1. PURPOSE

Arneca Technology considers corporate information a very valuable asset. Information is critical to the sustainability of our business operations and it needs to be properly protected. The Technology Information Security Management System (BGYS) implements the ISO 27001 standard to minimize the risks and impact of business information on Privacy, Integrity, Availability.

2. INFORMATION SECURITY POLICY

2.1. As Arneca Teknoloji and its employees, we undertake to apply the following rules in order to eliminate and manage all kinds of risks to our business continuity, information assets and personal data;

- To document, certify and make it a corporate culture and continuously improve it in a way to fulfill the requirements of our information security management system,
- To protect all information assets owned by Arneca Technology and belonging to customers, business partners, stakeholders, suppliers or other third parties,
- To ensure information security conditions within the framework of international standards, laws and regulations, to continuously improve, develop and review information security by managing existing and potential risks,
- To ensure the confidentiality, integrity and availability of information and protect it from unauthorized access,
- To prevent incidents and violations that will affect information security business continuity,
- To take the measures specified in the Personal Data Protection Law and to work in full compliance with the Personal Data Protection Policy,
- To assess Information security risks by all units in line with the processes and to prioritize the risks and to take necessary measures.

2.2. All employees and relevant third parties are personally responsible for fulfilling the requirements of the information security policy.

2.3. In case of non-application or neglect of the information security policy, the legal requirements of the relevant contracts are applied.

2.4. At least once a year, a penetration test is performed by an external source for our Company's Systems. Actions are planned for the findings detected.

2.5. Information Security awareness training is provided to our employees at least once a year. Our employees access Information Security policies and procedures through the common area they are authorized to access.

2.6. Information Security policies, procedures and security awareness training materials are reviewed once a year by the relevant responsible parties to ensure that the content is up-to-date. Updated documents are announced to employees and relevant third parties.

2.7. As a result of internal and independent audits, the corrective actions required to close the nonconformities or security violations related to information security are planned and followed up by the relevant unit managers.

2.8. Senior Management,leads the taking of corrective actions related to information security; monitors the closure by taking action.

2.9. In cases where sensitive and critical information must be shared with third parties outside the organization, the rules of information transfer must be determined and secured by contracts.

2.10. Legal department should be consulted when preparing information transfer agreements.

2.11. Information transfer agreements should include the following issues in terms of information security:

- Responsibilities for transmission, dispatch and receipt control and notification should be defined.
- Procedures should be defined to ensure traceability and non-repudiation.
- Minimum technical standards for packaging and transmission should be established.
- Escrow conditions should be defined.
- Standards for the identification of couriers should be established.
- In the event of an information security breach such as loss of data, the responsibility and liabilities should be determined.
- Access controls appropriate to the classification of the information transferred and acceptable levels of these controls should be determined.

2.12. Special methods, such as cryptographic controls, should be used to protect sensitive information in electronic media.

2.13. Procedures and standards should be established for the protection of the physical medium being transferred.

2.14. The oversight mechanism required to protect information during information transfer should be defined and implemented.

2.15. The specific mechanisms used for the transfer of confidential information should apply to all external organizations and be consistent with all types of agreements.

3. SANCTION

3.1 Judicial and administrative legal proceedings against personnel, stakeholders, and third parties who violate the rules and processes established under the safety of information may be performed and/or one or more of the terms of its sanctions under related agreements may be applied.

3.2 In case of violation of Information Security Policies, the Disciplinary Directive are implemented with the approval of the Information Security Team and the relevant manager.