colleagues, clients and stakeholders are treated with respect at all times, reinforcing a positive and respectful work environment where this Code of Conduct, regulations, policies and procedures are adhered to.

Driving openness and inclusion enables our colleagues to raise questions, concerns or any issues confidentially and safely, in the comfort that they will be dealt with promptly, with thoughtfulness and care.

What do I do if I witness poor behaviour in the workplace?

We are all collectively responsible for upholding our core behaviours and values; acting with respect and care for one one another. This extends to how we treat customers and partners too. If you have any concern about the conduct you are witnessing or experiencing, you should raise this immediately and can do so anonymously to a senior colleague, the People and Culture team, the Executive team or via the **SRG Whistleblowing facility.**

OUR RESPONSIBILITIES

We are committed to acting with integrity, professionalism, and care in everything we do. Everyone working for or on behalf of SRG, has ethical and contractual duties and is expected to comply with applicable laws, regulations, and regulatory requirements relevant to their role.

This means acting honestly, with due care and skill, treating customers fairly, managing risks responsibly, and cooperating openly with regulators.

We also look to ensure that we act ethically and always demonstrate professional office behaviours, in line with our non-financial misconduct responsibilities.

We all share responsibility for understanding our regulatory obligations, following policies and procedures, completing required training, and raising concerns where standards may not be met.

For further information or when in doubt, please speak to your relevant Compliance function.

How do regulatory obligations apply to non-customer-facing roles?

Even if you do not work directly with customers, your role may still impact outcomes, risk management, data quality, or decision-making. Regulatory standards apply to all roles that support the business; directly and indirectly and thus, reference should be made to the internal policies and procedures which help to navigate such requirements.

What should I do if I'm unsure about a regulatory requirement?

You should seek guidance from your manager or the Compliance team. Asking questions early helps prevent issues and supports good decision-making.

Conduct-related matters – what should I do if I am unsure about behaviour or a situation?

If you are unsure whether something is appropriate, compliant, or aligned with our Code of Conduct, you should pause and seek guidance. You can speak to your manager, People & Culture, or Compliance who can provide guidance and direct you to the relevant policies.

For example, in the UK, take a look at the **Conduct Policy** for further details.

RISK MANAGEMENT

We take a proactive approach to risk management, regularly assessing the risks we face and reviewing our controls to ensure they remain robust, effective, and aligned to our evolving business needs.

The SRG Risk Management Framework documents the processes including risk registers that are in place throughout SRG which contain the controls identified. The Risk & Control Self Assessment (RCSA) process is in place for risk and control owners to assess and reassess risks and controls to reflect the position at a given point in time. The process runs on a six-monthly cycle and ensures that all risk and controls are assessed, as a minimum, annually.

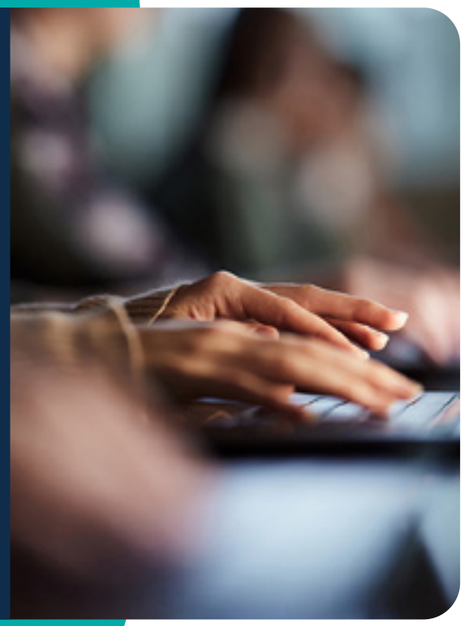
As well as formal reviews, we also maintain an Event Log, where issues, control failures and potential problems are recorded, assessed, and monitored, with clear ownership for managing and resolving them. We work closely with the business to identify and mitigate risks, escalate material issues where needed, and support adherence to our policies, standards, and frameworks. We also keep an eye on emerging risks to help protect our people, customers, and organisation.

For more details, look at our **Risk Management Policy.**

What is an Event Log and why is it important?

The Event Log is where we record and track risk events, incidents, or near misses for the UK and several of our entities. It helps us understand what has happened, take action to fix and report issues, and learn how to prevent similar risks in the future.

Reporting an event is quick and straightforward. Simply complete the **Event Reporting Form** and submit it.



