NETWORKS

ESB Networks DAC Compliance Code of Conduct for Staff

Issue date: October 2025

DOC-221008-AUB

Contents

Introduction

ESB Networks DAC, the Distribution System Operator, is committed to managing information and resources in compliance with our legal obligations and our Licence. Accordingly, a Compliance Code of Conduct has been developed to assist staff working for or interacting with ESB Networks DAC

Our Licence contains specific confidentiality and business separation provisions. We are also required by our licence to implement a Code of Conduct on the Transfer and/ or Movement of Employees.

This Code of Conduct sets out the correct procedures to ensure non-discriminatory behaviour in relation to ESB Networks DAC 's management of the national electricity infrastructure. No supplier or generator including ESB's own supply and generation businesses should gain a commercial advantage as a result of unfair discrimination, or access to confidential or commercially sensitive information relating to ESB Networks. Therefore, the core objective of this Code of Conduct is to avoid actual or potential conflicts of interest and to make sure that ESB Networks DAC takes its decisions independently, ensuring transparency and non-discrimination towards all network users.

The Code sets out the principles of compliance which staff must adhere to in carrying out their day to day duties. By adhering to the principles of compliance outlined in this Code we are not only fulfilling our legal and regulatory obligations (in particular the full respect of the rules on information unbundling) but we are also demonstrating that we are committed to ethical behaviour, transparency and fair competition.

Section 1
Scope & Principles Of The Code

1.1. Who does this Code Affect?

The Code applies to;

- All staff, either full or part-time, in the ESB Networks Business or ESB Networks DAC (collectively referred to as "ESB Networks Business Staff");
- Staff in business areas within ESB Group who provide services to or on behalf of ESB Networks;
- Staff who carry out corporate duties in relation to the ESB Networks Business; and
- Staff in other parts of ESB who interact with the ESB Networks Business;

Persons within the scope of this Code are collectively referred to as "ESB Networks Business Staff and Service Providers"

1.2. What is Commercially Sensitive ESB Networks Information?

Commercially sensitive information is defined as "any matter the disclosure of which would materially prejudice the interest of any person". Confidential information refers to any information relating to the business, affairs and finances of a system user being confidential to that system user, whether or not such information is marked confidential. Commercially sensitive and confidential information obtained or held by ESB Networks may include;

