Financial Crime Policy:

Anti-Bribery, Corruption & Fraud

Version: 1.0
Classification: Public
Date: 23 March 2026

EirGrid

The Oval, 160 Shelbourne Road, Ballsbridge, Dublin D04 FW28
Telephone: +353 1 677 1700 | www.eirgrid.ie

Contents

1 Policy Overview

1.1 Policy Statement

The EirGrid Financial Crime Policy brings together our existing Anti-Bribery and Corruption (ABC) and Anti-Fraud requirements into a single, consolidated standard. It outlines EirGrid's commitment to conducting its activities with integrity, transparency, and accountability, and to promoting ethical business practices across all operations.

EirGrid seeks to prevent and deter all forms of financial crime, including bribery, corruption, and fraud as defined under the Criminal Justice (Corruption Offences) Act 2018 and the Criminal Justice (Theft and Fraud Offences) Act 2001, as well as related risks such as modern slavery. Financial-crime considerations are embedded within EirGrid's Enterprise Risk Management (ERM) framework. The organisation encourages a culture of responsible conduct, supports the secure reporting of concerns, and takes appropriate action where misconduct is identified.

1.2 Purpose

This policy establishes the controls required to prevent, detect and respond to financial crime risks across our activities, projects, and third-party relationships. It is a core component of EirGrid's governance and resilience framework, integrating with our Codes of Conduct and Protected Disclosures policy.

The purpose of this policy is to:

- Sets out the responsibilities and behaviours we expect to ensure compliance with relevant legislation and our ethical standards.
- Enables the recognition and reporting of suspicions or concerns relating to financial crime, so they can be investigated, and corrective actions taken to protect EirGrid's assets, reputation and integrity.
- Explains how our organisational governance maintains effective accountability and oversight for financial crime risk and compliance.

1.3 What is Financial Crime?

- *Fraud*: It is a dishonest act intended to cause unfair or unlawful loss to another or gain for oneself, including deception, forgery, or embezzlement.
- *Bribery and Corruption*: Incentives or benefits that are offered, promised, or given to secure any commercial, contractual, regulatory, or personal gain, or the abuse of power to influence an action. This can include the improper offering, giving or receiving of gifts, hospitality or endorsements, as well as facilitation payments and kickbacks.
- *Market abuse*: Disclosing confidential, price-sensitive information to a third party outside the normal exercise of employment or professional duties.
- *Money laundering and financing terrorism*: Transforming the proceeds of crime into legitimate money or assets. Terrorist activity may be facilitated or sponsored by the proceeds of money laundering or from other fraudulent activities and may include bypassing sanctions or other controls.
- *Sanctions*: Legally binding restrictive measures targeting specific individuals, entities, sectors, or countries, such as asset freezes, financial prohibitions, trade restrictions, and travel bans; by the United Nations, European Union, United Kingdom, United States, and other countries imposing trade and financial restrictions known as sanctions.
- *Tax evasion*: Illegal practice of not paying or under-payment of taxes; not reporting income, or reporting expenses not legally owed, through deliberate and dishonest conduct.
- *Modern Slavery*: Deprivation of a person's liberty by another to exploit them for personal or commercial gain, whether through slavery, servitude, forced and compulsory labour, and human trafficking

1.4 Who must comply with this Policy?

This policy applies to all persons working for any EirGrid[1] company or on its behalf in any capacity, including employees at all levels, Board Members, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with EirGrid, wherever located. Throughout this Policy document, the terms employee / employees / staff may be read to include all of the above persons.

This policy is not a component of any employee's employment contract or the terms of engagement between EirGrid and its contractors and agents, and we reserve the right to modify it at any time. Nevertheless, adherence to this policy, along with other designated policies, will be a contractual obligation for EirGrid employees, as well as for EirGrid 's contractors and agents.

All consultants, intermediaries, subcontractors, distributors, partners, agents or other third parties engaged by the Group must ensure that they comply with the rules set out in this policy. Both individuals and EirGrid Group Companies can be held legally accountable for the actions of such third parties.

There are no geographical boundaries for the commission of a wrongdoing. Consequently, if the wrongdoing is committed abroad i.e. outside Ireland and Northern Ireland, this Policy still applies irrespective if the wrongdoing would be regarded as an offence in that country.

1.5 Governance Context

This Policy reflects obligations arising under legislation including:

- Ethics in Public Office Act (1995).
- Standards in Public Office Act (2001).
- Criminal Justice Act (2011).
- Companies Act (2014) as amended.
- Regulation of Lobbying Act (2015).
- Criminal Justice (Corruption Offences) Act 2018.
- Criminal Justice (Theft and Fraud Offences) Act 2001
- Public Procurement Policies
- UK Modern Slavery Act (2015).
- Criminal Law (Human Trafficking) Act 2008, as amended by the Criminal Law (Human Trafficking) (Amendment) Act 2013.
- Common Foreign and Security Policy (Article 215 TFEU), as well as in relation to “preventing and combating terrorism and related activities” (Article 75 TFEU)
- Protected Disclosures Act 2014 and Protected Disclosures (Amendment) Act 2022. European Union (Resilience of Critical Entities) Regulations 2024

While financial crime laws in different countries generally reflect similar principles, there are differences, both in the laws themselves and in what is considered best practice in complying with those laws. If you are ever in doubt as to whether an action is appropriate or not, you should seek guidance from your Head of Function or EirGrid’s legal department.

1.6 Related Documents

The following policy documents are related to or impacted by the Policy:

- Directors’ Code of Conduct
- Employee Code of Conduct
- Hospitality, Gifts & Entertainment Policy
- Protected Disclosure Policy
- Vendor Management Framework
- Conflicts & Disclosures of Interest Policy
- Procurement Policy
- Expenses Policy (including Travel & Subsistence)
- Acceptable Usage Policy

EirGrid complies with public-sector governance requirements and ethical obligations applicable to state bodies; this policy supports those obligations and the Board’s control and oversight responsibilities.