How does risk management support our Code of Conduct?

Effective risk management helps us track and manage our risk exposure, make informed decisions, and meet our commitments to customers, partners, and regulators. It supports our values and helps maintain trust in how we operate.

TRAINING & DEVELOPMENT

It is a regulatory requirement across all jurisdictions SRG operates within that colleagues meet minimum requirements to ensure knowledge and competence is maintained within the insurance industry.

We support colleagues to meet their requirements by providing training material and opportunities throughout the year on several key topics. Training is provided to colleagues via e-learning platforms, in person sessions, and by encouraging colleagues to ensure they share knowledge. This isn't just a box-ticking exercise, it's a concerted effort designed to ensure we all have the skills, knowledge, and expertise to perform our roles effectively and deliver good outcomes for customers.

We encourage all colleagues to retain appropriate records to ensure they have met the requirements expected of them to stay aware and compliant of their professional needs.

For further guidance on training in the UK, take a look at the **Training & Competency Policy** or speak to People & Culture or Risk & Compliance for further details.

As we grow as a Group, we want to ensure our colleagues keep on growing too. We have several programmes ongoing across the Group to help facilitate this. Take a look on the Intranet or speak with the People & Culture team for more details at what you can get involved with!

We also look to help colleagues grow with encouragement and support for colleagues. In the UK, this is exemplified with encouragement to undertake further CII qualifications and build upon their expertise.

We also think about our next Generation too!
We are currently in our third High Potential Programme designed to develop and empower the next generation of leaders across our Group.

For further details, please speak to People & Culture for how you can be helped in your journey of growth.

CONCERNS & SPEAKING UP

We encourage everyone to speak up and raise concerns if something does not feel right. Raising concerns early helps us address issues quickly and maintain a safe, ethical, and compliant environment.

You can raise concerns through the channel you feel most comfortable with. Reports can be raised to your line manager, People & Culture or to Compliance.

If you feel more comfortable remaining anonymous whilst raising your concerns, you may also file an anonymous report through the **SRG Whistleblowing facility.** We are committed to creating an open environment where people feel comfortable raising concerns. All such matters are treated with confidentiality and SRG does not tolerate any retaliation against those who speak up. This may lead to disciplinary action, up to and including termination.

When should I speak up?

You should speak up if you witness or suspect behaviour inconsistent with our values, policies, or legal obligations. You do not need to be certain, raising concerns early helps prevent issues.

What types of concerns should be reported?

Any actual or suspected misconduct, wrongdoing, breach of internal policies or breach of regulations. Examples include:

- Fraud, bribery, corruption, or financial crime.
- Breaches of law or regulation.
- Serious misconduct or unethical behaviour.
- Health and safety risks.
- Mistreatment of customers, including vulnerable customers.
- Retaliation against someone who has spoken up.

PREVENTING FINANCIAL CRIME

2

FINANCIAL CRIME

SRG is committed to preventing financial crime, including money laundering, evasion of sanctions, fraud, bribery, corruption, and the financing of terrorism. Financial crime harms customers, markets, and society, and exposes our organisation to serious regulatory, legal and reputational risk.

Financial crime risks can arise across products and transactions, including policy onboarding, premium handling, claims, refunds, and third-party relationships. We take a zero-tolerance approach to financial crime and expect everyone to remain alert, follow our policies and procedures, and raise concerns promptly to your Compliance function.

Examples of suspicious activities which may be indicative of Financial Crime include:

- Unusual payment methods or third-party payments.
- Overpayments followed by refund requests.
- Early policy cancellations with refund demands.
- Claims that do not align with policy details or risk profile.
- Reluctance to provide customer information.

What is money laundering?

Money laundering is the process of disguising the proceeds of crime to make them appear legitimate. This can involve placing, layering, and integrating illicit funds through financial systems, including insurance products.

What is Customer Due Diligence (CDD)?

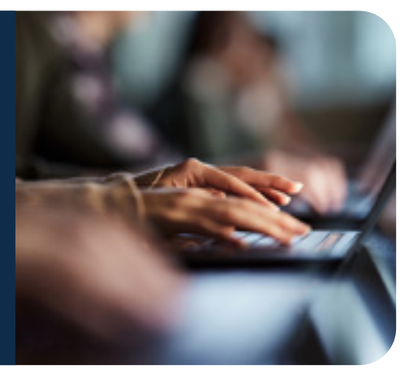
CDD is the process of verifying a customer's identity and understanding their risk profile. This helps ensure we know who we are doing business with and assess financial crime risk appropriately.