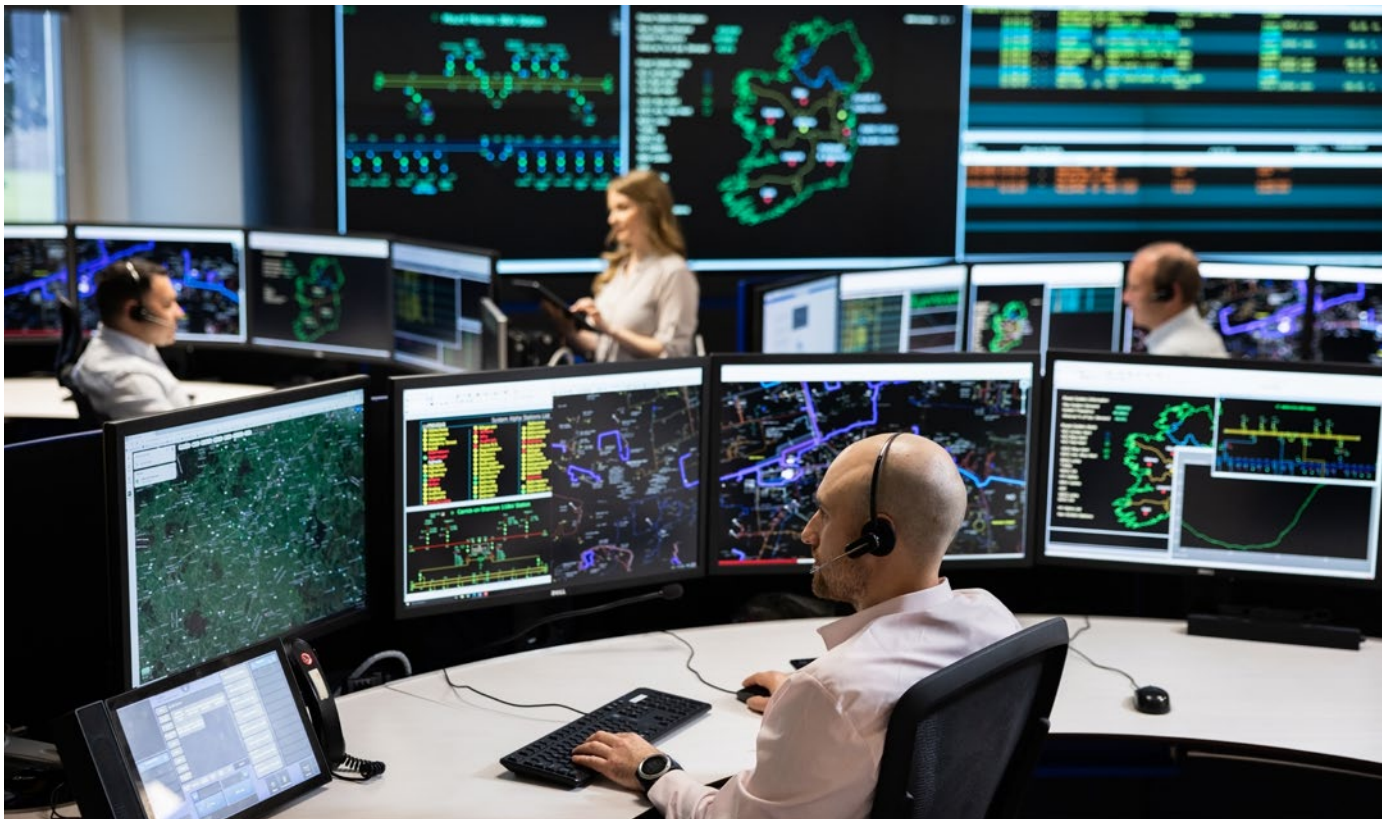
- Metering and use of system information relating to Suppliers or Generators;
- Commercial details of connections to the distribution or transmission system;
- Any ESB Networks information that could provide a Supplier or Generator with an unfair competitive advantage;
- ESB Networks information that has been marked by an authorised manager as commercially sensitive;
- Trade, business, activities, employment relations, procedures and arrangements, records, operations, organization, finances, dealings, security, methods and technology of and concerning ESB Networks DAC and/or any of its associated companies and/or their clients, which is not already in the public domain.

If you are unsure whether or not particular ESB Networks information is commercially sensitive or confidential you should consult your line manager.

Matters relating to commercially sensitive information are also addressed in the Protocol for the Disclosure of Commercially Sensitive Information which applies to ESB Group, which should be read in conjunction with this Code.

1.3. Principles we must adhere to when dealing with Confidential and Commercially Sensitive Information

- ESB Networks DAC is obliged to implement measures and procedures to preserve confidential and commercially sensitive information, to avoid actual or potential conflicts of interest and to ensure that ESB Networks DAC can make decisions independently, in a transparent and non-discriminatory way.
- This document is intended to ensure compliance with ESB Networks legislative obligations under the European Communities (Internal Market in Electricity)
- Regulations 2000 to 2014 and the European Communities (Internal Market in Electricity) (Electricity Supply Board) Regulations 2008 and the regulatory requirements on ESB Networks DAC made under this legislation.
- Additionally, in accordance with Licence requirements ESB Networks DAC may not discriminate unfairly against suppliers and generators, particularly in favour of ESB's Generation or Supply businesses
- All ESB staff are required to contribute to ensuring that ESB Networks DAC complies with these requirements. The purpose of this document is to set out clearly what is expected of all ESB Networks Business Staff and Service Providers in fulfilling these duties;
- With this in mind, ESB Networks DAC will strive to consistently apply ring-fencing protocols to ensure full compliance with legal and regulatory requirements.