[1] The terms “EirGrid” and “EirGrid Group” includes EirGrid plc and all its’ subsidiaries incorporated in the Republic of Ireland. SONI Ltd maintains its own Policy.

2 Financial Crime

Financial crime includes fraud and deception, the misuse of power through bribery and corruption, and the deliberate evasion of tax obligations. Also, business transactions with sanction listed persons or countries and crimes that cause profound social harm, specifically modern slavery and human trafficking, other exploitative practices.

Refer to Appendix 1 for examples of Financial Crime and Appendix 2 for an explanation of key words, abbreviations, acronyms or terms used in the Policy.

Our commitment to combating financial crime is fundamentally integrated into our Enterprise Risk Management (ERM) Framework. The ERM methodology ensures that efforts are not siloed but are embedded into our core business processes, including third-party due diligence, procurement, and financial reporting. By aligning accepted standards with the broader ERM strategy, we maintain a unified defence against ethical risks, protect our corporate reputation, and ensure continuous monitoring for emerging threats in the jurisdictions where we operate.

2.1 Fraud

Fraud is defined as any act where a person dishonestly, with the intent of making a gain or causing a loss, uses deception to induce another to act or refrain from acting. Examples of fraud include specific "red flags" such as expense abuse, payroll fraud (ghost employees), misuse of assets, phishing, ransomware, identity theft, "greenwashing", bid-rigging and collusion. And more examples of fraud ‘red flags' can be found in Appendix 3.

The effective application of the Enterprise Risk Management Framework is one of the measures in place to prevent and/or detect fraud, specifically during:

- Risk Assessments – the exposure to fraud risk should be considered during all risk assessments; and
- Control Identification & Effectiveness –fraud detection/prevention controls should be specifically identified and assessed for operating effectiveness.

2.2 Anti-Bribery and Corruption

EirGrid prohibits, without exception, offering, promising, giving, requesting, agreeing to receive, or accepting any undue advantage—directly or indirectly, including through third parties—to improperly influence any act or decision or to gain an improper advantage. This prohibition applies to interactions with public officials and private parties alike, in Ireland and abroad. EirGrid is dedicated to upholding anti-bribery measures, fostering a culture of integrity, and guaranteeing that issues can be reported securely and examined fairly.

2.3 Market Abuse

EirGrid prohibits all forms of market abuse, including insider trading and market manipulation, in line with the EU Regulation on Wholesale Energy Market Integrity and Transparency (REMIT). Market abuse includes using or sharing non-public inside information or engaging in behaviour that gives false or misleading signals about supply, demand, or prices in wholesale energy markets.

Inside information must be handled confidentially and disclosed promptly where REMIT requires it, ensuring transparency and fair market conditions. EirGrid will monitor market behaviour and fully cooperate with CRU and ACER in any assessment or investigation of suspected market abuse, as part of the EU-wide monitoring and enforcement framework.

Employees must escalate any potential market-abuse concerns immediately, in accordance with the Raising a Concern section, for assessment and regulatory reporting where required.

2.4 Sanctions

It is EirGrid's policy to comply with all applicable sanctions. Compliance with these laws is essential to the EirGrid Group's well-being and failure to comply could result in civil and criminal penalties, as well as damaging publicity. Business activities with or involving sanctioned persons or sanctioned countries, defined separately, could also conflict with obligations under the EirGrid Group's financing agreements.

Sanctions compliance is the process of ensuring that an entity does not deal with listed persons by directly or indirectly providing "funds" or "economic resources" (including goods, services, or property) to any individual or entity on an official sanctions list or by exporting or importing goods to sanctioned regions (e.g., specific territories in Ukraine, Russia, or Belarus). Or bypass restrictions by engaging in activities intended to circumvent these controls, such as using intermediary shell companies.

2.5 Modern Slavery

The Board, the Chief Executive and the executive team are committed to upholding and respecting all aspects of human rights including ensuring that slavery and human trafficking is not taking place in our business or any of our supply chains. EirGrid plc's Modern Slavery & Human Trafficking Statement summarises our approach to combatting modern slavery in our business and supply chains in accordance with the UK Modern Slavery Act 2015.

EirGrid's modern slavery approach, policies and codes include the following provisions and/or address the following issues:

- The business adheres to local, national, and international laws.
- Workers have the freedom to terminate their employment.
- Workers enjoy freedom of movement.
- There are freedom of association and the right to collective bargaining.
- Any threat of violence, harassment, and intimidation is prohibited.
- The use of worker-paid recruitment fees, including in the migrant worker's country of origin, is prohibited.
- Workers are provided with free, comprehensive, and accurate information regarding their rights and the conditions of their recruitment and employment in writing, in a language they understand.
- Compulsory overtime is prohibited.
- Child labour is prohibited.
- Discrimination is prohibited.
- Confiscation of workers' original identification documents is prohibited.
- Access to remedy, compensation, and justice for survivors of modern slavery is provided.
- Workers are informed, in a form and language they understand, of hazards to which they may be exposed, including exposure to toxic chemicals and their effects.

For the policies and practices to have the desired effect, it is supported through effective communications and where appropriate, training, resourcing, and collaboration of effort by appropriately skilled employees.

The aforementioned is contained in EirGrid's internal operating policies and are relevant to modern slavery. For guidance or support to adhere to the obligations above, employees can contact Governance, Risk and Compliance for guidance. Also refer to the Employee Code of Conduct, recruitment, and procurement practices.

3 Conduct Expectations

3.1 Prohibited & Restricted Conduct

EirGrid is opposed to Financial Crime in all forms. The following practices are prohibited, strictly prohibited or subject to defined restrictions to ensure compliance with legal, regulatory, ethical, and organisational standards. Definitions for restricted and strictly prohibited practices can be found in Appendix 2.

