



INNOVATION™
DELIVERY
RESULTS

INFORMATION SECURITY RISK OBJECTIVES STATEMENT

SIGNOFF SHEET

AUTHORS/CONTRIBUTORS

Author(s)	Position	Email	Contact Number
Van Dijk Auditors			
Gayle Roseveare	Chief Operations Officer	gayler@bui.co	+27 72 347 6112

CHANGE RECORD

Date	Author(s)	Version	Change Reference
2022-06-29	Van Dijk Auditors	V1	New Policy
2022-10-25	Dhiren Boodhia, Gayle Roseveare and Mekail Ramjee	V1.1	Clause Update

REVIEWS

Date	Author(s)	Version	Change Reference
2022-06-30	Gayle Roseveare	V1	Final Review

BUI GROUP

DIRECTORS: A. Sharp, R. Roseveare, W. Malan

CONTENT

1.	SCOPE	4
2.	OBJECTIVE	4
3.	PLAN TO ACHIEVE OBJECTIVES.....	5
4.	APPLICABILITY	5
5.	EXEMPTION	5

BUI GROUP

DIRECTORS: A. Sharp, R. Roseveare, W. Malan

GLOSSARY OF TERMS

Term	Explanation
Affiliated Companies	In relation to First Technology Investments (Pty) Ltd, a subsidiary of this entity, or any division or operating branch of each subsidiary of this entity and all of its subsidiaries
BUI	BUI Medical and Technology Suppliers (Pty) Ltd and all subsidiaries.
Electronic Document	Soft copy of a document that is electronically stored within BUI approved guidelines
Employees	An employee and/or any member of staff and/or independent contract and/or subcontractor of the Employer and/or any individual or entity involved in the provision of services on behalf of the Employer
External Document	Document originated by an external third party
Objective	The defined purpose or aim of a Process, an Activity, or an organisation. Objectives are usually expressed as measurable targets.
Official Document	Document established such as BUI Policies, Manuals and Processes
Permanent Employee	An employee appointed in a position on the staff establishment of an organisation on an open-ended contract.
Policy	A set of principles or rules formulated and enforced by top management intended to direct and limit actions in pursuit of an agreed practice or long-term goals.
Procedure	A fixed, step-by-step sequence of Activities or cause of action (with definite start and end points) that must be followed in the same order to correctly perform a task.
Process	A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs. A process may comprise of one or several Procedures.
Record	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction or business.
Standard	A standard specifies uniform uses of specific technologies or configurations. Here we are talking about a specific internal standard of an organisation.
Subsidiary(ies)	Shall mean the following wholly owned subsidiaries of BUI Medical and Technology Suppliers (Pty) Ltd (as updated from time to time): <ol style="list-style-type: none"> 1. BUI Security Services (Pty) Ltd 2. BUI Ltd 3. BUI Consulting LLC 4. MTOM Systems Ltd

BUI GROUP

DIRECTORS: A. Sharp, R. Roseveare, W. Malan

1. **SCOPE**

BUI's Exco is committed to establishing clear objectives and an effective information security plan to protect its key business activities and meet its obligations to interested parties, including customers, shareholders, employees, and suppliers.

As part of this commitment, the organization has established an Information Security Management System (ISMS) that complies with the requirements of the ISO 27001 international standard for information security.

In line with the standard, it is essential that our information security objectives are consistent with our policies, measurable where practicable, communicated effectively within the organization (and outside where appropriate) and updated as part of the ISMS management review process.

Objectives will be based on a clear understanding of our information security requirements, including those from interested parties, and will consider the results of risk assessments carried out at various levels within the organization.

BUI plan to meet its information security objectives is also described, including:

- What will be done.
- What resources will be required.
- Who will be responsible.
- When it will be completed.
- How the results will be evaluated.

This document should be read in conjunction with other components of the ISMS, which give background information about internal and external issues relevant to the organisation's purpose, the requirements of interested parties and the organisation's **Information Security Policy**.

These include:

- Information Security Context, Requirements and Scope
- Information Security Roles, Responsibilities and Authorities

2. **OBJECTIVES**

In order to assess whether the ISMS is working as intended it is essential that clear objectives are defined, and a system of monitoring and measurement established to record progress against targets.

High-level objectives for information security are described in **Annexure A** and the overall framework for setting lower-level objectives.

Methods for determining to what extent objectives are being met, are set out in **BUI's Monitoring, Measurement, Analysis and Evaluation Matrix**.

BUI's duty is to avoid and mitigate risk where possible. BUI has invested resources to enable the mitigation of residual risk through effective risk management. Risk treatment plans have been developed and to proactively manage risks should they arise.

2.1. As part of the ISMS management review process, objectives for information security are regularly set, reviewed and updated in the following major areas:

2.1.1. Quality – how the ISMS works in protecting the organisation’s information security assets

2.1.2. Capability – maintain the knowledge, skills and experience available

2.1.3. Cost – financial and resource utilisation required to maintain and improve upon the ISMS

2.1.4. Risk reduction – the degree to which known risks are identified and treated

In discussion with the management team and based upon documented requirements, BUI has agreed specific objectives in information security as shown in **Annexure A**.

Achievement against these objectives will be tracked as part of regular management reviews of the ISMS.

3. PLAN TO ACHIEVE OBJECTIVES

In order to achieve our objectives, it is essential that we have a clear plan that encompasses, adequate resources with the full support of BUI’s Exco. The success of this plan will determine whether BUI remains adequately protected against unwanted events and their potential impacts.

The plan shown in **Annexure A** details the tasks required in order to achieve each objective, together with the resources required, person responsible and completion timescale of each objective. The method for evaluating the success of each task will vary according to the nature of the task.

The plans progress will be tracked by the ISMS Manager and reported to BUI’s Exco in accordance with **BUI’s Management Review Standard**. This plan will be managed in conjunction with continual improvement activities, which may be driven by audit results (internal & external); risk assessments and management reviews and other competencies.

4. APPLICABILITY

This Statement applies to BUI Medical and Technology Suppliers (Pty) Ltd and Subsidiaries (“BUI”) and covers all BUI Employees, Consultants and Third Parties working under contract for BUI, to whom it shall abide by the requirements of this Policy.

5. EXEMPTION

The Group Chief Executive has the sole right to exempt a person or application from this Statement, or part thereof. The exemption will be null and void unless:

- It is in writing;
- It is signed and dated by the Chief Executive Officer;
- The Internal Audit Department is notified of the exemption; and
- A record is kept of the exemption