Section 2
Information Management

ESB Networks Business Staff and Service Providers are required by law and the ESB Networks DAC Licence to preserve the confidentiality of commercially sensitive or confidential information and shall prevent information about the ESB Networks DAC activities which may be commercially advantageous being disclosed in a discriminatory manner. This section sets out this duty in detail. See also Appendix 1 which contain Guidelines for Control of Information Flow.

It is essential that care is taken to ensure that commercially sensitive information or confidential information relating to the ESB Networks Business is not passed to supply or generation activities of ESB Group in a way that provides an unfair advantage for these businesses over third party Suppliers or Generators. competitive.

It is expected of all ESB Networks Staff and Service Providers that they shall keep confidential and shall not, except as authorised or required to do so by his/her duties, use or disclose, or attempt to use or disclose, to any person, partnership or body corporate, any of the commercially sensitive information of ESB Networks DAC which come into his/her knowledge during his/her contract.

Access to information systems containing commercially sensitive and confidential information will be restricted to personnel authorised in accordance with the procedure below. Staff who are authorised to have access to commercially sensitive ESB Networks information or confidential information must treat this information as confidential and may only disclose this information to staff and external advisers who are authorised to receive the information unless certain exceptions apply as outlined below.

2.1 Authorisation Procedure

Confidential or commercially sensitive information may only be disclosed to “authorised” ESB Networks Business Staff and Service Providers, unless certain exceptions apply.

ESB Networks Business Staff and Service Providers may be authorised on the basis that they:

- Require the information for the proper performance of theirduties;
- Undertake to maintain the confidentiality of this information in accordance with this Code;
- Undertake to use this information for the proper performance of their duties; and
- Undertake not to use this information to provide an unfair competitive advantage to ESB’s own Supply or Generation businesses.

The requirement to restrict disclosure of commercially sensitive or confidential ESB Networks information to authorised persons does not apply:

1. Where the information is already in the public domain;
2. Where disclosure is in accordance with a legal requirement (e.g. Freedom of Information Act 2014, Access to Information on the Environment Regulations 2007 – 2014), licence requirement or for any judicial process;
3. Where disclosure is in accordance with an industry wide agreement or arrangement (including the Grid Code, Distribution Code, Metering Code and the Trading and Settlement Code) and the information is related to the affairs of the person or business requesting the information.

2.2 Information Access Controls

- Staff engaged in certain areas such as the MRSO/RMDS will be subject to special arrangements to ensure that access to certain information is further restricted on a need to know basis to individuals who are subject to specific confidentiality agreements.
- As part of licence Business Separation requirements, Staff Transfer Guidelines are in place. These Guidelines are contained in Appendix 2. Arrangements for staff transfers into or from the ESB Networks Business which prevent the unauthorised transfer of commercially sensitive information are contained in Section 3 of this Code. Undertakings by individual staff regarding non-disclosure of information may be required. In particular, Service Providers and ESB staff from other unregulated business units (e.g. Enterprise Services or Engineering & Major Projects) who may be carrying out work for the ESB Networks Business will be required to sign confidentiality agreements where they have access to commercially sensitive information.
- Access controls are in place to prevent unauthorized access to ESB Networks Business information. ESB Networks Business Staff and Service Providers should not attempt to bypass password protections or gain unauthorised access to restricted systems.
- Where shared premises exist, access restrictions prevent the inadvertent passing of confidential information to other businesses of ESB Group.
- Matters relating to commercially sensitive information are also addressed in the Protocol for the Disclosure of Commercially Sensitive Information which applies to ESB Group, ensuring separate platforms for handling of such information have been implemented.