Topic	Approach	Practices
(i) **Bribery and Improper Influence**	Strictly Prohibited	Employees must never: - Offer, promise, give, request, or accept any financial or non-financial advantage intended to improperly influence a decision, obtain an undue advantage, or reward improper performance. - Engage in indirect bribery via third parties (e.g., consultants, intermediaries, agents, partners, subcontractors). - Manipulate procurement, tendering, permit acquisition, land access, stakeholder engagement, or regulatory processes through improper incentives. - Use personal relationships or confidential information to gain an unfair advantage for themselves or for EirGrid. This applies to all interactions with both public officials and private-sector individuals.
(ii) **Facilitation Payments**	Strictly Prohibited	EirGrid prohibits all facilitation payments—small, unofficial payments made to secure or expedite routine governmental or administrative actions. This prohibition applies: - Regardless of local customs or expectations. - Even if such payments appear to be “minor” or “customary”. - Whether made directly or indirectly via intermediaries. **Facilitation Payments in Life-Safety Situations**: The only exception is where a person faces an immediate threat to life, safety, or liberty. Such incidents must be reported to the Executive Committee and Head of Governance, Risk & Compliance as soon as practicable.
(iii) **Gifts, Hospitality, Entertainment and Travel**	Restricted	EirGrid recognises that modest and appropriate gifts or hospitality may be part of legitimate business engagement. However, they can create risks if not properly controlled. Strict rules apply for gifts, hospitality, entertainment or travel must never be offered or accepted if they: - Could improperly influence, or appear to influence, a business decision. - Create a sense of obligation or expectation of favourable treatment. - Occur during live tenders, competitive bidding, contract renewal, or regulatory decisions.

		- Involve cash or cash-equivalents (vouchers, gift cards, loans). - Are provided to or received from Public Officials without explicit prior approval. Refer to the Hospitality, Gifts & Entertainment Policy for further details including thresholds, approvals and reporting.
***(iv)* Political Contributions**	Prohibited	To avoid any perception of political influence: - EirGrid funds, resources, facilities, or staff time may not be used to support political parties, campaigns, candidates, or political events. - Personal political activity must be kept strictly separate from work and must not imply company endorsement. - Indirect political support through sponsorships, donations, third parties, or disguised contributions is prohibited.
***(v)* Charitable Donations, Sponsorships and Community Contributions**	Restricted	EirGrid supports legitimate charitable and community activities. However, such contributions must not be used to improperly influence decisions. Restricted unless approved; contributions must: - Be aligned with EirGrid's corporate social responsibility strategy. - Undergo due diligence on beneficiary organisations. - Be transparent, documented, and approved via defined processes. - Not be linked to any pending decision (e.g., planning, land access, procurement awards). - Not benefit individuals personally or indirectly.
***(vii)* Employment, Internships and Procurement-Related Favouritism**	Strictly Prohibited	Employees must not offer or accept: - Preferential hiring, internships, or work placements in exchange for favourable treatment. - Procurement bias (e.g., tailoring specifications, sharing confidential information, insider access). - Undisclosed conflicts of interest affecting recruitment, project decisions, or supplier selection. All recruitment, procurement, and engagement decisions must follow transparent, merit-based processes.
***(viii)* Conflict of Interest Mismanagement**	Prohibited	Conflicts of interest (actual, potential, or perceived) must be: - Declared immediately through formal channels. - Managed in accordance with the EirGrid Conflicts & Disclosures of Interest Policy and Code(s) of Conduct. - Avoided where they compromise or appear to compromise objectivity, fairness, or integrity. Examples include financial interests in suppliers, close personal relationships in procurement chains, outside employment, or advisory roles that intersect with EirGrid's operations.

***(ix)* Misuse of Confidential Commercial, or Insider Information**	Strictly Prohibited	It is prohibited to: - Share non-public information for personal gain or for the benefit of a third party. - Use insider knowledge to influence tenders, land acquisitions, market positions, or contract negotiations. - Withhold relevant information in order to manipulate decisions or outcomes.
***(x)* Manipulation of Records, Documentation, and Financial Controls**	Strictly Prohibited	Employees must not: - Create or maintain false, misleading, or incomplete records. - Conceal payments, benefits, services, or transactions. - Circumvent financial controls, approval pathways, or segregation-of-duties requirements. - Operate "off-book" accounts or side arrangements. Accurate record-keeping is essential for transparency and auditability.
***(xi)* Use of Third Parties, Intermediaries or Consultants for Improper Purposes**	Prohibited	EirGrid prohibits the use of third parties to perform actions that would be prohibited if done directly. Examples include: - Concealing the origin of payments. - Channelling inappropriate benefits through consultants or agents. - Using intermediaries to influence public officials. - Paying excessive commissions without clear justification. - Engaging "fixers," "expediters," or "agents" with opaque services. All third-party engagements must pass due diligence and be subject to contract clauses prohibiting bribery.
***(xii)* Modern Slavery**	Strictly Prohibited	EirGrid strictly prohibits all forms of modern slavery, human trafficking, forced or compulsory labour, and servitude. - Employees and suppliers must not engage in, benefit from, or ignore any exploitative labour practices, including coercion, restriction of movement, deceptive recruitment, or unsafe or abusive working conditions. - EirGrid will only work with suppliers who can demonstrate ethical labour practices, and any suspected instance must be reported immediately through established reporting channels.
***(xiii)* Retaliation Against Individuals Who Raise Concerns**	Strictly Prohibited	EirGrid prohibits any form of retaliation—direct or indirect—against persons who: - Report suspected wrongdoing in good faith. - Cooperate with investigations. - Decline to participate in corrupt behaviour. Any retaliation will itself be treated as a serious breach.
***(xiv)* Any Attempt to Circumvent or Obstruct Investigations**	Strictly Prohibited	This includes: - Destroying, altering, or concealing relevant documents. - Influencing witnesses or investigators. - Providing false or incomplete information. - Attempting to stop others from reporting concerns.

Appendix 1 presents more examples of financial crime prohibited by this policy.