What happens if we fail to prevent financial crime?

Failures can result in regulatory action, fines, criminal penalties, reputational damage, and harm to customers and markets.

How does training support the prevention of Financial Crime?

Training helps people recognise risks, understand red flags, and know how and when to escalate concerns. Mandatory training ensures consistent awareness across the organisation.



ECONOMIC SANCTIONS

We are committed to complying with all applicable economic and trade sanctions laws and regulations, including the sanctions regimes arising from the UK, EU, US, UN and relevant local jurisdictions.

Sanctions are designed to restrict dealings with certain countries, territories, organisations, entities, vessels, and individuals, and in certain trades and sectors whereby failure to comply can result in serious legal and reputational consequences.

Sanction risks may arise at differing stages of a risk placement or transactions. Everyone has a responsibility to remain alert to sanctions risks and follow our policies and procedures.

If you identify or suspect a sanctions issue, you must escalate it immediately in accordance with the applicable policies and processes and bring it to the attention of your Compliance function. Do not proceed with the transaction or further communication until guidance is received!

How do we manage sanctions risk?

We use screening, ongoing monitoring, due diligence, and controls to identify and manage sanctions risks at onboarding and throughout the lifecycle of a policy or claim.

How often do sanctions change?

Sanctions issued under the various regimes change frequently, at times daily. This is why ongoing monitoring, screening, and awareness are essential.

Do sanctions apply only to customer-facing teams?

No. Sanctions risks can arise in many areas including underwriting, claims, payments, procurement, investments and reinsurance, and in the procurement or use of IT licences, hardware or software. Everyone has a role to play.

What happens if sanctions rules are breached?

Breaches can result in corporate and personal liability such as severe penalties, including fines, regulatory action, criminal liability, and reputational damage. If you suspect sanctions exposure or a breach, please contact the Compliance function immediately.

GIFTS & HOSPITALITY

We sometimes give or receive gifts and hospitality as part of building positive business relationships. However, these must never influence business decisions.

Gifts and hospitality must be reasonable, proportionate, and appropriate, and must comply with our policies and approval requirements. We do not give or accept gifts or hospitality that could create a sense of obligation, give rise to a conflict of interest, influence decision-making, or damage trust.

Gifts of cash or cash equivalents, and gifts and/or hospitality to government officials are strictly prohibited.

Remember: Failing to record or declare gifts and hospitality or seek necessary approval is a breach of internal policy and could be seen as bribery or a conflict of interest. Providing full disclosure and keeping records protects both you and the company.

For the UK & Ireland, you can find the **G&H form** and more information on the **Gifts and Hospitality** section of the Compliance SharePoint page.

Alternatively, speak to your Compliance function for further details.

Does this apply to suppliers, customers, and brokers?

Yes. The rules apply to all third-party relationships, giving to or receiving from suppliers, customers, brokers, reinsurers, and other business partners.

What should I do if I'm unsure?

If in doubt, seek advice from Compliance before accepting or offering anything. Transparency and early guidance help avoid issues and ensures appropriate reporting is maintained.

CONFLICTS OF INTEREST

Managing conflicts helps us make fair, transparent, and objective decisions. It protects our people, our organisation, and our reputation.

It is fundamental that SRG ensures that Conflicts of Interests are managed appropriately. In the UK & Ireland, this is done by annual attestations, the **Conflicts of Interest declaration form**, training and following the **Conflicts of Interests policy.**

Alternatively, speak to your Compliance function for further details.

There are various examples of Conflicts of Interests, such as:

- Having a personal or family relationship with a supplier, customer, or competitor.
- Accepting gifts, hospitality, or benefits that could influence decision-making.
- Using confidential information for personal benefit.

A conflict of interest may put someone in a position where they are tempted to use inside information for personal gain or to benefit someone they know. If that information is used for trading or shared with others, it may result in insider trading.

What happens after I declare a conflict of interest?

The conflict will be reviewed and managed appropriately. This may include putting safeguards in place, removing you from certain decisions, or agreeing other actions to avoid potential influence.

Can conflicts of interest change over time?

Yes. Conflicts can arise as roles, relationships, or circumstances change. You should update your declaration if your situation changes.

Does this apply even if I don't work in investments or finance?