Q **If you get a request for ESB Networks Information you should ask yourself three questions**

1. Is the information confidential or commercially sensitive?

2. Is the person authorised to receive the information?

3. Do certain exceptions apply?

No restrictions apply to information flow required to ensure the safety of staff or third parties

Section 3
Staff Transfers to / from ESB Networks

Under its Licence, ESB Networks DAC is required to implement arrangements for staff transfers into or from the ESB Networks Business which prevent the unauthorised transfer of commercially sensitive information.

Staff who:

i. transfer into another business area, subsidiary, affiliate or related undertaking of ESB from the ESB Networks Business; OR

ii. transfer into the ESB Networks Business from another business area, subsidiary, affiliate or related undertaking of ESB;

will be subject to the following Staff Transfer procedure and the Staff Transfer Guidelines contained in Appendix 2.

Details of the procedures to be followed when transferring into/from ESB Networks are available on the hub.

http://bsc.esb.ie/HRHome/Starters/Movers/Pages/JobMove.aspx

As a general rule if you are transferring from a position where you were authorised to receive confidential ESB Networks information to a position where the same authorisation is no longer appropriate, the following will apply:

- You may not bring commercially sensitive or confidential ESB Networks information, either in hardcopy or electronic form, to the new position other than as may be authorised for the new position;
- Your access to the NT account will be revoked. You will receive a new email address and you must apply for appropriate access to IT systems based on your new role; and
- You will still be obliged to maintain the confidentiality of commercially sensitive and confidential information which was disclosed to you prior to the transfer.

3.1. Transfer Arrangements

HR Governance ESB Networks is notified of a staff transfer following completion of a movers form which is available in appendix 2 of this document, or on the hub:
http://bsc.esb.ie/HRHome/Starters/Movers/Pages/JobMove.aspx

HR Governance ESB Networks will then make contact directly with the staff member and request two forms to be completed and returned:

- "Declaration of personal data" confirming that you have transferred only personal data
- Confirmation that you have read and understand the Networks Compliance Code of Conduct

IT will be notified by HR Governance Networks of the staff transfer and IT will revoke access to the old account and create new account.

The staff member's new Line Manager will approve and arrange appropriate IT access for the new role.

Where, in the opinion of the Networks Compliance Officer, (hereinafter referred to as the "Compliance Officer"), the risk or the reasonably perceived risk of a conflict of interest arising from the transfer can be effectively and proportionately avoided or mitigated by the measures set out in this Code, the Compliance Officer may determine that they are suitable.

Any final decision on the application of this Code is for the ESB Group Compliance Officer (hereinafter referred to as the "Group Compliance Officer").

A quarantine period (until the expiry of an appropriate time up to a maximum of 3 months) may be viewed as proportionate by the Compliance Officer on a case by case basis. This requirement only applies where the seniority and level of access to commercially sensitive information, the period of time during which such information held is likely to remain sensitive, and the business activity to or from which the person is moving causes the Compliance Officer to determine that they are necessary to impose. A staff transfer from the ESB Networks business to either the Supply, or Generation, or Wholesale Markets businesses of ESB Group shall be for a minimum period of three months.

The Compliance Officer shall, in particular, review instances where a staff member has transferred between the different businesses on a number of occasions. For example, in the event a staff member returns to ESB Networks Business within twelve months of the initial transfer, a subsequent move to ESB' Generation or Supply businesses shall be subject to a quarantine period determined by the Compliance Officer.

3.2 Additional Requirements for Relevant Transfers of Senior Management with Access to Commercially Sensitive Information

The following additional requirements shall apply in all instances to transfers of Executive Directors/Managing Directors and Senior Management (direct reports to an Executive Director/ Managing Director) into or out of the ESB Networks Business.

Prior to the transfer, the Group Compliance Officer shall submit a proposal to the Commission for Regulation of Utilities ("CRU") outlining the nature of the role and providing details on the proposed arrangements which may be applicable to the transfer based on a risk assessment including details in respect of the following:

Quarantine Periods
A quarantine period (until the expiry of an appropriate time up to a maximum of 6 months) may be viewed as proportionate by the Group Compliance Officer on a case by case basis.