3.2 Gifts, Hospitality, Expenses, and Promotional Activities

Not all payments or the provision of gifts and entertainment are bribes. EirGrid recognises the legitimate role of reasonable and proportionate hospitality and promotional expenditures to build relationships. However, all such benefits must not, and must not be perceived to, improperly influence business decisions.

In particular, reasonable (relatively low value) bona fide gifts and hospitality are permissible if they are given or received in connection with EirGrid's services. You may never receive a gift or hospitality from any third party as a reward for unlawful or improper action or giving something in return. **EirGrid's Hospitality, Gifts & Entertainment Policy** outlines the guidelines and regulations pertaining to these matters.

Donations and sponsorships must be transparent, pre-approved, recorded, and never made to influence an official action or decision.

Whether a particular action or payment violates this Policy (and the law) may depend on the facts and circumstances in which it was done. While it is impractical to anticipate all of the possible scenarios that should raise red flags or corruption concerns, Appendix 3 presents a list of possible red flags which may raise concerns under various anti-bribery, anti-corruption, and modern slavery/human trafficking laws.

3.3 Modern Slavery Guidelines

Employees must adhere to the following guidelines:

Compliance	- Labour Standards: You are required to ensure that all business activities under your control comply with international labour standards and ILO core conventions[2]. You must not authorise any work that violates these standards. - Recruitment Compliance: You must adhere to the EirGrid Recruitment Policy in every hire. You are prohibited from using recruiters or third parties that do not meet the organisation's mandatory vetting criteria for subsidiaries and suppliers.
Oversight	- Responsible Procurement Oversight: If you are involved in purchasing, you must strictly follow the Procurement Policy. You are personally responsible for assessing how your specific buying decisions or deadline pressures might increase the risk of modern slavery.
Responsible business practices	- Accurate Costing and Budgeting: When calculating production or sourcing expenses, you must include legal and full labour costs. You are strictly prohibited from approving budgets that rely on artificially low costs indicative of slave or bonded labour. - Responsible Contract Termination: You must follow the Escalation and Exit Process when addressing modern slavery. You are responsible for documenting all corrective efforts and ensuring that a contract exit does not cause further harm to vulnerable workers. - Supplier Support: Managers overseeing external partners must provide support and guidance to suppliers to ensure they meet their remedial obligations when modern slavery is identified.

[2] ILO Core Conventions (also known as Fundamental Conventions) are a set of 10 International Labour Organization treaties covering fundamental principles and rights at work, including freedom of association, collective bargaining, elimination of forced/child labour, discrimination, and safe working environments. They are legally binding upon ratification and form the basis of international labour standards, promoting social justice and dignity.

Reporting	- Mandatory Reporting (Protected Disclosures): You have a duty to report any suspected modern slavery or labour violations via the Protected Disclosures mechanism. You must facilitate an environment where workers can report concerns without fear of retaliation.
Safeguards	- Due Diligence and Investigation: Designated officers must actively investigate and conduct ongoing due diligence on modern slavery risks within their specific departments and supply chains. Failure to oversee these standards constitutes a breach of duty. - Remedy and Safeguarding: You are obligated to support access to remedy for victims identified within your operations. You must take active measures to safeguard victims from further harm or victimisation during the remediation process.

4 Risk Management

Our approach to risk management recognises that different activities carry different levels of exposure. Rather than applying a uniform model, we focus attention and resources on areas where financial-crime risks are inherently higher, for example: high-value procurement, complex third-party engagements, or activities in jurisdictions where transparency challenges are more prevalent.

EirGrid's risk-based approach is supported by periodic assessments of financial-crime risks, proportionate due diligence on third parties, and internal controls designed to highlight unusual or inconsistent activity at an early stage. While specialist teams provide guidance and oversight, all employees are expected to remain aware of the risks relevant to their roles and to follow established processes so that residual risks remain within EirGrid's overall governance and ethical expectations.

4.1 Financial Crime Prevention Measures

Several preventative measures exist and are embedded within working practices throughout our operations. Measures in place include:

- **Culture & Governance** – A strong culture of integrity aligned with our governance obligations and supported by training, values, policies e.g. Employee Code of Conduct, Protected Disclosures Policy and associated ethics policies and procedures.
- **Risk Assessments** – Annual and event-driven financial-crime risk assessments covering internal and external threats, including fraud, bribery/corruption, sanctions exposure, insider-information risks, and third-party vulnerabilities; a targeted fraud risk **review** of key processes is conducted by Internal Audit or the Governance, Risk & Compliance function.
- **Process and Transaction Controls**
    - **Segregation of Duties**: Ensure no single individual has end-to-end control over sensitive processes, such as adding new vendors and approving payments.
    - **Authorisation Limits**: Expenditure above approved amounts requires written approval as per the internal rules and the EirGrid Expense Policy.
    - **Device & Software Security**: Keep all accounting software updated with the latest security patches. Use a firewall and reputable anti-virus solutions on all devices.
    - **Multi-Factor Authentication (MFA)**: Mandate MFA (passwords plus biometric or mobile app codes) for most internal systems.
- **Third Party Due Diligence**: Verification of all new suppliers and regular reviews of existing ones to prevent "ghost" vendors.

- **Awareness** – Training/Awareness Campaigns e.g. Cyber Security Briefings, Security Awareness Campaigns, focused training for specific high-risk areas and regular reporting of fraud-related incidents to the Executive Management Team and Board; and
- **Lessons Learned** – using actual examples of verified and/or attempted financial crime within/against EirGrid to enhance prevention measures and awareness.
- **Random Internal Audits**: Conduct unscheduled reviews of high-risk areas like account payments, tender processes, and inventory management to create a deterrent effect.

4.2 Third Party Due Diligence

All employees must be vigilant in monitoring the activities of third parties on an ongoing basis. Over-stated, false, or inappropriately described payment requests, unusual or overly generous subcontracts, unusual or incomplete documentation and refusals or failures to provide requested documentation may be signs of bribes by third parties.

