

ESB MRSO CONFIDENTIALITY POLICY

1 OVERALL POLICY

1.1 Policy

ESB MRSO, in conducting its business affairs will have access to Confidential Information and data including Commercially Sensitive Information and data;

ESB MRSO will conduct its business affairs in such a way as to maintain the confidentiality of said Confidential Information and Commercially Sensitive Information and data in its possession;

Appropriate internal controls, procedures and guidelines will be implemented to ensure this policy is adhered to.

1.2 Definitions

The term **Confidential Information** shall include:

All knowledge and information (whether or not recorded in documentary form or on computer disk or tape) relating to the trade, business activities, records, plans, operations, processes, organisation, finances, dealings, corporate plans, prices, quotations, business methods, business opportunities, research and development projects and technology of and concerning ESB MRSO [ESB or any of its Associated Companies].

All knowledge and information (whether or not recorded in documentary form or on computer disk or tape) in respect of which ESB MRSO owes an obligation of confidentiality

It shall specifically include **Commercially Sensitive Information** which is defined as:

All knowledge, information or data (whether or not recorded in documentary form or on computer disk or tape) being provided to ESB MRSO by a third party or other business of ESB, or any subsidiary or affiliate of ESB, which could, of it's nature, bestow a competitive advantage to a third party, or other businesses of ESB, or any subsidiary or affiliate of ESB.

2 INFORMATION FLOWS

2.1 General

Confidential Information obtained by ESB MRSO, concerning any particular entity will not be provided to or discussed with any other entity by ESB MRSO.

2.2 Commercially Sensitive Information

No Commercially Sensitive Information, or data which would enable Commercially Sensitive Information to be derived about an independent third party will be disclosed to another third party, or any other business of ESB, or any subsidiary or affiliate of ESB.

No Commercially Sensitive Information, or data which would enable Commercially Sensitive Information to be derived about a business of ESB or any subsidiary or affiliate of ESB will be disclosed to another third party, or other business of ESB, or any other subsidiary or affiliate of ESB

2.3 Exceptions

The exceptions to this policy 2.1 and 2.2 are

- 2.3.1 where at the time of disclosure the information is in or becomes part of the public domain other than through a breach of this policy.
(see Staff Guideline attached)
- 2.3.2 where the provision of confidential information is provided for in one of the electricity industry codes or bilateral agreements.
- 2.3.3 where the written permission of the originating organisation is obtained.
- 2.3.4 where the information is published by or the publication of which is required by a competent authority including but not limited to the Commission for Electricity Regulation, a competent authority of the European Union and the courts of any competent jurisdiction;
- 2.3.5 where the Commission for Electricity Regulation has agreed that certain information may be disclosed provided it is disclosed in accordance with any conditions which may be imposed by the Commission for Electricity Regulation.

3 PHYSICAL AND IT SECURITY

3.1 Physical Access

Regular access to ESB MRSO offices will be restricted to ESB MRSO staff only and will be restricted and controlled by means of appropriate methods.

3.2 Controls over printers, faxes and correspondence

Secure printing and fax facilities will be made available in the MRSO. Access to photocopiers will be controlled.

Incoming and outgoing postal arrangements will be managed by ESB MRSO.

3.3 Document and File Storage

All documents containing Commercially Sensitive Information will be treated in a confidential manner. Secure archive facilities will be provided for all files deemed to be confidential. Once archived, access to files will only be with the approval of a manager.

Staff will not maintain personal files (which include Confidential Information and excluding reference material) except for work currently in hand. Lockable cupboards/presses cabinets will be made available to all staff,

3.4 IT Controls

Adequate IT controls will be implemented to ensure the confidentiality, integrity and availability of information.

3.5 Document Disposal

Secure methods of document disposal will be provided.

4 PERSONNEL

4.1 Staff Mobility

Staff who transfer from ESB MRSO to another ESB business will not bring any Commercially Sensitive Information to the other business. Former MRSO staff may not be asked to divulge Commercially Sensitive Information and any incident of such may be reported to Manager Compliance and Information.

4.2 Staff Confidentiality

All employees of ESB MRSO will be required to sign an appropriate confidentiality agreement. This will include staff seconded to ESB MRSO on a temporary basis or staff providing a service to ESB MRSO who may obtain access to Confidential Information.

ESB staff who are given access to Commercially Sensitive Information for the purpose of internal audit or regulatory compliance will be required to sign a confidentiality agreement and will be bound by the terms of this policy.

4.3 Conflicts of Interest

Where conflicts of interest arise through membership of boards of directors or committees the individual concerned will report this to their immediate manager. The manager will take appropriate action to mitigate the conflict of interest.

4.4 Training

Management is committed to the introduction of these policies and subsequent procedures and will provide regular communication and appropriate training to ensure their successful implementation.

The MRSO will maintain guidelines for staff to assist in the interpretation and implementation of this policy.

5 USE OF DATA

5.1 Use of Third Party Data

Data obtained from third parties will only be used for the specific purpose for which it was intended and will be subject to the Data Protection Act or other duty of confidentiality, where appropriate.

If ESB MRSO wishes to use this data for any other purpose the written consent of the originating individual or organisation must be obtained.

6 OTHER EXTERNAL PARTIES

6.1 Use of Consultants

All external consultants will be required to sign confidentiality agreements and disclose any potential conflicts of interest. Where conflicts are identified ESB MRSO will ensure that the consultants have their own procedures in place to maintain the confidentiality of information received from ESB MRSO.

6.2 Provision of Data to External Bodies

Where there is a legal requirement, ESB MRSO will formally advise the relevant organisations of the disclosure.

Where there is no legal requirement to disclose information only information that is not commercially sensitive and/or information for which the consent of the originating individual(s) or organisation(s) has been received will be disclosed.

Staff Guideline for Condition 2.3.1 of MRSO Confidentiality Policy.

MSRSO should assume that confidential information is not in the public domain unless they have confirmation to the contrary.

For the purpose of confirmation a staff member may request

1. A copy of the publication
or
2. Confirmation from their immediate manager that the information is in the public domain.