This requirement only applies where the seniority and level of access to commercially sensitive information, the period of time during which such information held is likely to remain sensitive, and the business activity to which the person is moving such that the Group Compliance Officer determines that they are necessary to impose. The quarantine period should be proportionate to the sensitivity of the role and should not become an unnecessary cost or burden to the business.

Quarantine periods may be fulfilled in a number of ways including:

- period of annual leave;
- project assignment in a non-sensitive activity of the business;
- project assignment in an unregulated part of the business; or
- a combination of the above.

In addition, the Group Compliance Officer may make the transfer subject to the following:

- ***Trust & Confidence Declaration:*** The staff member has signed a confidentiality undertaking;
- ***Register of Material Decisions:*** A register of material decisions taken by the Senior Manager post transfer appointment (period to be determined on a case by case basis) which is available for review by CRU;
- ***Abstention:*** An obligation may be imposed on the senior or specialist staff member for an agreed period post transfer to:
  - recuse himself/herself from discussions, considerations and decisions of matters which directly and specifically affect the Relevant Activity from which they were transferred; and/or
  - abstain from contacting any clients, customers, suppliers or contacts of the previous employer or business unit without prior consent of his or her line manager or local Compliance officer.

The Group Compliance Officer will have the utmost regard to the view of CRU.

3.3. Appointment or Transfer of ESB Networks Compliance Officer

The appointment of the ESB Networks Compliance Officer will be subject to approval by CRU prior to the Officer assuming his/her responsibilities. Any subsequent transfer will also be notified to CRU along with reasons for the transfer.

Section 4
Non-Discrimination

In accordance with Licence requirements, ESB Networks DAC may not discriminate unfairly, particularly in favour of ESB's Generation (thermal and wind) or Supply businesses when carrying out the functions of the DSO, DAO and TAO. Therefore, if you work for ESB Networks or carry out an ESB Networks function on their behalf, the non-discrimination requirement will apply to certain aspects of your work.

Do

Consider all final consumers and embedded generators as customers of ESB Networks. ESB Networks is paid for providing services to these through their connection or use of system charges. All ESB Networks customers of a similar class should receive the same level of service.

If you are engaged in issuing jobs, organising outages or restoring supply you must perform these tasks without bias towards any particular Supplier or Generator. You should carry out day-to- day work on the transmission or distribution system based on professional and objective judgement.

Don't

You may not discriminate unfairly between customers on the basis of their supplier.

You may not promote the services of one supplier over those of another. Under no circumstances should you indicate or

imply that customers of an ESB Supply business would obtain a better standard of service from the ESB Networks business than customers of a non-ESB Supply business.

You may not provide any information, support, materials or services to ESB's Generation or Supply businesses or the ESB Wind Generation business other than on an arm's length basis and on the same basis as provided to others.

Section 5
Supporting Procedures

In addition to the measures outlined in Sections 1 to 4 above, the following procedures are in place to support and ensure compliance by ESB Networks DAC with its license requirements:

(i) Employment

The Managing Director of ESB Networks DAC or the senior management team may not be employed by any other part of ESB. The Managing Director reports directly to the Chief Executive of ESB. Board Members must comply with the ESB Code of Business Conduct for ESB Board Members.

Throughout the period of service with ESB Networks DAC each ESB Networks Business Staff and Service Providers should be bound by the terms of their service or employment contract, as the case may be. All ESB Networks Business Staff are expected to operate to a high degree of integrity and performance and comply with the ESB's Code of Ethics.

(ii) ESB Group Approach

Staff across ESB Group can make an important contribution to ensuring that ESB Networks DAC complies with its licence requirements.