We will not engage or retain any third party unless we are satisfied—through risk based due diligence—that they share our standards against Financial Crime. This includes:

- Risk based screening before appointment (ownership/beneficial ownership, sanctions, Politically Exposed Person, adverse media, prior enforcement).
- Contractual Anti-Bribery and Corruption clauses (no bribery warranties, audit/termination rights, certification of training/controls).
- Ongoing monitoring proportionate to risk (e.g., periodic re screening; red flag triggers).

4.3 Record Management

EirGrid maintains accurate, complete and timely records that fairly reflect transactions. We prohibit off book accounts and misleading records. Finance and operational controls (segregation of duties, delegated authority, verification, supporting documentation) apply to both financial and non-financial processes (e.g., permits, land access, community funds).

EirGrid seeks to prevent financial crime by filing and maintaining clear and verifiable:

- financial records for all expenses and receipts including those claimed under the Expenses Policy, and
- accounts, invoices, memoranda and other documents and records relating to dealings with third parties (e.g., clients, suppliers, business partners, and government officials).

Fraud, Anti-Bribery and Corruption relevant records (e.g., due diligence files, approvals, registers, training logs, investigations) must be retained according to EirGrid's retention schedule and any statutory requirements and be readily retrievable for audit/regulatory review.

4.4 Risk Assessment

To manage the threat of financial crime, EirGrid adopts a proactive, risk-based approach focused on identifying, assessing, and mitigating vulnerabilities within our specific operations and supply chains. We assess and review operational risks associated with financial crime across our operations on a regular basis through the risk identification and assessment process as outlined in the Enterprise Risk Management Framework (ERMF). All employees and third parties are expected to support this approach by remaining vigilant, reporting concerns promptly and adhering to all internal policies and legal obligations. The ERMF ensures that emerging risks are identified early and that effective controls remain in place to protect EirGrid's integrity.

4.5 Financial Crime Detection Measures

Furthermore, detection measures are embedded within our systems and working practices including:

- Automated system audit trails.
- Supervisory reviews of transactions.
- Data analytics e.g. abnormal values.
- “Right to Audit” clauses embedded in third party contracts.
- Speak up and protected disclosure channels.
- Management oversight controls; and
- Internal and External audit processes.

5 Raising a Concern

5.1 Required Actions for Reporting

All employees and contractors and/or third parties have a duty to report any suspected or actual incident of financial crime that they become aware of at the earliest possible opportunity. In the case of EirGrid employees, any such incident should be reported in the first instance:

- To the employee’s Head of Function; or
- To the Group Head of Internal Audit; or via
- EirGrid’s Protected Disclosures Policy and procedures.

In the case of contractors and/or third parties, such incidents should be reported to the relevant Head of Function or via EirGrid’s Protected Disclosures channel(s) or to the Governance Risk and Compliance (GRC) function.

Discovery of a potential financial crime incident	
Required Actions (The "Dos")	***Prohibited Actions (The "Don’ts")***
***Immediate Reporting**: Notify the Head of Function, GRC or report using the Protected Disclosure Tool as soon as a concern arises.*	***Do Not Investigate**: Refrain from conducting your own enquiries, accessing restricted files, or "testing" systems.*
***Preservation of Evidence**: Secure all relevant documentation, emails, and digital records in their original state.*	***Maintain Confidentiality**: Do not discuss the matter with colleagues or external parties to avoid "tipping off" or compromising the case.*
***Factual Accuracy**: Provide a comprehensive account of all known facts and objective observations.*	***No Confrontation**: Avoid contacting or confronting the individual(s) suspected of the activity, as this may jeopardize personal safety and legal proceedings.*

5.1.1 Protection

EirGrid is committed to ensuring that all parties to whom this policy applies can raise a concern relating to financial crime or suspicions of financial crime without fear of victimisation and that the strictest confidence will be maintained. For further information you should consult the Protected Disclosure Policy.

5.1.2 Confidentiality

EirGrid treats all information received confidentially. Investigation details will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect EirGrid from civil liability.

5.2 Investigations Process

EirGrid commits to investigate all financial crime that are discovered or suspected. Every case of attempted or suspected financial crime will be investigated and dealt with appropriately without regard to the position held or length of service of the individual(s) concerned, or their relationship to EirGrid.

The Head of Internal Audit has the primary responsibility for the co-ordination of investigation of all suspected financial crime acts, as defined in the policy. The Head of Internal Audit shall liaise with key stakeholders, as appropriate, including but not limited to: Head of Governance, Risk & Compliance, Head of Group Legal Services or relevant executive(s), in order to conduct an initial investigation. The investigation will be conducted by appropriately skilled person(s), in line with EirGrid's Financial Crime Response Process. Post conclusion of the initial investigation the Head of Internal Audit will confirm next steps of the financial crime investigation to the Chief Risk Officer role holder.

No person should attempt to conduct their own investigations.

The Head of Governance, Risk & Compliance reports all incidents of financial crime on a quarterly basis to the Executive Risk & Compliance Committee and the Audit & Risk Committee.

The investigation steps include the following:

- **Preliminary Scoping**: Conduct an initial review to determine if a full investigation is required.
- **Investigation**: Appoint an investigation team (internally or external experts) to gather evidence while maintaining due process.
- **Law Enforcement**: Notify An Garda Síochána where a criminal offence is suspected.
- **Recovery**: Commit to pursuing civil action to recover any lost funds.