Yes. Employees in underwriting, claims, reinsurance, procurement, IT, or project roles may all have access to information that could be considered inside information.

THIRD PARTY & COUNTERPARTY RISK

The Counterparty & Security function within central SRG Operations manages the onboarding, due diligence, and ongoing oversight of key Third-Party relationships. This function ensures compliance with financial crime regulations, effective risk management, and alignment with regulatory standards across Suppliers and our Trading Partners which consist of Producing Intermediaries, Introducers and Insurer Markets.

Producing Intermediary & Introducer Onboarding

Oversight and management of Terms of Business Agreements with Third-Party Trading Partners, including Producing Intermediaries, and Introducers.

Insurer Market – Security & Onboarding

Oversight and management of Terms of Business Agreements with Insurer Markets, including the evaluation of financial security, regulatory compliance, and ongoing monitoring.

Supplier Management

Oversight of Third-Party providers of goods and services, including due diligence, onboarding, ongoing monitoring, renewals, and contract administration. Formal suppliers are those with ongoing contracts/ agreements. Informal suppliers are those for one-off or ad-hoc services.

PROTECTING INFORMATION & SYSTEMS

3

DATA PROTECTION

As a regulated business, SRG is committed to protecting the privacy and personal data of clients, colleagues, and third parties. Personal data and confidential information must be handled lawfully, fairly, and securely, and only used for legitimate business purposes.

As a team, we all handle personal data daily, therefore, it's essential we always protect it by following the applicable data protection policy.

Our Risk & Compliance team handle queries on Data Protection such as Data Subject Access Requests (DSARs), how data is handled and data retention queries.

For the UK & Ireland, guidance may be found in the Data Protection Policy and for any queries email **DPO@specialistrisk.com**

What does Personal data look like?

Personal data is anything that can be used to identify a living person. This includes obvious details like names and contact information, as well as less direct information such as job titles, dates of birth, customer records, or anything that links back to an individual. Examples include names, email addresses, ID numbers, bank details, health information, and customer policy data.

What is a DSAR and what should I do if I receive a DSAR?

A DSAR is a request from an individual asking for access to the personal data we hold about them. Individuals have a legal right to make these requests. You must escalate it **immediately** to the data protection team. In the UK, as part of our procedures, the DSAR request **form** must be completed. DSARs have strict legal timeframes and must be handled carefully; read the **UK & Ireland DSAR procedure** for more details.

What are my responsibilities when handling personal data?

You must only access and use personal data where there is a legitimate business reason, keep it secure, follow our policies, and report any concerns or data incidents immediately.

What are data retention requirements?

Data retention requirements set out how long we must keep different types of data and when it should be securely deleted. We must not keep personal data for longer than necessary.

Read the **Data Retention policy** for more details.

TYPES OF CONFIDENTIAL INFORMATION

Confidential information can take different forms.

Common examples include:

- **Personal information (PII):** Information that identifies an individual, such as names, contact details, account numbers, national identifiers, and other personal data.
- **Employee information:** Colleague records such as HR files, payroll details, performance information, absence records, and disciplinary matters.
- **Customer and client information:** Customer personal data, account details, transaction data, communications, and service records.
- **Business confidential information:** Commercially sensitive information such as business plans, financial results before release, pricing, contracts, intellectual property, strategy papers, and M&A materials.
- These types of information may then be assigned a classification level based on the sensitivity of the data and the impact if it is lost, shared, or accessed without authorisation.
- Once the information type has been identified, it should be classified according to the level of harm that could arise from unauthorised access, disclosure, alteration, or loss. Typical classification levels are Public, Internal (Private), Confidential, and Restricted (Highly Confidential). These labels indicate the level of protection and handling controls required.