- Staff who work for ESB's Supply business may not indicate that their customers would receive preferential treatment from the ESB Networks Business over any other suppliers.
- Staff who work for ESB's Generation (thermal and wind) or Supply business may not seek information, support, advice, materials or any preferential treatment from the ESB Networks Business.
- If Staff or Service Providers are not authorised to receive commercially sensitive ESB Networks Business information but inadvertently receive or get access to the information other than that relating to the affairs of their own business area (as provided for under exceptions identified in the Code) they should:
- Advise the sender or IT security that an inadvertent disclosure has occurred;
- Return or destroy any copies of the information disclosed; and
- Notify their line manager.
- Staff should recognise and accept that colleagues in other parts of ESB are obliged to maintain the confidentiality of commercially sensitive and confidential ESB Networks business information and should not solicit the information if they are not authorised to receive it.
- Where for governance and supervisory reasons, ESB Networks DAC provides information to corporate functions of the ESB, the Protocol on Disclosure of Commercially Sensitive Information approved by the CRU will apply to such disclosures.

(iii) Additional Procedures and Guidelines

There may be specific requirements that apply to the work that certain ESB Networks Business Staff and Service Providers are performing. The responsible line manager will advise if there are additional guidelines and procedures to be followed to ensure compliance with this Code and Licence Conditions.

(iv) Breaches of the Code

A staff member must bring his/her line manager's attention to inadvertent breaches of these or any other applicable compliance requirements so that corrective action can be taken. The incident should also be reported to the Compliance Officer so that arrangements can be reviewed to reduce the risk of a reoccurrence.

Deliberate breaches of this Code will be handled in line with existing disciplinary procedures. Breaches of this Code may have serious consequences for ESB Networks DAC not only in terms of its reputation for business integrity but also from a legal, regulatory and business continuity perspective.

(v) Overall Responsibility for Compliance

In accordance with Licence requirements the Board of ESB Networks DAC appointed a Compliance Officer on 20th April 2009. The Compliance Officer's appointment is subject to the approval of CRU. The Compliance Officer reports annually to the Managing Director and/or the Board of ESB Networks DAC on compliance issues.

The Compliance Officer's role is to ensure the Compliance Programme is implemented and adhered to at all times by requiring the manager of each area within the ESB Networks Business to report in relation to compliance with all areas of the compliance programme, by briefing all staff and senior management on the Compliance Programme requirements, and by reviewing the Compliance Programme when required.

The Compliance Officer shall report to the CRU, in such form and at such times as the CRU requires, on the effectiveness of the practices, procedures and systems implemented by the Licensee under the compliance programme.

As part of the ESB Networks DAC Compliance Programme approved by CRU, annual compliance sign-offs may be sought from ESB Networks Business Staff and Service Providers that the necessary measures and controls have been put in place to ensure compliance with Licence requirements.

(vi) Communication of the Code

This Compliance Code of Conduct is available on the ESB Networks DAC website, the ESB Group Intranet, from the Business Line Human Resources Manager, or the Compliance Officer. In particular, this Code must be made available for review to all staff subject to the staff transfer procedures in Section 3 and the staff member and the Compliance Officer must sign the checklist at Appendix 2 to this effect.