6 Responsibilities & Implementation

6.1 Roles & Responsibilities

The key roles and responsibilities in relation to this Policy are as follows:

All Employees & Workers	- Have a duty act with integrity and to immediately report any suspected or discovered wrongdoing. - Familiarise themselves with this Policy, ensure adherence, aid in the effective execution of this Policy. - Participate in financial crime training programmes to comply with related policies, including specific training as part of their induction process. - Cooperate in investigations, if requested.
Heads of Functions	- Operate and maintain an effective governance to promote the prevention, detection and investigation of wrongdoing. - Consider exposure to financial crime risk and implement initiatives to enhance risk management effectiveness. - Take day-to-day operational responsibility for the implementation of this Policy. - Ensure that adequate and suitable resources are allocated to implement and uphold this Policy, which includes training and awareness programmes, so that employees are informed about the steps to take if they come across any instances of wrongdoing. - Maintain internal systems of control to comply with sanctions or restrictions on activities with respect to targeted individuals, countries, governments, or entities

	- Encourage openness and transparency, fostering an environment that is supportive of employees who raise concerns. - Ensure that all employees under their responsibility are informed about the stipulations of this Policy and the associated risks within their business unit; and - Report incidents of wrongdoing and support the investigation of those incidents.

Governance, Risk & Compliance	- The Head of Governance, Risk and Compliance maintain oversight of the Financial Crime Policy and procedures and the associated compliance and risk frameworks in relation to their application.
	- Ensure arrangements exist for training and ongoing awareness and guidance on financial crime, including.
	  ○ Annually inform all employees about the Policy.
	  ○ Introduce all new employees to the Policy during the induction process.
	- Heads of Functions will ensure that all accountable employees are specifically aware of the financial crime risks unique to their business unit or function.
	- Quarterly report to the Executive Risk & Compliance Committee and Audit and Risk Committee on financial crime incidents.

People and Capabilities	- Conduct thorough background checks and screenings to confirm that, to the best of our knowledge, our employees and those acting on our behalf possess the necessary work rights, and that none of our employees or representatives are sanctioned individuals or have participated in financial crimes.
Board	- Approve the Policy. - Define the EirGrid Group's ethical climate. - Responsible for the internal control environment, overseeing risk management framework and determination of this Policy. - Audit and Risk Committee reviews the effectiveness of internal controls and oversees the internal audit plan.
Executive Management Team	- Communicate a clear commitment to this Policy through leading by example while facilitating a culture of openness and respect that supports the disclosure of wrongdoing. - Accountable for implementation and resourcing. - Embed controls in business processes. - Review the procedures for preventing and detecting these risks and receive reports on any non-compliance.
Internal Audit	- The Head of Internal Audit provides assurance over the effectiveness of the internal control environment, including anti-fraud measures, independently assessing the governance framework in place for managing and detecting instances of financial crime; and incorporating fraud assessments into individual audit reviews. - The Head of Internal Audit is responsible for agreeing the terms of reference of and appointing investigators for, investigating breaches of this Policy and for providing independent oversight of all investigations undertaken. - Mandatory Auditor Reporting: Under Section 393 of the Companies Act 2014, the Company's statutory auditors are legally required to report to the CEA if they have reasonable grounds to believe a Category 1 or 2 offence (e.g., fraudulent trading, falsification of records) has been committed.
EirGrid	- EirGrid will not obstruct, and will fully cooperate with, any investigation conducted by the Corporate Enforcement Authority (CEA). This includes providing access to books, documents, and records as required by law.

6.2 Policy Violations

All credible allegations will be assessed and, where appropriate, investigated under our investigation procedures. Substantiated violations may result in disciplinary action up to and including dismissal, contract termination, and referrals to An Garda Síochána, the Director of Public Prosecutions, or other authorities.

Enforcement

Any individual who is under investigation for suspected or discovered wrongdoing may be suspended, pending the outcome of the investigation.

Where the allegations are substantiated, disciplinary action, up to and including termination of employment may be taken.

Where the allegations are substantiated, any other party to whom this policy applies may have their contract with EirGrid terminated and/or appropriate action may be taken against the individual(s) concerned, and legal redress may be sought.

EirGrid is obliged under statute to report suspected criminal activity to An Garda Síochána. Furthermore, in accordance with the Companies Act 2014, EirGrid acknowledges the statutory role of the Corporate Enforcement Authority (CEA) in investigating breaches of company law.

Implications of policy non-compliance

Any breach of this policy will be treated as serious misconduct and may result in disciplinary action, and EirGrid reserves the right to seek criminal prosecution and civil recovery of losses.

Non-compliance by EirGrid employees may be treated as a disciplinary matter. Non-compliance by any other party (e.g. broader definition of workers) to whom it applies, may result in a recommendation to terminate their contract with EirGrid or terminate the engagement of the individual(s), within that contracting entity, found to be in breach of the policy.

In the case of either of the above, EirGrid may also take action to recover any losses incurred, which may include the issuing of civil and/or criminal proceedings against the employee / contractor and/or other individual or company concerned.

6.3 Training & Awareness

Consistent with the expectations set out in the Code of Practice for the Governance of State Bodies (2016), EirGrid aims to provide induction and periodic refresher training to help employees, management, and Board members understand and recognise key financial crime risks, including fraud, bribery, and sanctions. Training will be scaled to the needs of different roles and will support awareness of good governance and responsible conduct. EirGrid will seek to maintain appropriate records of training activity to support oversight and continuous improvement.

Refer again to section 6.1 on Roles and Responsibilities for further details.

6.4 Policy Review

This Policy shall be reviewed by the Head of Governance, Risk & Compliance and approved by the EirGrid plc Board at least every two years or following significant legislative changes.

This policy has been updated in line with the EU Corporate Sustainability Reporting Directive (CSRD) and as such recognises the specific risk of Bribery and Corruption that certain functions within the organisation are exposed to. This policy defines these at-risk functions as any role or activity within the Organisation that, due to its responsibilities, decision-making authority, or interactions with public officials or third parties, is exposed to an increased likelihood of improper influence, bribery, or corrupt practices.

7 Appendices

Appendix 1: Financial Crime Examples

Bribery & Corruption

Any attempt to engage in any of the below activities or to conceal or destroy information relating to any of the above.

