

First Issue Date
04.12.2023

Revision No/ Last Revision Date

Page No
1/2

ATÜ Turizm İşletmeciliği A.Ş. takes all necessary measures to protect customer data, which is the most valuable asset it owns, and makes developments in the focus of people, process and technology. Like every company in the information technology world, ATÜ Turizm İşletmeciliği A.Ş. uses suppliers/consultant companies and receives support in its processes. All third party companies from which ATÜ Turizm İşletmeciliği A.Ş. receives services should take the technical measures communicated by ATÜ Turizm İşletmeciliği A.Ş. and specified in the contracts and work with ATÜ Turizm İşletmeciliği A.Ş. in the light of these rules. In order to control this situation, ATÜ Turizm İşletmeciliği A.Ş. periodically audits its suppliers and provides a continuous development environment by eliminating nonconformities.

In line with the checklists prepared on the basis of world-accepted best practices and standards, ATÜ Turizm İşletmeciliği A.Ş. expects all its suppliers serving in the field of information technology to basically comply with the following issues:

- Establishing access policies and ensuring access controls of sensitive data in accordance with the principle of need to know
- Implementation of multiple authentication methods where necessary by implementing strong password policies for all internal and external accesses
- Tightening of systems based on internationally accepted standards
- For systems and applications that process or store sensitive data; using the appropriate encryption, masking or anonymization steps
- Using an effective anti-virus method to protect systems from viruses, trojans or other harmful things
- Implementation of data classification, data discovery and data loss prevention processes to prevent unauthorized removal of sensitive data
- Making secure software development processes a culture throughout the organization and identifying and closing the shortcomings before the applications are brought to the live environment
- Designing data centers according to the best standards by ensuring the physical security of the environments where data is kept
- Operating an effective incident recording and incident management process, operating detection mechanisms before an incident occurs and operating reporting processes in accordance with regulations



**ISMS POLICY FOR OUTSOURCED
EMPLOYEES**

QUALITY MANAGEMENT SYSTEM
Reference: ATU.PL.14

First Issue Date
04.12.2023

Revision No/ Last Revision Date

Page No
2/2

- Regular testing of applications and systems by operating vulnerability management processes
- Establishing corporate policies, procedures and processes to work according to best practices and creating a continuous improvement environment that will keep cyber resilience at the highest level