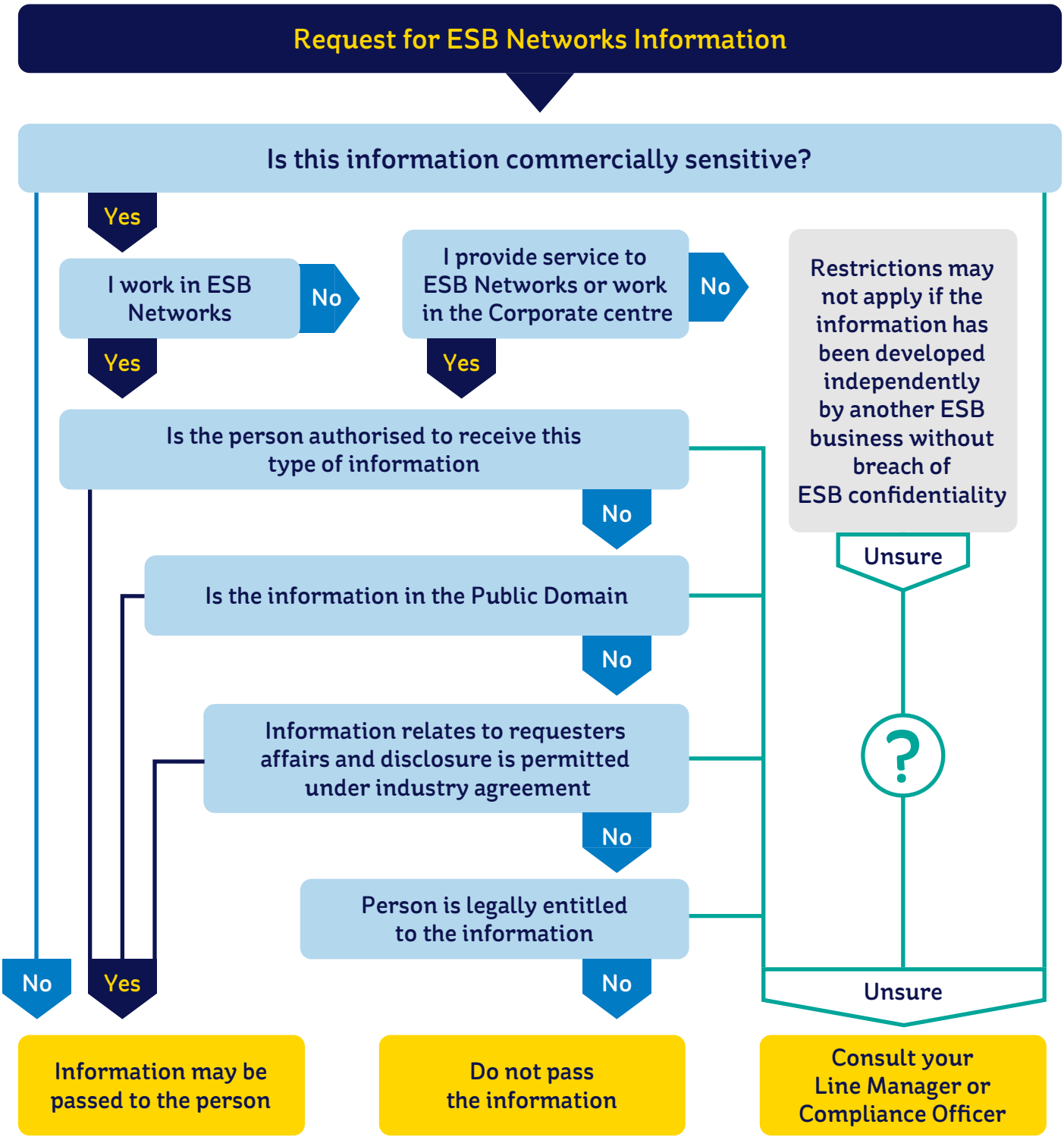
As part of the Compliance Activity Programme requirements, ESB Networks Business Staff are updated regularly on compliance issues and briefed on the Compliance Code of Conduct. An Annual Compliance Report is submitted to CRU for approval.

(vii) Revision of Code

This Code of Conduct for Staff Transfers is effective from 1 October 2020.

The Code will be formally reviewed every two years by the Group Compliance Officer. Significant changes to market arrangements may require an interim review to be conducted. CRU may request a formal report from the Group Compliance Officer on the operation of the Code at their discretion.

Appendix 1
Guideline for Control of Information Flow



Restrictions on Information Flow do not apply to matters of Safety

Appendix 2
Staff Transfer Guidelines

In order to meet Licence conditions ESB Networks DAC is legally obliged to implement a process for staff transfers to or from certain business areas.

