Insert company logo here

Communication Procedure

Document Control

Document Number:	ISMS-PRO-006
Version Number:	1
Review Date:	Insert date
Next Review:	Insert date
Authorised by:	Insert Job Title and Department

Version History

Version	Date	Author	Brief Description of Changes
1	Insert Effective Date	Insert Author	Describe changes that were made to document in order to qualify changing the Version.

1. Purpose

The purpose of this procedure is to ensure that effective internal and external communication takes place within Insert company name.

2. Scope

The **scope** of this procedure covers the process for communicating with staff to involve them in the achievement of ISMS objectives and to ensure that staff is informed of certain information

The **objective** is that management should actively encourage feedback and communication from people as a means of involving the staff in its security achievements

3. References

- ISO 27001:2013 Standard

4. Associated Documents

- None

5. Responsibility

Management has the responsibility, designated authority and accountability to ensure that:

- Effective communication processes are established, implemented and maintained in accordance with the requirements of this procedure.
- Internal and external communication processes are established, implemented and maintained in terms of the requirements of this procedure. These processes shall include the communication processes of the organisation that conveys important messages, encompassing summaries of critical meetings to all staff.
- All Company employees have the responsibility to conduct themselves in a circumspect manner ensuring that the image of the Company is not damaged or discredited in any manner or means.

The Security Officer or designate shall be responsible to ensure that all staff are appropriately informed of agreed information to comply with the Standard and that this procedure is fully implemented.

The Security Officer or designate shall collect feedback and report such to the Director, after the feedback had been analysed for trends, etc.

6. Definitions

- None

7. Internal Communication

The management team shall clearly define intra and inter communication lines for the organization. These communication lines shall be documented; and communicated to all staff. Adherence shall be maintained unless under exceptional cases.

Specific duties, responsibilities and authorities for all employees are defined in their relevant job descriptions and employment contracts.

Communication to interested parties will depend on the level of interest and the relevance of the communication to be done.

The Security Officer shall implement an effective and efficient process for communicating the security policy, requirements, objectives and accomplishments.

The Security Officer shall communicate the organization's performance improvement and directly involve employees in the achievement of information security objectives. The Security Officer will actively encourage feedback and communication from the staff as a means of involving them.

Activities for communication within the company includes, for example, but is not limited to:

- Management-led communication in work areas,
- Team briefings and other meetings, such as for recognition of achievement,
- Notice-boards and posters,
- Electronic media, such as email and websites, and
- Employee suggestion schemes.

A staff member who wishes to address any business matter, at any given time, whether verbally or in writing, shall do so through their relevant manager and the Security Officer**,** a meeting shall be arranged; for discussion as is appropriate to the need.

Action items arising out of these meetings shall be attended to and their actions communicated to the relevant staff members without undue delay or at the next scheduled meeting.

Electronic communication shall be used to make information more readily available between staff.

Senior staff meetings are called by the Approval Authority's for discussions which may include:

- announcements of business and organisational changes
- reviews of turnover and business objectives
- noting performance and customer satisfaction
- discussing problems requiring corrective action
- safety and security problems
- general business and technical matters.

From these discussions certain information is identified as being important for communication to employees, whilst maintaining discretionary confidence.

What will be Communicated	Frequency of Communication	To Whom	By Whom	Method of Communication
All aspects surrounding the Information Security Management System (ISMS)	As required, but at a minimum once a year	All Employees	Management ISMS Representative/s	Meetings, Training Sessions, Notice Boards
Performance of the Information Security Management System (ISMS)	As required, but at a minimum once a year	Top Management	Management ISMS Representative/s	Management Review Meetings
Information Security Policy	As required, but at a minimum once a year	All Employees	Management ISMS Representative/s	Meetings, Training Sessions, Notice Boards

8. External Communication

The organization shall ensure that there are proper communication channels available to communicate with external parties. These external parties include, but are not limited to the following:

- Suppliers / Contractors
- Authorities
- Clients, etc.

Communication should be directed in writing, if and when possible, in the forms of:

- Emails
- Formal Letters, or,
- Telephonically with follow up email

Any external issues relating to breach of contract/ information security, should be dealt with in a professional and timeous manner. Any employee that is aware of any of these issues, if and when they arise, should inform Management to ensure that a resolution can be brought forward and that the external party is informed of the issue/matter. External communication can also be related to positive feedback relating to the party in question.

Refer to: ISMS-SP-001 Strategic Plan

What will be Communicated	Frequency of Communication	To Whom	By Whom	Method of Communication
Certification Award, information regarding procurement requirements (Requests for	As and when required, but once a year at a minimum	Suppliers and Contractors	Insert Responsible Person	E-mails, Telephonic, Meetings

information), Non-compliance as well as contractual obligations				
Information Security breaches	As and when required	All relevant staff, suppliers and interested parties	Insert Responsible Person Management ISMS Representative/s	E-mails, telephonic
Declarations, Compliance certificates and documentation etc.	When and if required	Statutory and Regulatory Authorities	Management ISMS Representative/s	E-mails, online platforms
Information Security Policy	When and if required	All Interested Parties (external)	Management ISMS Representative/s	E-mails