Confidentiality and disclosure PROCEDURE

P-24

	Designation	Name	Signature
Prepared by			
Approved by			

List of Revision

Index	Date	Altered Item	Page no.

1) Purpose

1-1 The purpose of this Confidentiality and disclosure procedure is to lay down the principles that must be observed by all who work with Bureau Veritas Egypt and have access to confidential information.

1-2 This procedure, where relevant, shall be read in conjunction with the appointment letter and/or employment contract applicable to Bureau Veritas Egypt employees and personnel, and other work rules, policies and procedures applicable to Bureau Veritas Egypt employees and personnel.

1-3 Also this procedure will be applicable to Bureau Veritsa Egypt outsource process in conjunction with the contract.

2) Scope of Application

2-1 The scope of confidential information includes any information which is not publicly known. It can concern technology, business, finance, transaction or other affairs of the company. It includes information which is commercially valuable such as trade secrets or business information, as well as personal information. Examples of confidential information include but are not limited to: any document, improvement, product specification, formulations, plans, ideas, accounts, data, reports, drafts of documents of all kinds, correspondence, client information, lists and files, decisions, information about employees, strategies, drawings, recommendations, designs, office precedents, policies and procedures, budget and financial information in any form, i.e. physical, electronic, electromagnetic or otherwise. Confidential information to do with unpublished product conformity assessment can be particularly sensitive.

2-2 Disclosure of a product conformity assessment before a decision made to certification will cause irreversible loss of intellectual property rights to the owner of the product conformity application. Even after the certification audit has been completed, care must be taken not to disclose improvements to the product conformity until implemented and released by applicant. Trade secret protection will also be lost through open disclosure of the secret.

3) Reference

- ISO 17065:2012
- ISO 17002:2004
- ISO 17004:2005
- ISO 27001:2019
- ISO 27002:2022

4) Responsibility for Application

- Department managers
- Quality Manager
- Auditors
- Experts
- Staff
- Outsource

5) Definitions

- **Asset:**anything that has value to the organization
- **access control**: means to ensure that access to **assets** is authorized and restricted based on business and security requirements
- **accountability:**responsibility of an entity for its actions and decisions
- **authentication:** provision of assurance that a claimed characteristic of an entity is correct
- **availability:** property of being accessible and usable upon demand by an authorized entity
- **confidentiality:** property that information is not made available or disclosed to unauthorized individuals, entities, or **processes**
- **Control:** means of managing **risk,** including **policies. procedures** , **guidelines** , practices or organizational structures, which can be administrative, technical, management, or legal in nature
- **information asset:** knowledge or data that has value to the organization
- **information security:** preservation of confidentiality , integrity and availability of information

- **risk treatment:** process of selection and implementation of measures to modify risk

6) Procedure

6.1 PRINCIPLES

BVE expects all of its employees and personnel to handle all confidential information in a sensitive and professional manner. BVE employees and personnel are under an obligation not to gain access or attempt to gain access to information which they are not authorised to have. BVE, however, recognises the importance of an open culture with clear communication and accountability. BVE wishes to maintain personal and organisational safety and expects all employees and personnel to handle confidential information in a way which protects organisational security.

The purpose of confidentiality is essentially two fold. Firstly it protects sensitive or confidential information of BVE and its clients and customers. Secondly, in order for BVE to be effective, BE employees and personnel must be able to share information and knowledge, and therefore confidentiality is necessary as a condition of trust. The best protection against breaches in confidentiality is to keep the number of employees and personnel who have access to sensitive information to a necessary minimum. Intentional, repeated, accidental, or unauthorised disclosure of any confidential information by any member of staff will be subject to disciplinary action. Any such disciplinary action will take account of the confidential and possible sensitive nature of the information and will make sure that in dealing with it, no further breaches of confidentiality take place.

6.2 MAINTENANCE OF CONFIDENTIALITY & NON-DISCLOSURE

BVE employees and personnel:

- must keep confidential all confidential information;
- may use confidential information solely for the purposes of performing their duties as an employee of BVE; and
- may only disclose confidential information to persons who are aware that the confidential information must be kept confidential and who have a need to know (but only to the extent that each person has a need to know).
- All employees of BVE deals with client and handle client (service provider) information such as Auditor will sign form F-24-02
- Other employees of BVE who have to deal with the client (service provider) information for day-to-day work such as sales or operation manager will follow the BVE general code of ethics.

The employee's and personnel's obligation of maintaining confidentiality and non-disclosure does not extend to confidential information that is required to be disclosed by the employee pursuant to an order of a Court or any statutory authority. The employee or person will promptly notify the Company of any such requirement to enable the Company to take necessary action as deemed fit by the Company in the circumstances. BVE will use the confidentiality and disclosure risk assessment to control associated risks F-24-01.

At the end of the period of employment, BVE employees and personnel must return to BVE:

- all confidential information in material form;
- those parts of all notes and other records in whatsoever form,
- based on or incorporating confidential information;
- all copies of confidential information and notes and other records based on or incorporating confidential information; and
- all of BVE property and assets, in the possession or control of BVE employee or personnel.

The obligation of maintaining confidentiality and non-disclosure will continue even after the end of the period of employment or engagement in respect of all confidential information.

Any employee found to be in breach of this confidentiality and non-disclosure obligation, whilst employed by BVE will be disciplined, and in serious instances, dismissed. Any ex-employee found to be in breach of this confidentiality obligation may be subject to legal action being taken against them, dependent upon the circumstances of the breach, including cancellation/ withdrawal of any or all benefits if extended to the ex-employee by the Company.

This procedure will operate in conjunction with the contract of employment or letter of appointment BVE employees and personnel.

6.3 NEED TO KNOW

Confidential information is only to be disclosed on a "need to know" basis, only when the information is necessary to the employee for performing his or her employment duties effectively.

6.4 CIRCUMSTANCES IN WHICH INFORMATION CAN BE DISCLOSED

• If the information is required by or under a Court order or of a statutory authority, the employee or person will promptly notify the Company of any such requirement to enable the Company to take necessary action as deemed fit by the Company in the circumstances.

• Where disclosure can be justified for any other purpose. This is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. A request for information by the police must be carefully considered.

BVE employee must be able to justify any decision when information has been disclosed.

6.5 STORAGE OF DATA

No written document containing confidential information must be left visible where it can be read by anyone. This includes telephone messages, computer prints, letters and other documents. All hardware containing confidential information must be housed in a secure environment. Security precautions must be taken in accordance with BVE Policy and Procedures.

6.6 THE MEDIA

Confidential information must not be passed on to members of the press, or other media communications without the written consent of QA manager and for a particular purpose.

6.7 DISPOSAL OF INFORMATION

All media containing confidential information must be disposed off in a manner that ensures that information is not disclosed to an unauthorized person.

7) Forms:

#	Name	Code
1.	**Confidentiality and Non-disclosure Declaration**	F-24-01
2.	**Confidentiality and disclosure Risk Assessment Form**	F-24-02
3.		