ISMS Policy

It is the policy of **BARUTI** that information in all its forms written, spoken, recorded electronically, or printed will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period to be determined by each entity within **BARUTI**.

At each entity and/or department level, additional policies, standards, and procedures will be developed detailing the implementation of this policy and set of standards and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

The aim of the **BARUTI** ISMS is to measure and verify our commitments on the availability, confidentiality, and integrity of the information, by relying on a business continuity and traceability process in a field of application in strong interaction with the infrastructures of our customers. This covers the activities of the IT services (monitoring and operation) and Support (guarantee, maintenance and proactive support).

We endeavor to efficiently take into consideration our customers' expectations on information security, while complying with the legal and regulatory requirements applicable to our activity, the contractual obligations and the requirements of the ISO/IEC 27001:2013 standard. Information security risk management is accomplished in accordance with the ISO/IEC 27005:2018 standard.

We are continually improving our ISMS by performing risk analyses, reviews and audits and keeping close track of our performance indicators, while listening to our customers.

The **BARUTI** management is in charge of communication and ensuring everyone understands our policy and related objectives. Management also ensures that the system which is set up is planned, shared and deployed efficiently by providing the necessary human, organizational and technical resources.

A. The scope of information security includes the protection of the confidentiality, integrity and availability of information.

B. The framework for managing information security in this policy applies to all **BARUTI** entities and workers, and other Involved Persons and all Involved Systems throughout **BARUTI**.

C. This policy and all standards apply to all protected information and other classes of protected information in any form as defined in **Information classification matrix.**

Approved by:

Muhamet Veliu - CEO

Date: 12.05.2022

Place: Prishtina