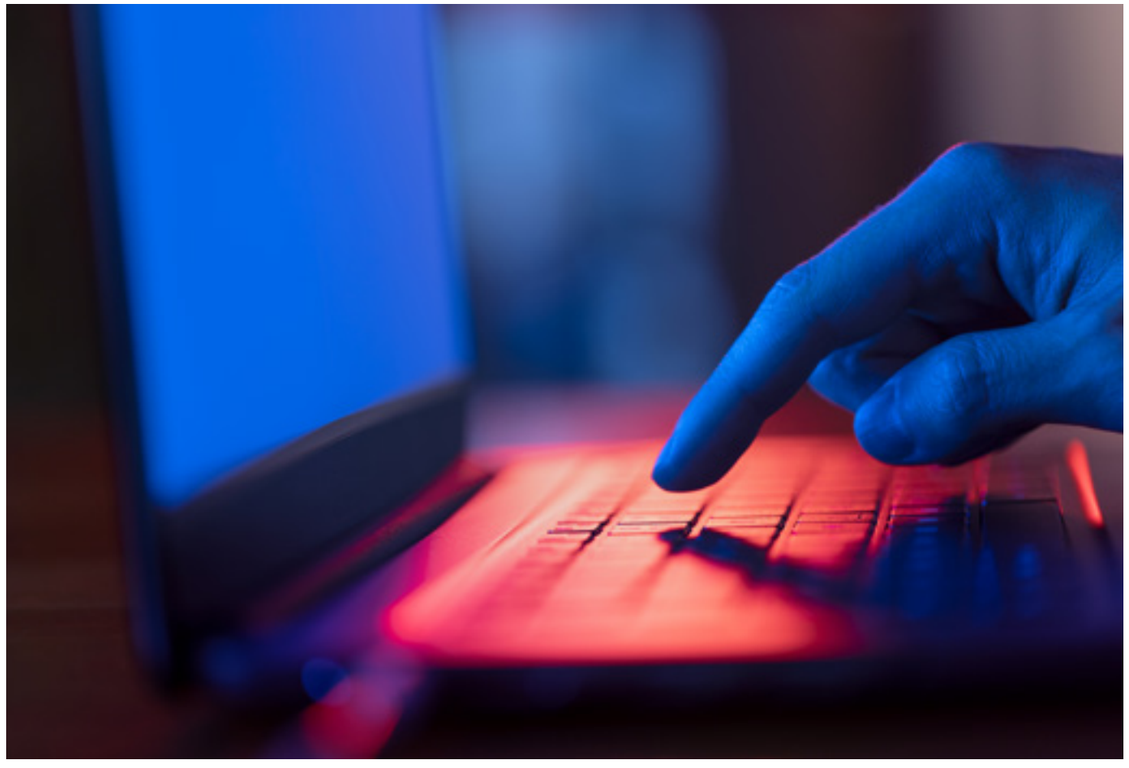
What should I consider before sharing confidential information?

Check the information type, confirm the classification, make sure the recipient has a legitimate need to know, and use the right protection measures for sharing and storage.

What happens if information is classified too low?

It may not receive the controls it needs, which can increase legal, regulatory, operational, and reputational risk.

CYBER SECURITY



Cyber Security is an ever-growing challenge for many businesses, including SRG as we look to protect our information, systems and assets from unauthorised access and misuse.

Every employee has a responsibility to follow security best practices to protect SRG from legal, financial and reputational risks.

Further information can be found in our **Information Security Policy.**

What is Social Engineering?

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information, using trickery, persuasion, and exploiting human tendencies like trust or urgency, rather than technical hacking.

What should I be looking out for?

Social Engineering can take several forms:

Psychological manipulation: Exploiting human behaviour, emotions (fear, curiosity, helpfulness), and social cues to deceive victims.

Exploitation of trust: Attackers often impersonate trusted sources, like IT support or familiar companies, to build rapport and lower defences.

Information gathering: Trying to obtain sensitive data (passwords, bank details) or prompt users to take risky actions, like clicking malicious links.

Broad range of activities: Tactics like phishing (email), SMS (smishing), call (vishing) and in-person methods like following someone into a restricted area.

Sense of urgency: Enable people to identify when this is being used explicitly or surreptitiously.

How can I protect myself and SRG?

There are several actions we can all take:

- Exercise caution when opening emails, links, or attachments, particularly from unknown or unexpected sources.
- Verify requests for sensitive information or payments through appropriate channels.
- Use corporate email and messaging systems responsibly and securely
- Only use corporate email for business purposes.
- Never share your password or multi-factor authentication codes.
- Lock your screen when away from your desk.

For further support you can reach out to **security.support@specialistrisk.com**

RELATIONSHIPS WITH OUR COMMUNITY

4

MODERN SLAVERY

We operate in line with fundamental human rights and have zero tolerance for forced or compulsory labour. Holding someone in slavery or servitude is a criminal offence and SRG does not tolerate any form of slavery or human trafficking.

SRG monitors compliance with its internal Group policies and procedures to ensure that we are conducting business in an ethical and transparent manner. We identify and mitigate risks across a range of areas, including slavery and human trafficking, by integrating these policies and procedures in our decision-making process.