The staff transfer arrangements approved by the Commission for Regulation of Utilities (CRU) in relation to ESB Networks DAC's activities are outlined in the Compliance Code of Conduct available on ESB Group Intranet and the Job Movers process on the hub.

In all cases the transfer arrangements require that:

- a staff member's IT access is revoked,
- that the staff member does not bring commercially sensitive information in electronic or hard copy format to the new position, and
- commercially sensitive information is not subsequently disclosed.

In order to ensure that ESB Networks meets these requirements a Movers form must be completed by Managers for all staff transfer regardless of the duration of the assignment.

Once the Movers Form has been completed HR Operations will forward details of the move to HR Governance, ESB Networks to co-ordinate the Move. HR Governance ESB Networks will then make contact directly with the staff member and request two forms to be completed and returned:

- "Declaration of personal data" confirming that you have transferred only personal data
- Confirmation that you have read and understand the Networks Compliance Code of Conduct

A template of the forms is set out below.

Adherence to these arrangements will be subject to monitoring by HR Governance in ESB Networks.

Communication Template to Transferring staff

Dear XX

Under its Licence, ESB Networks is required to implement arrangements for staff transfers into or from the ESB Networks Business which prevent the unauthorised transfer of commercially sensitive information.

Therefore on XX XX XXXX you will be provided with a new NT account, email and P drive by our IT department. All access associated with your previous role will be revoked and you must re-apply for appropriate access to IT systems based on your new role.

Further information on ESB Networks Code of Compliance can be found on the hub: Compliance Code of Conduct Booklet Link

I will notify IT of your move and they will contact you directly with all details, I have also attached two forms which you will need to sign, scan and return to me by email please.

- Declaration re Personal Data
- Confirmation in relation to the Compliance Code of Conduct

If you have any questions or concerns, please call me.

Thank you

HR Governance ESB Networks

Staff Transfer Form 1

ESB Networks Compliance Code of Conduct

In carrying out its licensed functions as Distribution System Operator (DSO) ESB Networks DAC is obliged to operate independently of other ESB businesses.

A Compliance Code of Conduct, approved by CRU (see link below), outlines the requirements in relation to operating on an arm's length, non-discriminatory basis with third parties with whom we do business.

Compliance Code of Conduct Booklet Link

The Code not only applies to Networks but also to staff within ESB Group who provide services to or on behalf of ESB Networks and staff who interact with Networks.

I confirm that I have read, understood and will comply with ESB Networks Compliance Code of Conduct.

Name: _____

Print Name: _____

Staff Number: _____

Date: _____

Completed forms should be scanned and emailed to Outlook account:
DSO - IT Compliance (ESB Networks)

Staff Transfer Form 2

IT Compliance for Movers Into or Out of ESB Networks Transfer of Personal Data Only

In order to meet the confidentiality and non-discriminatory conditions of our DSO Licence, ESB Networks is legally obliged to implement a process for employee transfers both into or out of ESB Networks. The licence requires that when an employee is moving into or out of ESB Networks the following takes place:

- The employee's IT access is revoked
- The employee does not bring confidential information in electronic or hard copy format to the new position
- Confidential information is not subsequently disclosed.

When an employee moves into or out of ESB Networks they will be given:

- A new NT account,
- New Outlook account,
- A new P Drive and
- Any access appropriate to the new role.

As part of this process an employee can be facilitated in transferring personal data. You are now required to sign a declaration to confirm that only personal data has been transferred.

I confirm that only personal data has been transferred from my IT systems as part of my move either into or out of ESB Networks.

Name: _____

Print Name: _____

Staff Number: _____

Date: _____

Completed forms should be scanned and emailed to Outlook account:
DSO - IT Compliance (ESB Networks)

ESB NETWORKS
Three Gateway,
East Wall Road,
Dublin 3,
DO3 R583

Tel 1800 372 757 or +353 21 2386555
Email esbnetworks@esb.ie

esbnetworks.ie