Introduction

BESA has in place an Information Security Management System (ISMS) which conforms to the ISO/IEC 27001 international standard. This ISMS helps to provide governance and control of the framework our organization uses to protect its information assets and reduce its risk. It is important that everyone involved in the ISMS understands their role and how the activities they perform contribute to meeting business and information security requirements and the overall objectives of the organization.

The establishment and ongoing maintenance of information security awareness and competence is a key process within the ISMS as it underpins many of the other processes in use. Creating and maintaining an effective relationship with business management, users and other interested parties will ensure that information security controls are implemented in ways that the business wants, thus limiting impact on business performance and growth.

This document sets out how interested parties both within and outside of BESA will be communicated with on the subject of information security. It identifies who the interested parties are and how an effective communication channel will be established.

Communication Programme

The general approach to ensuring effective engagement and communication with respect to the ISMS within BESA is as follows:

1. Identify the audience/interested parties
2. Define the appropriate communication topics for each interested party
3. Agree the most appropriate methods of engagement and communication
4. Implement the program
5. Obtain and act on feedback about the success of the communication, via input to the continual improvement plan

These steps are considered individually in the following sections.

Audience

This communication program is aimed at interested parties, both internal and external, contract and permanent, who have a part to play in the operation and development of the ISMS within BESA.

mfi@besa.org.al
www.fondibesa.com

The interested parties include:

- Shareholders
- BESA Management Board
- BESA IT Security Steering Committee
- BESA IT Security Officer
- BESA Local Company Management Board (BESA LCMB)
- Second Level Banks
- Competitors
- Customers
- Employees of the organization
- Contractors providing services to the Organization
- National government organizations
- Competitors
- Media
- EU Authorities
- ISO 27001 Certification Body
- External Auditor
- The Commissioner for the Protection of Personal Data

Communication Topics

The communication program is intended to communicate the key items of information in the following main areas:

- The business environment in which the ISMS operates, including significant changes as and when they occur
- The overall framework of the ISMS including the vision, policies, plans and objectives that are to be achieved
- How the information security measures in place relate to the needs of the business, both now and going forward?
- How the ISMS is intended to capture and fulfil the business requirements for information security
- The statutory, regulatory and contractual requirements and constraints within which the ISMS must operate
- Updates on how plans are progressing towards meeting the defined objectives of the ISMS
- Awareness of information security issues and risks and our approach to addressing them

The level of detail required in the above areas will vary across the interested parties involved.

mfi@besa.org.al
www.fondibesa.com

Communication Methods

There are a number of established communication methods in place within BESA and these will be used where possible. These include:

1. Regular Team Meeting (Once per month)
2. Email Communication
3. Phone call communication. Webpage uses for wide communication with public
4. Internal Chat

Where appropriate, additional methods will be put in place, on either a temporary or permanent basis, to supplement those already available.

A breakdown of the ways in which the necessary information will be communicated to the relevant interested parties is shown in the following table.

Interested Party	Subject of Communication	Method(s)	Frequency
Executive Management	Information security strategy High level risk management Policy setting High level reporting	Board briefings [Information Security Manager] 1-1 with Finance Director	Yearly
Departmental Management	Information security awareness Security requirements for new IT systems Review of risks and issues Reviews of security breaches	IT Steering Group Specific agenda items at Senior Management Team Meetings IT Change Advisory Board	Yearly
IT Users	Communication of Information Security Policy Ad-hoc reminders when important events occur e.g. breaches Warnings and awareness	Newsletters Surveys E-Zine articles Emails	Yearly
IT staff	Communication of Information Security Policy Suggestions for improvement Penetration testing	Briefings Project meetings	Yearly

mfi@besa.org.al
www.fondibesa.com

Second Level Banks	Information security policy Contractual requirements Supplier obligations Suggestions for improvement	Supplier meetings Project meetings	Yearly
Customers	Purpose of the ISMS Information security policy Controls in place	Described on website	Ongoing

Table 1 - Communication methods

Communication Procedures

Procedures will be established for each of the communications methods identified above so that they are performed in a managed, repeatable way.

These procedures are referenced here:

1. Verbally
2. Mail
3. Phone call
4. Meeting

Feedback about Communication

For each interested party, a designated relationship owner will be agreed who is responsible for obtaining feedback on the success of communication and managing the relationship on an ongoing basis. Relationship owners are shown in the following table.

Interested Party	Relationship Owner
Executive Management	Chief Financial Officer
Departmental Management	Information Security Officer
IT Users	Information Security Officer
IT staff	Information Security Officer
Second Level Banks	Information Security Officer + IT Manager
Customers	IT Steering Committee

mfi@besa.org.al
www.fondibesa.com

Other interested parties	Information Security Officer

Table 2 - Relationship owners

In general, reviews will be held with each interested party at least once per year. They may be held more frequently if top management feel it is warranted.

Feedback about the success of communication will be collected, evaluated and, if appropriate, incorporated into the program as soon as possible.

Conclusion

Having effective communication with interested parties is absolutely key to the success of the ISMS implementation within BESA. The communication methods set out in this document should help to ensure that everyone involved remains well informed about information security issues and has an opportunity to provide feedback both on the channels used and their content.

mfi@besa.org.al
www.fondibesa.com