EMPLOYEE	• Giving of cash or a gift, or some other form of consideration e.g. a hotel voucher, or other advantage to a person knowing that it will be used to facilitate an offence. • Accepting gifts or other rewards in return for sharing confidential information with a person outside the organisation. • Corruptly creating or using a document (which includes documents in electronic format and emails and texts held electronically on devices such as smartphones) knowing or believing it to contain a false or misleading statement with the intention of inducing another person to do an act in relation to his/her office, employment, position or business to the prejudice of that other person. • Threatening harm to a person with the intention of corruptly influencing that person or another person to do an act in relation to that person's office employment, position or business. • Stealing/theft/embezzlement of money and/or goods belonging to EirGrid or others. • Accepting a gift or hospitality during any commercial negotiations or tender process, if this could be perceived as intended or likely to influence the outcome.

Fraud

		Internal	External
EMPLOYEE	• Over-claiming expenses (falsified transactions and mileage)	✓	
	• Unrecorded holiday/sick leave	✓	
	• Fabricated receipts	✓	
	• Entertainment without legitimate business purpose	✓	
	• Fraudulent use of office resources – e.g. running a private business with official assets	✓	
	• Theft of cash/assets	✓	
	• Payroll (overtime, ghost employees)	✓	
	• Unauthorised use of corporate credit card	✓	
	• False CVs: Providing false qualifications or non-existent prior work experience during the recruitment process.	✓ ✓	✓ ✓
CYBERCRIME	• Denial of Service Attacks		✓
	• Sabotage	✓	✓
	• Ransomware		✓
	• Bank Transfer (Wire) Fraud	✓	✓
	• Identity Theft / Personal Data Harvesting	✓ ✓	✓ ✓

	• File Sharing • Hacking • Viruses • Phishing/Vishing		✓ ✓ ✓
PROCUREMENT	• Bribes, Kickbacks, Bid-Rigging • False statements in obtaining contracts • Substandard materials • Fraudulent testing or false quality assurance representations • Failure to comply with contract specifications • Inflated bills for goods or services • False cost or pricing data. • Fake suppliers / shell company schemes	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
ACCOUNTING	• Writing off recoverable assets or debts • Unauthorised transactions • Transactions (expenditure/receipts/deposits) recorded for incorrect sum • Embezzlement • Deliberate/Incorrect treatment of Accounts Payable & Receivable • Fake Suppliers • Personal Purchases • Creating fictitious employees on the payroll to divert salary payments to the fraudster's own bank account.	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	 ✓ ✓
FINANCIAL MISSTATEMENT	• False recognition of costs/revenues • Deliberate/Incorrect classification of costs/revenues • Incorrect presentation • Misleading disclosures	✓ ✓ ✓ ✓	

Appendix 2: Definitions & Abbreviations

Key Abbreviations

- **ABC**: Anti-Bribery and Corruption / Anti-Bribery and Anti-Corruption.
- **ACER:** The European Union Agency for the Cooperation of Energy Regulators.
- **CEA:** The Corporate Enforcement Authority is the independent statutory agency responsible for the general promotion of compliance with company law and the investigation of suspected breaches. It replaced the Office of the Director of Corporate Enforcement (ODCE), taking over all its previous functions. The CEA's mandate is largely derived from the Companies Act 2014, with its powers further clarified by the Companies (Corporate Enforcement Authority) Act 2021.
- **CJCOA**: Criminal Justice (Corruption Offences) Act 2018 (the primary Irish legislation).
- **CRU:** The Commission for Regulation of Utilities.
- **GDPR:** General Data Protection Regulation, often relevant when data breaches constitute fraud.
- **ILO:** International Labour Organization; the UN agency that sets international labour standards.
- **PD:** Protected Disclosures also called whistleblowing or reporting on potential fraud under Irish law.
- **PDA**: Protected Disclosures Act 2014, the primary legislation governing whistleblowing.
- **REMIT:** Regulation on Wholesale Energy Market Integrity and Transparency.
- **SOP**: Standard Operating Procedure (often used for due diligence and reporting workflows).

Essential Definitions

- **Attempted Fraud**: Acts where the perpetrator intended to commit fraud but failed to achieve the desired gain or loss.
- **Bribery**: Offering, promising, giving, requesting, or accepting any gift, consideration, or advantage as an inducement or reward for an act related to a person's office, employment, or business.
- **Collusion**: Cooperation between two or more individuals (internal or external) to commit a fraudulent act.
- **Corruption**: The misuse of entrusted power for private gain, including "active" (offering) and "passive" (accepting) forms.
- **Deception:** Intentionally creating a false impression (including regarding the law or one's intentions) to induce someone to act.
- **Dishonestly**: Acting without a claim of right made in good faith.
- **Facilitation Payments**: Small, unofficial payments made to secure or speed up a routine or necessary action (e.g., government permits). These are strictly prohibited under Irish law.
- **Financial Statement Fraud**: Deliberate misrepresentation of financial results.
- **Forced Labour**: All work or service exacted from any person under the menace of any penalty and for which the person has not offered themselves voluntarily.