To find out more on how we look to combat Modern Slavery please read our **Modern Slavery Statement.**

What happens if a risk is identified?

Concerns are reviewed and assessed carefully. Where issues are confirmed, we take appropriate action, which may include remediation, corrective action plans, or reconsidering our business relationships.

What are some warning signs of modern slavery?

Warning signs may include:

- Workers appearing fearful, withdrawn, or controlled by others.
- Poor or unsafe working conditions
- Lack of freedom to leave work or change employers.
- Withheld wages, identity documents, or excessive recruitment fees.

VULNERABLE CUSTOMERS

We as an insurance broker have a duty to ensure that vulnerable customers can be accommodated and we avoid any barriers to financial services.

Supporting vulnerable customers is a shared responsibility and is central to acting in line with regulatory expectations and our values.

How do we do this? We have systems and processes in place to support reasonable adjustments for vulnerable customers, alongside training that builds the skills, confidence, and awareness of all colleagues.

For further guidance take a look at our **SRG Vulnerable Customer Policy** applicable to the UK operations.

How does this link to regulatory expectations?

Regulators expect firms to identify vulnerability, respond appropriately, and deliver fair outcomes. Supporting vulnerable customers is a key part of treating customers fairly and acting in line with regulatory codes of conduct.

What if I'm unsure how to support a vulnerable customer?

Seek guidance from your manager or specialist teams. Asking for help ensures customers receive the right support and outcomes.

How should vulnerability be recorded?

Any vulnerability information should be recorded sensitively and in line with data protection requirements and shared only where necessary to support the customer.

ENVIRONMENTAL, SOCIAL & GOVERNANCE (ESG)

As we continue to grow, we embed Environmental, Social, and Governance (ESG) principles into our current operations and these principles are a core pillar in our future growth strategy.

In our London operations, we have implemented processes based on these principles with respect to the suppliers we engage and take an active role in the UK Government's Energy Saving Opportunity Scheme (ESOS).

Additionally, throughout our office portfolio, we have selected products and services with ESG credentials being a key part of the selection process.

Environmental

- Use resources responsibly, minimise waste where possible.
- Be mindful of our environmental impact as we scale operations.
- Ensure ESG forms part of our supplier and product selection process.
- Comply with applicable environmental regulations.
- Seek practical and sustainable choices.

Social

- Create a safe, inclusive, and respectful workplace.
- Treat employees, customers, contractors, and partners fairly and ethically.
- Support wellbeing, diversity and equal opportunity.
- Act responsibly within the communities where we operate.

Governance

- Operate with integrity, transparency, and accountability.
- Implement and manage effective Compliance frameworks.
- Comply with laws, regulations, and internal policies.
- Avoid conflicts of interest and unethical behaviour.
- Protect company and personal data.

HEALTH & SAFETY

SRG is committed to providing a safe and healthy work environment for all our colleagues, contractors, customers, and visitors. We aim to prevent any accidents, injuries, and illnesses that may arise from our work activities.

The responsibility for health and safety lies with everyone in the company. The senior management is accountable for setting the health and safety policy and ensuring its implementation.

The managers and supervisors are responsible for ensuring that all colleagues follow the policy and procedures. All colleagues are responsible for complying with the **policy and procedures** and reporting any health and safety concerns.

To achieve this, we:

- Comply with all relevant health and safety laws and regulations.
- Identify and assess the risks and hazards in our workplace and implement appropriate control measures.
- Provide adequate information, instruction, training, and supervision to our colleagues on health and safety matters.
- Consult and communicate with our employees on health and safety issues.
- Provide sufficient resources, equipment, and facilities to support health and safety.
- Monitor and review our health and safety performance and take corrective actions as needed.
- Continually improve our health and safety management system.

Commitment to a safe and healthy work environment for all colleagues, highlighting:

- Everyone is responsible for reporting hazards and following procedures.
- Mandatory reporting of accidents and near-misses; logged centrally.
- Fire safety: clear exits, drills twice yearly, follow evacuation rules.
- Manual handling: avoid heavy lifting; use equipment; training available.
- DSE guidance: good workstation setup; regular breaks; assessments done.
- Hazardous substances: avoid use unless authorised; cleaners' materials restricted.
- First aid: trained first aiders; equipment checked periodically.

specialistrisk.com

DIFFICULT.
DONE WELL.