- **Fraud**: An intentional act of deceit, or failure to disclose information, designed to gain a personal or third-party advantage, or to cause loss to another.
- **Gain / Loss**: In Irish law, these refer exclusively to money or other property, whether the impact is permanent or temporary.
- **Human Trafficking**: The recruitment, transportation, or harbouring of persons through force, fraud, or deception for the purpose of exploitation.
- **Misappropriation of Assets**: Theft or misuse of an organization's resources (e.g., equipment, cash, intellectual property).
- **Modern Slavery**: An umbrella term for practices such as forced labour, debt bondage, and human trafficking where individuals are exploited for personal or commercial gain.
- **Prohibited practices**" (when not labelled as "strictly prohibited") generally refer to conduct that is forbidden by company rules but may have nuanced exceptions or specific thresholds that differentiate them from zero-tolerance "strictly prohibited" acts like direct cash bribery. Prohibited practices include (i) hospitality during sensitive periods; (ii) political contributions; facilitation payments in life-safety situations; or (iii) conflicts of interest etc.
- **Public Official**: Includes any person holding a legislative, administrative, or judicial office (elected or appointed), and employees of public bodies or international organisations.
- A **sanctions list** is an official register—maintained by a government or international body—identifying specific individuals, groups, entities, or vessels that are subject to legal restrictions. Being "**sanctioned**" means they are subject to legal prohibitions aimed at curtailing their activities or influencing their behaviour in response to violations of international law, such as terrorism, human rights abuses, or military aggression.
- **Sanctioned country** is a nation or territory subject to official restrictions imposed by international bodies (such as the UN or EU) or national governments. These measures are used as a non-military tool to influence a country's behaviour, respond to human rights violations, or deter aggression and terrorism.
- **Sanctioned persons** is an individual, entity, or body that has been specifically listed under international restrictive measures.
- **Strictly prohibited practices** refer to specific illegal or unethical actions that an organisation refuses to tolerate under any circumstances. These practices are primarily governed by the Criminal Justice (Corruption Offences) Act 2018.
- **Subject to defined restrictions practices** refers to business activities that are legal and acceptable only when they stay within specific, pre-approved limits. Unlike "strictly prohibited" actions (like cash bribes), these practices are recognized as legitimate parts of professional networking, provided they do not cross into "improper performance".
- **Trading in Influence**: Corruptly offering or accepting benefits to induce a person to exert improper influence over an Irish or foreign official.
- **Wrongdoing**: A broad term used in many local policies to collectively describe any unlawful or dishonest activity, malpractice or impropriety within the workplace including but not limited to fraud, bribery, and corruption.

Appendix 3: Financial Crime Red Flags

Bribery & Corruption	
A third-party(ies)	• Engages in, or has been accused of engaging in, improper business practices. • Demands lavish entertainment or gifts before commencing or continuing contractual negotiations or provision of services. • Has a reputation for paying bribes or requiring that bribes be paid to them or has a reputation for having a "special relationship" with foreign government officials. • Insists on receiving a commission or fee payment before committing to sign up to a contract with us or conducting a government function or process for us. • Insists on the use of side letters or refuses to put terms agreed in writing. • Requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made. • Request that payment is made to a country or geographic location different from where the third-party resides or conducts business. • Request an unexpected additional fee or commission to "facilitate" a service. • Requests that a payment is made to "overlook" potential legal violations. • Requests that you provide employment or some other advantage to a friend or relative. • Request or requires the use of an agent, intermediary, consultant, distributor, or supplier that is not typically used by or known to us. • Who refuse to provide transparency regarding their own subcontractors or ownership structures.
An employee(s)	• Insistence on dealing with a particular service provider/supplier/bank account him/herself, or insistence of a service provider/supplier on dealing only with a specific employee. • Employees in key roles who never take annual leave, live significantly beyond their visible means, or insist on handling specific contractors exclusively.
Procedural & Emerging Red Flags	• Payment is requested for an invoice that includes a commission or fee payment that appears large given the service stated to have been provided. • Requests for payments to offshore accounts, "split invoices" to bypass approval limits, or vague "admin fees" with no supporting documentation. • Receive an invoice from a third-party that appears to be non-standard or customised. • Urgent demands to bypass the standard procurement process or an unexplained preference for a specific third party without a competitive tender.

Modern Slavery/Human Trafficking	
You become aware that a worker / contractor operating in our business or supply chains:	• Appears to be under the control of someone else and is reluctant to interact with others. • Appears frightened or withdrawn or shows signs of physical or psychological abuse. • Appears to be working excessive hours. • Appears not to be able to move around freely, and/or may not have access to personal identification. • Do not have possession of their own passports, visas, or ID documents. • Has few personal belongings, wears the same clothes every day or wears unsuitable clothes for work. • Is reluctant to engage with you or colleagues.

	• Is being dropped off and collected for work always in the same way, especially at unusual times – very early or late at night. • Lacks basic training and protective equipment for the work undertaken. • A third-party is unable to demonstrate supply chain transparency in a tendering process. • A third-party refuse to provide/disclose its human trafficking measures when requested. • You become aware that a third-party supplier to EirGrid is linked to modern slavery/human trafficking violations.

Fraud	
Behavioural	• Living Beyond Means: An employee exhibiting sudden wealth (e.g., luxury vehicles, costly vacations) that does not align with their known income. • Control Issues: A marked unwillingness to share responsibilities, delegate tasks, or take required annual leave, typically to keep their fraudulent actions concealed. • Unusual Vendor Relations: Having an unusually close or secretive relationship with a specific vendor or customer. • Defensiveness: A noticeable increase in irritability, suspicion, or aggressive reactions when asked routine questions regarding financial transactions.
Financial & Accounting	• Missing Documentation: Regular reports of "lost" or absent invoices, receipts, or contracts, or reliance on photocopies instead of original documents. • Unexplained Discrepancies: Inconsistencies between general ledger accounts and sub-ledgers, or an excessive number of manual journal entries and "adjustments" made without adequate explanation. • Duplicate Payments: Repeated payments to the same vendor on the same date or for identical amounts, which may suggest a "ghost" vendor scheme. • Mismatched Payees: Cases where the name on a cleared cheque or bank transfer does not correspond with the name recorded in the accounting system.
Procedural & Emerging Red Flags	Contemporary fraud also encompasses advanced digital and procedural evasion methods: • Evasion of Controls: Staff frequently omitting approval processes or "dividing" substantial invoices into lesser sums to remain within authorisation thresholds. • Artificial Intelligence (AI)-Driven Deception: The application of deepfakes (audio or video) in social engineering to facilitate urgent payments or "emergency" transfers. • Irregular Activity Hours: Employees entering financial systems or physical locations at extremely unusual times without a valid business justification.

Appendix 4: Financial Crime Response Process

The Investigation process is presented in the diagram below.